

NORTH-HOLLAND  
MATHEMATICAL LIBRARY

---

# Covering Codes

G. COHEN  
I. HONKALA  
S. LITSYN  
A. LOBSTEIN

North-Holland

## COVERING CODES

# North-Holland Mathematical Library

## *Board of Honorary Editors:*

M. Artin, H. Bass, J. Eells, W. Feit, P.J. Freyd, F.W. Gehring,  
H. Halberstam, L.V. Hörmander, J.H.B. Kemperman, H.A. Lauwerier,  
W.A.J. Luxemburg, F.P. Peterson, I.M. Singer and A.C. Zaanen

## *Board of Advisory Editors:*

A. Björner, R.H. Dijkgraaf, A. Dimca, A.S. Dow, J.J. Duistermaat,  
E. Looijenga, J.P. May, I. Moerdijk, S.M. Mori, J.P. Palis, A. Schrijver,  
J. Sjöstrand, J.H.M. Steenbrink, F. Takens and J. van Mill

VOLUME 54



ELSEVIER

Amsterdam – Lausanne – New York – Oxford – Shannon – Tokyo

# Covering Codes

Gérard COHEN

*ENST, Paris, France*

Iiro HONKALA

*University of Turku, Finland*

Simon LITSYN

*Tel-Aviv University, Israel*

Antoine LOBSTEIN

*CNRS - ENST, Paris, France*



1997

ELSEVIER

Amsterdam – Lausanne – New York – Oxford – Shannon – Tokyo

ELSEVIER SCIENCE B.V.  
Sara Burgerhartstraat 25  
P.O. Box 211, 1000 AE Amsterdam, The Netherlands

ISBN: 0 444 82511 8

© 1997 Elsevier Science B.V. All rights reserved.

No part of this publication may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, mechanical, photocopying, recording or otherwise, without the prior written permission of the publisher, Elsevier Science B.V., Copyright & Permissions Department, P.O. Box 521, 1000 AM Amsterdam, The Netherlands.

Special regulations for readers in the U.S.A. – This publication has been registered with the Copyright Clearance Center Inc. (CCC), 222 Rosewood Drive, Danvers, MA 01923. Information can be obtained from the CCC about conditions under which photocopies of parts of this publication may be made in the U.S.A. All other copyright questions, including photocopying outside of the U.S.A., should be referred to the publisher.

No responsibility is assumed by the publisher for any injury and/or damage to persons or property as a matter of products liability, negligence or otherwise, or from any use or operation of any methods, products, instructions or ideas contained in the material herein.

This book is printed on acid-free paper

Printed in The Netherlands

*To*

*Aude, Clairette and Maurice*

*Aino, Kauko and Juha*

*Maya, Elena, Lola and Nathan*

*Martine, Doud and André*

This Page Intentionally Left Blank

# Preface

Covering and packing the euclidean space by spheres are old and well-known problems. The discrete counterpart of the packing problem has been extensively studied within the theory of error-correcting codes. Its dual, the covering problem, has received much less attention over the years. The last decade, however, has witnessed the blossoming of active research in the area, now materialized in the publication of over 500 papers. We feel that during these ten years the area of covering codes has come of age and developed into an elegant discipline with its own flavour and techniques. Our purpose is, on the one hand, to give an account on the state of the art in the theory of covering codes and, on the other hand, to show how a number of issues are related to – or can be viewed as – covering problems.

In a basic covering problem, we have a vector space over a finite alphabet which we wish to cover with as few spheres of a given radius as possible. This means that we can approximate any point in the space by one or more of the centres with a given accuracy. The covering problems are mathematically and aesthetically appealing in their own right, and lend themselves to technical applications, e.g., data compression.

This book is intended for people involved in communication, algorithms, computer science, discrete mathematics, geometry, algebra or number theory. We have strived to remain accessible to a wide audience, although a minimal background in coding theory, algebra and discrete mathematics is occasionally required. The chapters are fairly independent, which should allow nonlinear reading.

Roughly speaking, the first half of the book is about the covering radius of codes – and we shall emphasize binary codes – whereas the second half deals with generalizations and related problems. We begin with basic definitions and results in the first two chapters. Chapters 3, 4 and 5 are devoted to constructing codes with small covering radius. In Chapter 4 we study normality, the amalgamated direct sum construction and various generalizations. Chapter 5 focuses on linear codes. In Chapters 6 and 7, we present nonexistence results for nonlinear and linear codes, and show how to improve on

the sphere-covering bound. In Chapter 8 bounds are derived on the maximum possible covering radius of a code with a given length, cardinality and minimum or dual distance. In the next two chapters we study the covering radius of certain families of codes including the Reed-Muller and BCH codes. In Chapter 11 we give a thorough account of perfect codes. Chapter 12 is devoted to asymptotical covering radius problems. The next two chapters discuss natural generalizations of the covering radius problem, like weighted coverings, multiple coverings and multiple coverings of deep holes. Chapter 15 deals with a more recreational application, namely, how to use covering codes in connection with football pools. Chapter 16 studies partitions of the binary space into tiles, i.e., cosets of a given set. In the next chapter, we study a general model of constrained memories; it turns out to rely on the worst-case behaviour of the covering radius of shortened codes. In Chapter 18 we explore the connections between graphs, groups and codes and how specific techniques pertaining to these three areas are intertwined. Chapter 19 is devoted to variations on the theme of perfect coverings by spheres, namely coverings by unions of shells, by spheres of two or more radii, or by spheres all of different radii. In Chapter 20 we study various complexity issues related to the field.

We are greatly indebted to Noga Alon, Volodya Blinovskii, Sasha Davydov, Tuvi Etzion, Peter Frankl, Philippe Godlewski, Laurent Habsieger, Heikki Hämäläinen, Juha Honkala, Olivier Hudry, Osnat Keren, Ilia Krasikov, Tero Laihonen, Françoise Levy-dit-Vehel, Skip Mattson, Patric Östergård, Arto Salomaa, Juriaan Simonis, Jakov Snyders, Patrick Solé, Aimo Tietäväinen, Alex Vardy, Gilles Zémor and Victor Zinoviev for their comments and inspiring discussions.

We gratefully acknowledge the assistance of Gloria Garcia, Titia Kraaij, Manuel Moreni, Michelle Nahum and Arjen Sevenster.

# Contents

<b>Preface</b>	<b>vii</b>
<b>Contents</b>	<b>ix</b>
<b>List of Symbols</b>	<b>xv</b>
<b>List of Tables</b>	<b>xxi</b>
<b>1 Introduction</b>	<b>1</b>
1.1 Covering problems . . . . .	2
1.2 Applications . . . . .	10
<b>2 Basic facts</b>	<b>15</b>
2.1 Codes . . . . .	15
2.2 The MacWilliams identities . . . . .	24
2.3 Krawtchouk polynomials . . . . .	27
2.4 Hamming spheres . . . . .	32
2.5 Finite fields . . . . .	40
2.6 Families of error-correcting codes . . . . .	45
2.7 Designs, constant weight codes, graphs . . . . .	52
2.8 Notes . . . . .	57
<b>3 Constructions</b>	<b>61</b>
3.1 Puncturing and adding a parity check bit . . . . .	62
3.2 Direct sum . . . . .	63
3.3 Piecewise constant codes . . . . .	64
3.4 Variations on the $(u, u + v)$ construction . . . . .	66
3.5 Matrix construction . . . . .	70
3.6 Cascading . . . . .	72
3.7 Optimal short nonbinary codes . . . . .	73
3.8 Simulated annealing and local search . . . . .	79
3.9 Notes . . . . .	80

<b>4 Normality</b>	<b>85</b>
4.1 Amalgamated direct sum . . . . .	85
4.2 Normality of binary linear codes . . . . .	94
4.3 Abnormal binary nonlinear codes . . . . .	102
4.4 Normality of binary nonlinear codes . . . . .	106
4.5 Blockwise direct sum . . . . .	110
4.6 Notes . . . . .	114
<b>5 Linear constructions</b>	<b>119</b>
5.1 Basic facts about linear covering codes . . . . .	120
5.2 The case $R = 1$ ; examples of small codes . . . . .	122
5.3 Saving more than one coordinate . . . . .	127
5.4 Davydov's basic construction . . . . .	129
5.5 Notes . . . . .	143
<b>6 Lower bounds</b>	<b>145</b>
6.1 Bounds for the cardinality of the union of $K$ spheres . . . . .	146
6.2 Balanced codes . . . . .	149
6.3 Excess bounds for codes with covering radius one . . . . .	151
6.4 Excess bounds for codes with arbitrary covering radius . . . . .	156
6.5 The method of linear inequalities . . . . .	158
6.6 Table on $K(n, R)$ . . . . .	165
6.7 Lower bounds for nonbinary codes . . . . .	170
6.8 Notes . . . . .	177
<b>7 Lower bounds for linear codes</b>	<b>181</b>
7.1 Excess bounds for linear codes . . . . .	181
7.2 Linear codes with covering radius two and three . . . . .	184
7.3 Tables for linear codes . . . . .	191
7.4 Notes . . . . .	213
<b>8 Upper bounds</b>	<b>215</b>
8.1 Codes with given size and distance . . . . .	216
8.2 Covering radii of subcodes . . . . .	222
8.3 Covering radius and dual distance . . . . .	226
8.4 Notes . . . . .	235
<b>9 Reed-Muller codes</b>	<b>237</b>
9.1 Definitions and properties . . . . .	238
9.2 First order Reed-Muller codes . . . . .	241
9.3 Reed-Muller codes of order 2 and $m - 3$ . . . . .	247
9.4 Covering radius of Reed-Muller codes of arbitrary order . . . . .	251
9.5 Notes . . . . .	258

<b>10 Algebraic codes</b>	<b>261</b>
10.1 BCH codes: definitions and properties . . . . .	262
10.2 2- and 3-error-correcting BCH codes . . . . .	266
10.3 Long BCH codes . . . . .	269
10.4 Normality of BCH codes . . . . .	277
10.5 Other algebraic codes . . . . .	279
10.6 Notes . . . . .	281
<b>11 Perfect codes</b>	<b>285</b>
11.1 Perfect linear codes over $\mathbb{F}_q$ . . . . .	286
11.2 A nonexistence result . . . . .	290
11.3 Enumeration of perfect binary codes . . . . .	296
11.4 Enumeration of perfect codes over $\mathbb{F}_q$ . . . . .	307
11.5 Mixed codes . . . . .	310
11.6 Generalizations of perfect codes . . . . .	312
11.7 Notes . . . . .	314
<b>12 Asymptotic bounds</b>	<b>319</b>
12.1 Covering radius of unrestricted codes . . . . .	320
12.2 Greedy algorithm and good coverings . . . . .	322
12.3 Covering radius of linear codes . . . . .	324
12.4 Density of coverings . . . . .	328
12.5 Coverings of small size . . . . .	332
12.6 Bounds on the minimum distance . . . . .	338
12.7 Covering radius as a function of dual distance . . . . .	342
12.8 Packing radius <i>vs</i> covering radius . . . . .	346
12.9 Notes . . . . .	351
<b>13 Weighted coverings</b>	<b>355</b>
13.1 Basic notions . . . . .	355
13.2 Lloyd theorem for perfect weighted coverings . . . . .	357
13.3 Perfect weighted coverings with radius one . . . . .	361
13.4 Weighted coverings and nonexistence results . . . . .	365
13.5 Notes . . . . .	368
<b>14 Multiple coverings</b>	<b>371</b>
14.1 Definitions . . . . .	371
14.2 Perfect multiple coverings . . . . .	373
14.3 Normality of multiple coverings . . . . .	378
14.4 Constructions . . . . .	381
14.5 Tables for multiple coverings . . . . .	382
14.6 Multiple coverings of deep holes . . . . .	385
14.7 Notes . . . . .	389

<b>15 Football pools</b>	<b>393</b>
15.1 Constructions for mixed binary/ternary codes . . . . .	394
15.2 Tables for mixed binary/ternary codes . . . . .	397
15.3 On the early history of the ternary Golay code . . . . .	401
15.4 Notes . . . . .	402
<b>16 Tilings</b>	<b>403</b>
16.1 Preliminaries . . . . .	403
16.2 A sufficient condition . . . . .	405
16.3 Small tiles . . . . .	406
16.4 Periodicity of tilings . . . . .	409
16.5 Recursive decomposition of tilings . . . . .	412
16.6 Tilings and perfect binary codes . . . . .	415
16.7 Nonexistence results . . . . .	417
16.8 Notes . . . . .	420
<b>17 Writing on constrained memories</b>	<b>423</b>
17.1 Worst case coverings and WOMs . . . . .	423
17.2 The error case . . . . .	428
17.3 A model for correcting single errors . . . . .	429
17.4 Single-error-correcting WOM-codes . . . . .	430
17.5 Nonlinear WOM-codes . . . . .	433
17.6 Notes . . . . .	436
<b>18 Subset sums and constrained memories</b>	<b>439</b>
18.1 Cayley graphs . . . . .	439
18.2 Subset sums . . . . .	441
18.3 Maximal sum-free sets . . . . .	446
18.4 Constrained memories ( $W^*Ms$ ) . . . . .	448
18.5 Translation-invariant constraints . . . . .	449
18.6 Domatic number and reluctant memories . . . . .	452
18.7 Defective memories . . . . .	455
18.8 The error case . . . . .	456
18.9 Notes . . . . .	456
<b>19 Heterodox coverings</b>	<b>461</b>
19.1 Perfect coverings by $L$ -spheres . . . . .	461
19.2 Perfect coverings by spheres of two radii . . . . .	467
19.3 Coverings by spheres all of different radii . . . . .	470
19.4 Multicovering radius . . . . .	472
19.5 Perfect coverings of a sphere and constant weight coverings . . . . .	473
19.6 Notes . . . . .	475

<i>Contents</i>	xiii
<b>20 Complexity</b>	<b>479</b>
20.1 Basic facts about the polynomial hierarchy	479
20.2 The complexity of computing the covering radius of a binary code	483
20.3 Derandomization	490
20.4 Notes	493
<b>Bibliography</b>	<b>495</b>
<b>Index</b>	<b>537</b>

This Page Intentionally Left Blank

# List of Symbols

$\mathbb{N}$  set of nonnegative integers

$\mathbb{Z}$  set of integers

$\mathbb{Q}$  set of rational numbers

$\mathbb{R}$  set of real numbers

$\mathbb{C}$  set of complex numbers

$S_n$  symmetric group on  $\{1, 2, \dots, n\}$

$\coloneqq$  is equal to, by definition

$\lfloor x \rfloor$  floor function, the largest integer less than or equal to  $x$

$\lceil x \rceil$  ceiling function, the smallest integer greater than or equal to  $x$

$[i, j] = \{\ell \in \mathbb{Z} : i \leq \ell \leq j\}$

$A \subseteq B$  set  $A$  is included in set  $B$

$A \subset B$  set  $A$  is included in set  $B$  and  $A$  cannot be equal to  $B$

$\delta_{ij}$  Kronecker symbol

$\binom{a}{b}$  binomial coefficient

$\mathbb{Z}_q = \{0, 1, \dots, q-1\}$  additive group of integers modulo  $q$

$\mathbb{F} = \mathbb{F}_2 = \{0, 1\}; \mathbb{F}_q$  finite fields

$\mathbb{F}_q^*$  the multiplicative group of  $\mathbb{F}_q$

$\psi_u(x)$  additive character of  $\mathbb{F}_q$

$Q$  arbitrary alphabet of size  $q$

$\mathbf{a} = (a_1, a_2, \dots, a_n) = (a_1 a_2 \dots a_n) = a_1 a_2 \dots a_n$ ,  $\mathbf{b}_i = b_{i,1} \dots b_{i,n}$ ,  $\mathbf{c}, \dots$  vectors (usually  $(0, 1)$ -vectors), generally assumed to be row vectors

$\mathbf{a}^\pm$  the  $(-1, 1)$ -vector obtained from a binary  $(0, 1)$ -vector  $\mathbf{a}$  by changing 0's to 1's and 1's to  $-1$ 's

$\bar{\mathbf{a}}$  the complement of  $\mathbf{a}$ , i.e., the vector obtained from  $\mathbf{a}$  by changing 0's to 1's and 1's to 0's

$\mathbf{A} = (a_{i,j}), \mathbf{B}, \mathbf{C}, \dots$  matrices

$\mathbf{A}^T$  the transpose of matrix  $\mathbf{A}$

$\mathbf{1}, \mathbf{0}$  all-1 or all-0 row, column or matrix (of size determined by the context)

$\mathbf{1}^n, \mathbf{0}^n$  all-1 or all-0 vector of length  $n$

$\mathbf{1}^{n \times m}, \mathbf{0}^{n \times m}$  all-1 or all-0 matrix of size  $n \times m$

$\mathbf{I}$  identity matrix

$\mathbf{I}_n$  identity matrix of size  $n \times n$

$(\mathbf{x}|\mathbf{y})$  or  $(\mathbf{x}, \mathbf{y})$  concatenation of  $\mathbf{x}$  and  $\mathbf{y}$

$\langle \mathbf{x}, \mathbf{y} \rangle$  scalar product of  $\mathbf{x}$  and  $\mathbf{y}$

$\mathbf{x} * \mathbf{y}$  componentwise product of  $\mathbf{x}$  and  $\mathbf{y}$

$\text{supp}(\mathbf{x})$  support of  $\mathbf{x}$

$w(\mathbf{x})$  Hamming weight of  $\mathbf{x}$

$\mathbf{e}_i$  binary vector with support equal to  $\{i\}$

$\pi(\mathbf{x})$  parity check of  $\mathbf{x}$

$d(\mathbf{x}, \mathbf{y})$  Hamming distance between  $\mathbf{x}$  and  $\mathbf{y}$

$B_i(\mathbf{x})$  Hamming sphere (or ball) of radius  $i$  centred at  $\mathbf{x}$ ;  $B_i^n(\mathbf{x})$  may be used when it is important to have  $n$  specified

$B_i(X) = \cup_{\mathbf{x} \in X} B_i(\mathbf{x})$

$V_q(n, i)$  size of the Hamming sphere of radius  $i$ ; subscript  $q$  may be dropped in the binary case

$S_i(\mathbf{x})$  set of vectors at distance  $i$  from  $\mathbf{x}$

$S_i$  set of vectors of weight  $i$

- $\mathbb{E}^n$  set of binary even weight vectors of length  $n$   
 $\mathcal{A}_i = \mathcal{A}_i(C)$  number of words of weight  $i$  in code  $C$   
 $\mathcal{A}_i(\mathbf{x}) = |\{\mathbf{c} \in C : d(\mathbf{c}, \mathbf{x}) = i\}|$   
 $\mathcal{B}_i = \mathcal{B}_i(C)$  distance distribution of  $C$   
 $C_a^{(i)}$  subcode  $\{\mathbf{c} \in C : c_i = a\}$   
 $\langle A \rangle$  vector space generated by  $A$   
 $k = k(C) = \dim(C)$  dimension of a linear code  $C$   
 $R = R(C)$  covering radius of  $C$   
 $d = d(C)$  minimum distance of  $C$   
 $d^\perp = d^\perp(C)$  minimum distance of  $C^\perp$ , the dual code of a linear code  $C$   
 $e = e(C) = \lfloor (d(C) - 1)/2 \rfloor$  error-correcting capability of  $C$   
 $\mu(C)$  density of  $C$   
 $\mathbf{G} = \mathbf{G}(C)$  generator matrix of a linear code  $C$   
 $\mathbf{H} = \mathbf{H}(C)$  parity check matrix of a linear code  $C$   
 $\kappa = \kappa(C) = \log_2 |C|/n = k(C)/n$  information rate of  $C$   
 $\delta = \delta(C) = d(C)/n$  normalized distance of  $C$   
 $\delta^\perp = \delta^\perp(C) = d^\perp(C)/n$  normalized dual distance of  $C$   
 $\rho = \rho(C) = R(C)/n$  normalized covering radius of  $C$   
 $[n, k, d]R$  binary linear code of length  $n$ , dimension  $k$ , minimum distance  $d$ , covering radius  $R$ ;  $d$  or  $R$  may be dropped when irrelevant  
 $(n, K, d)R$  binary (not necessarily linear) code of length  $n$ , cardinality  $K$ , minimum distance  $d$ , covering radius  $R$ ;  $d$  or  $R$  may be dropped when irrelevant  
 $t[n, k]$  smallest covering radius among all  $[n, k]$  codes  
 $t(n, K)$  smallest covering radius among all  $(n, K)$  codes  
 $k[n, R]$  smallest dimension of a binary linear code with length  $n$  and covering radius  $R$

- $K(n, R)$  smallest cardinality of a binary code with length  $n$  and covering radius  $R$   
 $\ell(m, R)$  smallest length of a binary linear code of covering radius  $R$  and codimension (or redundancy)  $m$   
 $a[n, d]$  maximal dimension of a binary linear code of length  $n$  and minimum distance  $d$   
 $A(n, d)$  maximal cardinality of a binary code of length  $n$  and minimum distance  $d$   
 $n[k, d]$  smallest length of a binary linear code of dimension  $k$  and minimum distance  $d$   
 $g[k, d]$  Griesmer bound on  $n[k, d]$   
 $[n, k, d]_q R, (n, K, d)_q R, t_q[n, k], t_q(n, K), k_q[n, R], K_q(n, R), \ell_q(m, R), a_q[n, d], A_q(n, d), n_q[k, d]$  and  $g_q[k, d]$  are the corresponding notations for the  $q$ -ary case  
 $F(v, k)$  minimal cardinality of a  $2$ -( $v, k, 1$ ) covering design  
 $C^\circ$  code  $C$  shortened in one coordinate  
 $C^*$  code  $C$  punctured in one coordinate  
 $\widehat{C}$  code  $C$  extended  
 $A \oplus B$  direct sum of codes  $A$  and  $B$   
 $A \dot{\oplus} B$  amalgamated direct sum of  $A$  and  $B$   
 $\mathcal{BCH}(e, m)$  primitive BCH code of length  $2^m - 1$  and designed distance  $2e + 1$   
 $\mathcal{BCH}_h(e, m)$  nonprimitive BCH code of length  $(2^m - 1)/h$  and designed distance  $2e + 1$   
 $\mathcal{GOP}(L, g)$  Goppa code with defining set  $L$  and polynomial  $g$   
 $\mathcal{HAD}_n$  Hadamard code of length  $n$   
 $\mathcal{H}_m$  Hamming code of length  $2^m - 1$   
 $\mathcal{P}_m$  Preparata code of length  $2^m$ ,  $m$  even  
 $\mathcal{QR}(p)$  quadratic residue code of length  $p$   
 $\mathcal{RM}(r, m)$  Reed-Muller code of order  $r$  and length  $2^m$   
 $\mathcal{RS}(k, q)$   $q$ -ary Reed-Solomon code of length  $q - 1$  and dimension  $k$

$\mathcal{SIM}_m$  simplex code of length  $2^m - 1$

$\Gamma = (V, E)$  graph with vertex set  $V$  and edge set  $E$

$Tr(x)$  trace function

$P_j^n(x)$  Krawtchouk polynomial; superscript  $n$  may be omitted

$L_j^n(x)$  Lloyd polynomial; superscript  $n$  may be omitted

$H(x) = -x \log_2 x - (1-x) \log_2(1-x)$  binary entropy of  $x$ ,  $0 \leq x \leq 1$

This Page Intentionally Left Blank

# List of Tables

2.1	The field of 16 elements.	43
2.2	Upper and lower bounds on $A(n, d)$ .	53
2.3	Upper and lower bounds on $a[n, d]$ .	54
2.4	Bounds on $F(v, k)$ .	56
6.1	Bounds on $K(n, R)$ .	166
6.2	Bounds on $K_3(n, R)$ .	174
6.3	Bounds on $K_4(n, R)$ .	175
6.4	Bounds on $K_5(n, R)$ .	175
7.1	Bounds on $t[n, k]$ .	193
7.2	Bounds on $\ell(m, R)$ .	202
7.3	Bounds on $\ell(m, R)$ , $R \leq 4$ .	209
7.4	Bounds on $\ell(m, R)$ , $n \leq 24$ .	211
9.1	Bounds on the covering radius of Reed-Muller codes.	252
10.1	Covering radius of binary primitive BCH codes.	269
10.2	Bounds on the covering radius of extremal doubly-even self-dual codes.	281
14.1	Bounds on $K(n, 1, \mu)$ .	383
14.2	Bounds on $K(n, 2, \mu)$ .	383
14.3	Bounds on $K(n, 3, \mu)$ .	384
14.4	Bounds on $K(n, 4, \mu)$ .	384
14.5	Upper bounds on $F(n, r, \mu)$ .	388
15.1	Bounds on $K_{3,2}(t, b, R)$ .	398
17.1	Parameters of a few WOM-codes, linear or not.	436
18.1	Values of $s_G(R)$ .	457
20.1	Achievable sizes for $t$ -independent families $\mathcal{F}$ : $ \mathcal{F}  \geq 2^{c_t n}$ .	493

This Page Intentionally Left Blank

# Chapter 1

## Introduction

Covering and packing are traditional issues that have attracted the attention of mathematicians and engineers.

A natural packing problem in the conventional  $n$ -dimensional euclidean space is to ask for the maximal number of identical non-intersecting spheres in a large volume. This has a number of interesting connections to different areas of mathematics like geometry, group theory, number theory and quadratic forms. At the same time it has important engineering applications like constructing signals for communication systems.

The covering problem in the euclidean space asks for the minimal number of identical spheres needed to cover a large volume. For example, in a mobile radio network, minimizing the required number of base stations whose range is given, typically 10 km, is a covering problem in the two-dimensional euclidean space.

The covering and packing problems in the euclidean space have been extensively studied, see, e.g., Conway and Sloane [175], Fejes Tóth [234] and Rogers [560].

The same issues can be considered in the  $n$ -dimensional *Hamming space* consisting of binary words, i.e., vectors whose  $n$  components are zeros and ones. The elements of the Hamming space are also called *points*. In contrast to the euclidean space, the number of points in this space is finite. An arbitrary nonempty subset of the Hamming space is called a *code*, and its elements are called *codewords*. The (*Hamming*) *distance* between two vectors is the number of coordinates (components) in which the vectors differ. The *minimum distance* of a code is the smallest of the pairwise distances between the codewords. In a natural way the *sphere* of radius  $r$  consists of all the vectors within distance  $r$  from the centre. For example, the sphere of radius one with centre 01011 in the five-dimensional Hamming space consists of the vectors 01011, 11011, 00011, 01111, 01001, 01010.

Now we can formulate the following two questions.

- **Packing problem:** Given  $n$  and  $r$ , what is the maximal number of non-intersecting Hamming spheres of radius  $r$  that can be placed in the  $n$ -dimensional Hamming space?
- **Covering problem:** Given  $n$  and  $r$ , what is the smallest number of Hamming spheres of radius  $r$  that can be placed in such a way that every vector in the space is contained in at least one of them?

The packing problem is fundamental in *error correction*. The centres of such a packing are at least distance  $2r + 1$  apart from each other and constitute the code, i.e., the set of possible messages. Assume that one of these messages is transmitted and that at most  $r$  coordinates are corrupted during the transmission. To decode, i.e., to decide which of the messages was actually sent, we compute the Hamming distances between the received vector and all the centres. Since at most  $r$  errors occurred, the transmitted word is the nearest centre, and we can correct the errors. The question of constructing good packings has been widely studied in the last five decades, see, e.g., Berlekamp [68], Blake and Mullin [83], van Lint [438], MacWilliams and Sloane [464], Peterson and Weldon [534], Pless [542] and van Tilborg [653].

In this monograph we deal with the covering problem in the Hamming space. That is, we search for a code such that the spheres of radius  $r$  centred at the codewords cover the whole  $n$ -dimensional Hamming space. Such a set is called a *covering code* or simply a *covering* in what follows. It is clearly a covering also for all radii greater than  $r$ . For any code we can determine the smallest integer  $r$  such that the spheres of radius  $r$  centred at the codewords cover the whole space. This integer is called the *covering radius*.

We now informally discuss several examples illustrating some of the basic problems in this area.

## 1.1 Covering problems

**Example 1.1.1** Let  $n = 5$  and  $r = 1$ . What is the smallest number of spheres of radius one needed to cover all the vectors in the five-dimensional Hamming space?

To describe such a covering we give a list of the centres: for example,

$$\begin{array}{cccccc}
 0 & 0 & 0 & 0 & 0 \\
 0 & 1 & 0 & 0 & 0 \\
 1 & 0 & 0 & 0 & 0 \\
 1 & 1 & 0 & 0 & 0 \\
 0 & 0 & 1 & 1 & 1 \\
 0 & 1 & 1 & 1 & 1 \\
 1 & 0 & 1 & 1 & 1 \\
 1 & 1 & 1 & 1 & 1
 \end{array} \tag{1.1.2}$$

This code has a very simple structure. It consists of all the vectors that end with 000 or 111 and obviously enjoys the desired property; assume given an arbitrary vector of length five. If it does not belong to the covering, then the number of 1's in the last three coordinates is one or two; if it is one, changing this single 1 to 0 gives a codeword which has distance one to our vector. If it is two, changing the single 0 to 1 similarly gives a codeword.

In fact, one can manage with the following seven words:

$$\begin{array}{cccccc}
 0 & 0 & 0 & 0 & 0 \\
 0 & 0 & 1 & 1 & 1 \\
 0 & 1 & 1 & 1 & 1 \\
 1 & 0 & 1 & 1 & 1 \\
 1 & 1 & 1 & 0 & 0 \\
 1 & 1 & 0 & 1 & 0 \\
 1 & 1 & 0 & 0 & 1
 \end{array} \tag{1.1.3}$$

Furthermore, this code has a special structure; we say that a vector is of type  $(a, b)$  if the number of ones in the first two positions is  $a$  and the number of ones in the last three positions is  $b$ . Our covering thus consists of all the words of types  $(0, 0), (0, 3), (1, 3), (2, 1)$ . The codeword of type  $(0, 0)$  covers all the vectors of types  $(0, 0), (0, 1), (1, 0)$ , the codeword of type  $(0, 3)$  covers all the vectors of types  $(0, 2), (0, 3), (1, 3)$ , the codewords of type  $(1, 3)$  cover all the vectors of types  $(0, 3), (1, 2), (1, 3), (2, 3)$  and finally the codewords of type  $(2, 1)$  cover all the vectors of types  $(1, 1), (2, 0), (2, 1), (2, 2)$ . Hence all the vectors in the space are covered, the vectors of types  $(0, 3)$  and  $(1, 3)$  in fact twice.

Let us show that seven is the smallest possible size of such a covering. We know that each sphere contains six vectors (the word itself and the five vectors that differ from it in exactly one coordinate). To cover all the  $2^5 = 32$  vectors we therefore need at least  $\lceil 32/6 \rceil = 6$  spheres. This argument establishes the so-called *sphere-covering bound*. To prove that the minimum number of codewords is in fact seven we need to introduce the following simple concepts. The *weight* of a vector is the number of its nonzero coordinates. The number

of words of weight  $i$  in a covering is denoted by  $\mathcal{A}_i$ . The *complement* of a vector is obtained by changing all the 0's to 1's and vice versa.

Assume now that there is a covering with only six words. There are at least ten pairs consisting of a vector and its complement not included in the covering; indeed, there are initially sixteen pairs and each codeword can only belong to one of them. Without loss of generality, assume that neither 00000 nor 11111 belongs to the covering.

In order to cover the vector 00000, we need at least one codeword of weight one, and therefore

$$\mathcal{A}_1 \geq 1. \quad (1.1.4)$$

Consider now how the five vectors of weight one are covered. A codeword of weight one covers only one vector of weight one, namely itself. A codeword of weight two covers two vectors of weight one. Consequently,

$$\mathcal{A}_1 + 2\mathcal{A}_2 \geq 5. \quad (1.1.5)$$

Adding these two inequalities and dividing by two, we get

$$\mathcal{A}_1 + \mathcal{A}_2 \geq 3. \quad (1.1.6)$$

In the same way, considering how the vectors of weight four and five are covered, we obtain the inequalities

$$2\mathcal{A}_3 + \mathcal{A}_4 \geq 5$$

and

$$\mathcal{A}_4 \geq 1,$$

which imply that

$$\mathcal{A}_3 + \mathcal{A}_4 \geq 3.$$

Since  $\mathcal{A}_1 + \mathcal{A}_2 + \mathcal{A}_3 + \mathcal{A}_4 = 6$ , we know that  $\mathcal{A}_1 + \mathcal{A}_2 = 3$  and  $\mathcal{A}_3 + \mathcal{A}_4 = 3$ . Subtracting  $\mathcal{A}_1 + \mathcal{A}_2 = 3$  from (1.1.5), we get  $\mathcal{A}_2 \geq 2$ . Hence  $\mathcal{A}_1 = 1$  and  $\mathcal{A}_2 = 2$ . Furthermore, since all the vectors of weight one are covered by the codewords of weight one and two, without loss of generality these three codewords are

$$\begin{array}{cccccc} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1. \end{array}$$

All the other vectors of weight two except

$$\begin{array}{ccccc} 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 \end{array} \quad (1.1.7)$$

are covered by these three codewords.

By symmetry, the codewords of weight three and four are obtained from the vectors

$$\begin{array}{ccccc} 0 & 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 \end{array}$$

by a suitable permutation of the coordinates. In particular, there is a codeword of weight three that begins with 1, and hence covers at most one of the vectors in (1.1.7). But no word of weight three can cover more than two of the vectors in (1.1.7), a contradiction. Consequently, the smallest possible number of codewords in a covering of the five-dimensional Hamming space using spheres of radius one is seven.

If we instead consider spheres of radius two, then we can clearly choose the two words

$$\begin{array}{ccccc} 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 \end{array}$$

as the centres of the spheres, and this is the smallest possible number.  $\square$

**Example 1.1.8** Consider again the code (1.1.2): it enjoys a property known as *linearity*, namely that the coordinatewise sum (mod 2) of any two codewords also belongs to the code. For instance, the sum of the fourth codeword 11000 and the sixth codeword 01111 gives the seventh codeword 10111. In particular, the all-zero word belongs to every linear code, since it is the sum of any codeword with itself.

Another way of representing such a linear code is by a set of equations on the coordinates. For example, our code is defined by the equations

$$\begin{aligned} x_3 + x_5 &= 0 \pmod{2} \\ x_4 + x_5 &= 0 \pmod{2}. \end{aligned}$$

In the matrix form the corresponding system is  $\mathbf{H}\mathbf{x}^T = \mathbf{0}$ , where  $\mathbf{x} = (x_1, x_2, x_3, x_4, x_5)$ ,  $\mathbf{0} = (0, 0)^T$ , and

$$\mathbf{H} = \begin{pmatrix} 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 \end{pmatrix}$$

is called a *parity check matrix* for the code.

The number of solutions of such a system of equations is always a power of two. Taking into account the sphere-covering bound according to which *any* covering with  $n = 5$  and  $r = 1$  has at least six codewords, we conclude that this code is the smallest among linear codes.

As we have already seen, in this case there exists a better nonlinear code. However, linear codes have a natural simple structure, which is helpful in many situations.

Clearly, the covering radius of this code is one: if it were zero, all the 32 vectors in the space should be codewords.

For example, the linear code

$$\begin{array}{cccccc}
 0 & 0 & 0 & 0 & 0 \\
 0 & 0 & 0 & 1 & 1 \\
 0 & 1 & 1 & 0 & 0 \\
 0 & 1 & 1 & 1 & 1 \\
 1 & 0 & 1 & 0 & 0 \\
 1 & 0 & 1 & 1 & 1 \\
 1 & 1 & 0 & 0 & 0 \\
 1 & 1 & 0 & 1 & 1
 \end{array}$$

consisting of all the words having an even number of 1's both in the first three coordinates and the last two coordinates has covering radius two. To see that the covering radius is *at most* two, notice that a vector that begins with 0 has distance at most two to 00000 or 01111, and a vector that begins with 1 has distance at most two to 10100 or 11011. To see that the covering radius is *at least* two, notice that every word having an odd number of 1's both in the first three coordinates and the last two coordinates clearly has distance at least two to all the codewords.

In fact, the maximal possible covering radius for a linear code of length five with eight codewords is two. Indeed, assume the existence of a linear code with covering radius three. As before, we may assume that 11100 has distance three to the code. If any two distinct codewords coincide in the last two coordinates, then their sum is nonzero and ends with two 0's, and hence its distance to 11100 is at most two. Therefore a linear code with covering radius three can have at most four codewords. In the same way we see that the covering radius of a linear code of length five with eight codewords cannot be four or five, either.  $\square$

**Example 1.1.9** Consider again the code (1.1.3) consisting of the seven words

$$\begin{array}{cccccc}
 0 & 0 & 0 & 0 & 0 \\
 0 & 0 & 1 & 1 & 1 \\
 0 & 1 & 1 & 1 & 1 \\
 \\
 1 & 0 & 1 & 1 & 1 \\
 1 & 1 & 1 & 0 & 0 \\
 1 & 1 & 0 & 1 & 0 \\
 1 & 1 & 0 & 0 & 1,
 \end{array}$$

where we have partitioned the code into two subcodes according to whether the first coordinate is 0 or 1. The distance between a vector and a subcode is defined to be the smallest of the distances between the vector and the codewords in the subcode. A routine verification shows that the sum of the distances from any given vector to the first and second subcodes is at most three.

This property is called *normality*. More precisely, we say that the code is normal with respect to the first coordinate. Notice that since the sum of the distances is at most three, one of the distances is at most one. Hence this property implies that we have a covering with  $r = 1$ .

We now construct a new code of length seven by repeating the first coordinate twice, which gives us the new codewords

$$\begin{array}{ccccccc}
 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
 0 & 0 & 0 & 0 & 1 & 1 & 1 \\
 0 & 0 & 0 & 1 & 1 & 1 & 1 \\
 \\ 
 1 & 1 & 1 & 0 & 1 & 1 & 1 \\
 1 & 1 & 1 & 1 & 1 & 0 & 0 \\
 1 & 1 & 1 & 1 & 0 & 1 & 0 \\
 1 & 1 & 1 & 1 & 0 & 0 & 1.
 \end{array}$$

We show that this code is a covering with  $r = 2$ .

Divide this new code into two corresponding subcodes. Consider any given vector of length seven and calculate its distances to the first subcode and to the second subcode. We claim that the sum of these distances is at most five. Whatever the first coordinate is, it contributes one to the sum, since it agrees with all the words in one of the subcodes and disagrees with all the words in the other subcode. The same applies to the second coordinate. Therefore we only need to consider the last five coordinates, whose contribution to the sum is known to be three or less. Hence the sum is at most  $1 + 1 + 3$  and one of the distances is at most two.  $\square$

**Example 1.1.10** As we have seen, it is possible to cover the five-dimensional Hamming space using seven spheres of radius one. A natural generalization of this problem is to ask how many are needed to cover at least twice each vector in the space.

If we change the last coordinate from 0 to 1 or from 1 to 0 in each of the seven words in (1.1.3), we obtain another covering. Its words together with the original ones clearly form a two-fold covering with 14 codewords.

However, we can achieve the same goal with the 12 codewords

$$\begin{array}{cccccc}
 0 & 0 & 0 & 0 & 0 \\
 1 & 0 & 1 & 0 & 1 \\
 1 & 1 & 0 & 1 & 0 \\
 0 & 1 & 1 & 1 & 1 \\
 0 & 0 & 0 & 0 & 1 \\
 1 & 0 & 1 & 0 & 0 \\
 1 & 1 & 0 & 1 & 1 \\
 0 & 1 & 1 & 1 & 0 \\
 0 & 0 & 0 & 1 & 1 \\
 1 & 0 & 1 & 1 & 0 \\
 1 & 1 & 0 & 0 & 1 \\
 0 & 1 & 1 & 0 & 0.
 \end{array}$$

In fact, 12 is the smallest number of codewords in such a two-fold covering; by the sphere-covering argument, at least  $\lceil 2 \cdot 32/6 \rceil = 11$  codewords are required. Assume there is such a covering with only 11 words. Without loss of generality, at most five of them begin with 0. Consider how the 16 vectors in the Hamming space beginning with 0 are covered by the codewords. Notice that a codeword beginning with 0 covers exactly five of them, namely the codeword itself and the four vectors obtained by changing one of the last four coordinates. A codeword that begins with 1 only covers one such vector, the one obtained by changing the first coordinate from 1 to 0. But this means that all the codewords together can cover at most  $5 \cdot 5 + 6 \cdot 1 = 31 < 2 \cdot 16$ , a contradiction.  $\square$

**Example 1.1.11** The following *Hamming code* of length seven and size 16 is truly exceptional: it turns out that the spheres of radius one centred at the codewords not only cover the whole space, but are also pairwise disjoint. Such a code is called *perfect*. It is linear, with parity check matrix

$$\mathbf{H} = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}.$$

Notice that all the nonzero vectors of length three appear as columns in  $\mathbf{H}$ . Let  $\mathbf{x}$  be any vector of length seven. If  $\mathbf{H}\mathbf{x}^T = \mathbf{0}$ , then  $\mathbf{x}$  itself is a codeword. Otherwise,  $\mathbf{H}\mathbf{x}^T$  is one of the columns of  $\mathbf{H}$ , and changing the corresponding coordinate in  $\mathbf{x}$  yields a codeword at distance one to  $\mathbf{x}$ . For example, if  $\mathbf{x} = 1011000$ , then  $\mathbf{H}\mathbf{x}^T = (1, 1, 0)^T$  and changing the sixth coordinate gives the codeword 1011010. Hence the covering radius equals one.

Each of the 16 codewords covers eight of the 128 vectors in the whole space. Because the codewords together cover the whole space, every vector in

the space is covered by exactly one codeword, and the spheres of radius one centred at the codewords are disjoint.  $\square$

Most codes have been designed for error correction. In this case, the minimum distance, measuring the number of correctable errors, is of primary interest.

Yet, the covering radius is also an important parameter of error-correcting codes for several reasons. First of all, if it is less than the minimum distance, then no vector in the Hamming space can be added to the code without decreasing its minimum distance. Such codes are called *maximal* and are clearly of interest for error correction. Second, if we decode the received vector to the nearest codeword (maximum-likelihood decoding), then the covering radius measures the largest number of errors in any correctable error pattern. Indeed, if the number of errors exceeds the covering radius, there is another codeword closer to the received vector than the transmitted one, hence leading to incorrect decoding.

Now, having gone through a number of simple examples, we state the general problems studied in this monograph.

- Given the length and covering radius, how to construct small coverings or lowerbound their sizes?
- Which codes are normal? What are possible extensions of the notion of normality and how can they be applied to construct good coverings?
- What is the maximal covering radius of a linear code with given length and size?
- What connections are there between covering radius and minimum distance? Is it possible to construct codes that at the same time have small covering radius and large minimum distance?
- What is the covering radius of the well-known families of error-correcting codes?
- What is the asymptotic behaviour of the parameters of the best coverings?
- What are the parameters of the best multiple coverings? Are there other natural generalizations of the usual coverings?

## 1.2 Applications

Covering codes have a number of applications and interrelations with other areas of mathematics. We illustrate this with a series of examples giving the crucial ideas of such applications.

**Example 1.2.1 Compression with distortion:** Assume some information has been encoded into a long binary vector. We divide it into parts consisting of seven bits. Our aim is to compress each of these 7-bit vectors to 4 bits, thus achieving a compression ratio of  $4/7$ . Does this mean that we lose  $3/7$  of the information? The answer is no. Use the Hamming code of length 7 discussed in Example 1.1.11; index the codewords with the 4-bit vectors, then replace each 7-bit vector with the index of the closest codeword, and afterwards retrieve the original vector with at most one error, since the Hamming code has covering radius one. Thus, at most  $1/7$  of the original long vector is distorted. In general, using a covering of the  $n$ -dimensional Hamming space with  $2^k$  spheres of radius  $r$  gives a compression ratio  $k/n$  along with a distortion rate at most  $r/n$ .  $\square$

**Example 1.2.2 Data compression:** Assume given a set of sixteen different 7-bit vectors — their order being irrelevant — that we want to compress without distortion. With no compression we can simply store the information using  $16 \cdot 7 = 112$  bits. However, there are better strategies.

Since the number of such sets is  $\binom{2^7}{16}$ , indexing them all and storing the index uses  $\lceil \log_2 \binom{2^7}{16} \rceil = 67$  bits. Storing in advance all the possible sets and their indices is impractical because of space limitations. However, the previous argument demonstrates that every compression method requires at least 67 bits.

We now give another compression algorithm that uses the Hamming code. First, index the 16 codewords of the Hamming code; to each codeword attach a list of all the 7-bit vectors among the sixteen to which the codeword is the nearest one. Some of these lists may of course be empty. Consider now a fixed codeword and the list attached to it. Since the covering radius of the Hamming code is one, every 7-bit vector occurring in the list attached to a codeword differs from it in at most one position. We may therefore represent each 7-bit vector by writing the number of the coordinate in which it differs from the codeword (or 0, if they agree). This representation requires three bits. We now attach the prefix 0 to each of these 3-bit vectors and the additional prefix 1 to the whole list. For example, assume that the list of 7-bit vectors attached to the codeword 1110000 is 1100000, 1110001, 1110000. We compress this list to 1 0 011 0 111 0 000. If the list happens to be empty, this compression simply

yields the bit 1. We perform the same operation with each list and store the outcomes consecutively.

The original set of vectors can now be retrieved in the following way: we read the stored information from the beginning. We know that first appears the information about the list attached to the first codeword. If the second bit is 1, the list is empty. If the second bit is 0, the following three bits contain the location of the coordinate in which one of our original 7-bit vectors differs from the codeword, and we retrieve it. If the next bit is 1, we have reached the end of the list attached to the first codeword. Otherwise, we continue retrieving our 7-bit vectors until the 1 is encountered and we move to the next list. Evidently, we can drop the very first bit, so the algorithm uses 79 bits.

One can do better by using long covering codes and even obtain compression rates tending to the optimal.  $\square$

**Example 1.2.3 Decoding of errors and erasures:** Let  $C$  be a code of length  $n$  with minimum distance  $d = 2e + 1$ . Then we can in principle use  $C$  to correct up to  $e$  errors. However, assume that we have an efficient algorithm for correcting up to  $e' \leq e$  errors. The algorithm gets as an input any binary vector of length  $n$ , and outputs the unique codeword within Hamming distance  $e'$  or tells us that no such codeword exists.

We wish to use the algorithm for correcting  $t \leq e'$  errors and  $f$  erasures, where  $2t + f < d$ . In other words, we should be able to retrieve the transmitted codeword if during the transmission at most  $f$  of the 0's and 1's in the word are erased, i.e., replaced by \* indicating that we do not know if the symbol is 0 or 1, and in at most  $t$  places 0 is replaced by 1 or 1 is replaced by 0.

For notational convenience, let us assume that the erasures occur among the first  $f$  coordinates and that  $\mathbf{v}$  is the binary vector formed by the last  $n - f$  coordinates in the received vector. Because  $d - f > 2t$ , we know that there is a unique codeword  $\mathbf{c} = (\mathbf{c}_0, \mathbf{c}_1)$ , where  $\mathbf{c}_0$  is a binary vector of length  $f$ , such that  $\mathbf{c}_1$  and  $\mathbf{v}$  disagree in at most  $t$  places. Trivially we find  $\mathbf{c}$  by running the algorithm with the input  $(\mathbf{a}, \mathbf{v})$  for all the  $2^f$  possible choices of  $\mathbf{a}$ . However, it is sufficient to let  $\mathbf{a}$  go through the sphere centres in a covering of the  $f$ -dimensional Hamming space by spheres of radius  $e' - t$ . Indeed, one of the centres, say  $\mathbf{b}$ , is within Hamming distance  $e' - t$  from  $\mathbf{c}_0$ , and therefore  $(\mathbf{b}, \mathbf{v})$  is within Hamming distance  $(e' - t) + t = e'$  from  $\mathbf{c}$ . With the input  $(\mathbf{b}, \mathbf{v})$ , the algorithm outputs  $\mathbf{c}$ .

Notice that in the case of pure erasures — when  $t = 0$  — and  $e = e'$ , the algorithm is run twice, the related covering being a repetition code.  $\square$

**Example 1.2.4 Broadcasting in interconnection networks:** Hypercube architecture is one of the common structures for connecting several processors in a network. Suppose we have 32 processors. Assign each of them a 5-bit index and connect two processors if and only if the Hamming distance between their indices is one.

Consider the following model of information transmission in the network. At every time unit, each processor may receive and send. Having received a piece of information, a processor always retransmits it to all its neighbours during the next time unit. In the beginning, a particular message is transmitted to one or more of the processors in the network. The question is: how many time units will elapse before the message has reached all the nodes of the hypercube? If the information is originally transmitted to only one of the processors, say with index 00000, then it clearly takes five time units to reach 11111. To update all processors in one time unit, one needs to send the information directly to all of them and pay for 32 connections. A trade-off can be achieved by allowing one time unit delay. In this case, send the information to the seven processors listed in (1.1.3), thereby using only seven connections. Since the words in (1.1.3) constitute a covering with  $r = 1$ , each node will then be reached within one time unit.  $\square$

**Example 1.2.5 Football pools:** Assume we wish to place bets on the winners of  $n$  football matches. A *bet* is a prediction of the winners of these  $n$  matches — where no tie is allowed — i.e., a binary word of length  $n$ . What is the smallest number of bets needed to guarantee that at least one of them has at most  $r$  incorrect predictions? Clearly such a collection of bets is a covering of the  $n$ -dimensional Hamming space with spheres of radius  $r$ .

Accepting ties as possible outcomes leads to an analogous problem with ternary words.  $\square$

**Example 1.2.6 Write-once memories:** Consider a storage medium  $n$ -WOM consisting of  $n$  binary positions called *wits* initially set at 0. A wit can be irreversibly overwritten with a 1, e.g., by a laser beam in some digital optical disks. Covering codes can be employed to efficiently reuse a WOM, as we now show on a simple but striking example: *two bits may be written twice on a 3-WOM*.

Consider the repetition code  $C = \{000, 111\}$ . Its parity check matrix is

$$\mathbf{H} = \begin{pmatrix} 1 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix}.$$

Represent the two bits to be written on the WOM as column vectors  $\mathbf{s}_i$ , indexed by the columns of  $\mathbf{H}$ . Thus  $\mathbf{s}_0 = (00)^T, \mathbf{s}_1 = (11)^T, \mathbf{s}_2 = (01)^T, \mathbf{s}_3 =$

$(10)^T$ . Now, to write  $s_i, i \neq 0$ , burn position  $i$  on the WOM. To write  $s_0$ , do nothing. Notice that the maximal number of burnt wits in the first step is 1 and equals the covering radius of the code  $C$ . Let us show on an example how to reuse the WOM for a second writing. Suppose that, after the first writing, the state of the WOM is  $y_1 = (100)$ , representing  $s_1 = (11)^T = \mathbf{H}y_1^T$ . To encode, say,  $s_2 = (10)^T$ , we need to write  $s'_2 = s_1 + s_2 = (01)^T$ , using the shortened matrix

$$\mathbf{H}' = \begin{pmatrix} * & 0 & 1 \\ * & 1 & 0 \end{pmatrix}.$$

Remember that the rules of the game forbid us from reusing the first position and therefore we may only access a shortened version of  $\mathbf{H}$ .

Now,  $s'_2$  is the second column of  $\mathbf{H}'$ , so we burn position 2 of the WOM, getting  $y_2 = (110)$ , representing  $\mathbf{H}y_2^T = s_2$ .

In general, in order to estimate the number of wits to be burnt in each step we need to know the covering radius of a given code  $C$  and all codes obtained by shortening it.  $\square$

**Example 1.2.7 Berlekamp-Gale game:** The game is played on a  $10 \times 10$  array of light bulbs, each of them being initially on or off. The initial state is decided by the first player. The second player has control over ten row and ten column switches. If a switch is thrown, all the lights in the corresponding row or column that are on turn off and the ones that are off turn on. The aim of the second player is to throw the switches so as to minimize the number of lights on. Correspondingly the first player sets the initial state to prevent the second player from achieving too good a result.

Represent a state by a binary vector of size 100, with ones corresponding to the lights on and zeros to the lights off. If the initial state is zero (all lights off), then all possible states constitute a linear code of length 100 with  $2^{10}$  words. If the initial state is not zero, then we get a coset of the linear code, i.e., the set consisting of the codewords shifted by a fixed binary vector. Clearly a vector of minimal weight in such a coset gives a minimal configuration of lights. Let us call the weight of this vector the coset weight. Now the problem reduces to finding the maximum over all cosets of the coset weights, i.e., the covering radius of the considered linear code.  $\square$

**Example 1.2.8 Speech coding:** The following problem arises in connection with efficient speech coding. Let  $\mathbf{x} = (x_1, \dots, x_n)$  be a point on the surface of an euclidean sphere of radius one, i.e.,  $x_1^2 + \dots + x_n^2 = 1$ . We pick  $K$  codewords that are in a sense uniformly distributed on the surface, and represent any  $\mathbf{x}$  by the index of the closest codeword (in euclidean distance). One thus uses  $\log_2 K$  bits to store (with some distortion) the coordinates of an arbitrary

point on the sphere. If  $K$  does not exceed  $2^n$ , then a natural method of construction is to pick a good covering code  $C$  of size  $K$ , and then substitute every word  $(c_1, \dots, c_n)$  by  $((-1)^{c_1}/\sqrt{n}, \dots, (-1)^{c_n}/\sqrt{n})$ .  $\square$

**Example 1.2.9 Cellular telecommunications:** The following problem originates in cellular telecommunication technology. In order to provide mobile telephone service to a given area using a limited band in the radio spectrum, the strategy is to dispatch the set of users in the area into cells. When a call is placed from a user, it is allocated a radio frequency. The same frequency may be used simultaneously by another user, provided the distance between the cells they originate from exceeds some threshold, to avoid interferences. This leads to the following formalization; see Baldi [42]. Let  $\Gamma = (V, E)$  be a graph (vertices in  $V$  corresponding to cells and edges in  $E$  connecting neighbouring cells) with the metric induced by the shortest path between vertices. Let  $f$  be the call function, i.e.,  $f(x)$  is the number of (active) users in cell  $x$ . The *call colouring problem* on  $\Gamma$  consists in assigning  $f(x)$  colours (frequencies) to each vertex  $x$  in  $V$  with the constraint that, within every sphere of a given radius  $r$  centred at  $x$  (for the graph distance), no other point has a colour in common with  $x$ . Of course, for economical... and mathematical reasons, the number of colours should be minimized. The cells of a given colour clearly make for a code of minimum distance  $r + 1$  (i.e., a *packing*). In the case when  $f$  is identically equal to one, i.e., when exactly one user per cell is active, these packings are disjoint. The problem is then to find a minimum — perfect — covering by packings.  $\square$

**Example 1.2.10 Subset sums and Cayley graphs:** Let a code have parity check matrix  $\mathbf{H}$  with columns  $\mathbf{h}_1, \dots, \mathbf{h}_n$ , where each  $\mathbf{h}_i$  is a binary  $m$ -tuple. As it will be shown, the covering radius of the code equals the minimal number  $r$  such that every binary  $m$ -tuple can be expressed as a componentwise sum modulo 2 of at most  $r$  columns of  $\mathbf{H}$ . It is a particular case of the following group-theoretic problem:

*Given an abelian group  $(G, +)$ , and a generating subset  $S$ , containing zero, find the minimal  $r$  (covering number of  $G$ ) such that  $S + S + \dots + S = G$ , where the sum extends over  $r$  copies of  $S$ .*

The set  $\{\mathbf{h}_i\}$  can be used for constructing the Cayley graph  $\Gamma$  as follows. Let the  $2^m$  vertices of the graph be associated to all binary  $m$ -tuples, with an edge between two vertices if and only if their componentwise sum modulo 2 is a column of  $\mathbf{H}$ . Then the covering radius of  $C$  is the diameter of  $\Gamma$ .  $\square$

# Chapter 2

## Basic facts

In this chapter we introduce some necessary basic notions. We first define codes and their most important parameters with special emphasis on covering radius and its simplest properties. We next present the MacWilliams transform and study a family of orthogonal polynomials, called the Krawtchouk polynomials, which play a crucial role in connection with the MacWilliams transform. We then analyze the sizes of intersections and unions of Hamming spheres, as well as an extremal property of the sphere. The theory of finite fields is briefly reviewed in Section 2.5. The final two sections are devoted to some well-known families of error-correcting codes and combinatorial designs.

### 2.1 Codes

The main object studied in this book is a (binary) *code*. A binary code of length  $n$  is simply a nonempty set of binary vectors of length  $n$ . More generally, we have the following definition.

**Definition 2.1.1** *Let  $Q$  be a finite set with  $q$  elements. A nonempty subset  $C$  of  $Q^n = Q \times Q \times \dots \times Q$  is called a  $q$ -ary code of length  $n$ .*

The vectors belonging to a code are called *codewords*. A code with only one codeword is called *trivial*. Whenever convenient, codes are assumed to have at least two codewords.

The set  $Q$  is called the *alphabet*. We use the term *vector* for an  $n$ -tuple over an arbitrary alphabet, not only in the case when  $Q$  is a field. The elements of  $Q^n$  are also called *points* or *words*. The set  $Q^n$  is called the ( $q$ -ary) *Hamming space*.

The *Hamming distance* between two vectors  $\mathbf{x} = (x_1, x_2, \dots, x_n)$ ,  $\mathbf{y} = (y_1, y_2, \dots, y_n)$  in  $Q^n$  is the number of coordinates in which they differ, i.e.,

$$d(\mathbf{x}, \mathbf{y}) = |\{i : x_i \neq y_i\}|.$$

The Hamming distance satisfies the *triangle inequality*

$$d(\mathbf{x}, \mathbf{y}) + d(\mathbf{y}, \mathbf{z}) \geq d(\mathbf{x}, \mathbf{z})$$

for all  $\mathbf{x}, \mathbf{y}, \mathbf{z} \in Q^n$ , and is a metric. If  $V \subseteq Q^n$ , then we denote

$$d(\mathbf{x}, V) = \min_{\mathbf{v} \in V} d(\mathbf{x}, \mathbf{v}).$$

Assume that  $0 \in Q$ . The *Hamming weight*  $w(\mathbf{x})$  of a vector  $\mathbf{x} = (x_1, x_2, \dots, x_n) \in Q^n$  is defined by

$$w(\mathbf{x}) = d(\mathbf{x}, \mathbf{0}) \tag{2.1.2}$$

where  $\mathbf{0} = 0^n = (0, 0, \dots, 0)$ . A vector with even (odd) weight is called *even* (*odd*). The set of even (odd) codewords of a code  $C$  is called the *even weight* (*odd weight*) *subcode* of  $C$  and is denoted by  $C_e$  ( $C_o$ ). The *support* of a vector  $\mathbf{x} \in Q^n$  is the set  $\{i : x_i \neq 0\}$  and is denoted by  $\text{supp}(\mathbf{x})$ . In the case of a binary alphabet, vectors can be identified with their supports, and for two binary vectors,  $\mathbf{x}$  and  $\mathbf{y}$ , of the same length,  $\mathbf{x} \subset \mathbf{y}$ ,  $\mathbf{x} \cup \mathbf{y}$ ,  $\mathbf{x} \cap \mathbf{y}$  and  $\mathbf{x} \setminus \mathbf{y}$  refer to the supports of  $\mathbf{x}$  and  $\mathbf{y}$ .

The *minimum distance*  $d$  of a code  $C \subseteq Q^n$  is the smallest of the distances between different codewords of  $C$ , i.e.,

$$d = d(C) = \min_{\mathbf{a}, \mathbf{b} \in C, \mathbf{a} \neq \mathbf{b}} d(\mathbf{a}, \mathbf{b}).$$

Two codes  $C_1 \subseteq Q^n$  and  $C_2 \subseteq Q^n$  are called *equivalent* if  $C_2$  is obtained from  $C_1$  by applying to all the codewords of  $C_1$  a fixed permutation of the coordinates and to each coordinate a permutation of the symbols in the alphabet (which may vary with the coordinates).

The *Hamming sphere* (or *ball*)  $B_r(\mathbf{x})$  of radius  $r$  centred at the vector  $\mathbf{x} \in Q^n$  is defined by

$$B_r(\mathbf{x}) = \{\mathbf{y} \in Q^n : d(\mathbf{y}, \mathbf{x}) \leq r\},$$

and its cardinality is

$$V_q(n, r) = \sum_{i=0}^r \binom{n}{i} (q-1)^i.$$

The subscript  $q$  is usually omitted if  $q = 2$ . More generally, if  $V \subseteq Q^n$ , we denote

$$B_r(V) = \bigcup_{\mathbf{x} \in V} B_r(\mathbf{x}).$$

It is also convenient to have a notation for the *layers* (or *shells*) of the Hamming sphere, and we therefore denote

$$S_r(\mathbf{x}) = \{\mathbf{y} \in Q^n : d(\mathbf{y}, \mathbf{x}) = r\},$$

and

$$S_r = \{\mathbf{y} \in Q^n : w(\mathbf{y}) = r\}.$$

A vector  $\mathbf{x}$  is said to be *r-covered* (or simply *covered* if  $r$  is clear from the context) by a vector  $\mathbf{y}$  if  $d(\mathbf{x}, \mathbf{y}) \leq r$ , i.e.,  $\mathbf{x} \in B_r(\mathbf{y})$  or equivalently  $\mathbf{y} \in B_r(\mathbf{x})$ . A vector  $\mathbf{x}$  is *r-covered* by a set  $V$  if it is *r-covered* by at least one element of  $V$ .

**Definition 2.1.3** The covering radius of a code  $C \subseteq Q^n$  is the smallest integer  $R$  such that every vector  $\mathbf{x} \in Q^n$  is  $R$ -covered by at least one codeword of  $C$ , i.e.,

$$\begin{aligned} R = R(C) &= \max_{\mathbf{x} \in Q^n} d(\mathbf{x}, C) \\ &= \max_{\mathbf{x} \in Q^n} \min_{\mathbf{c} \in C} d(\mathbf{x}, \mathbf{c}). \end{aligned}$$

In other words, the covering radius measures the distance between the code and the farthest-off vectors in the space. Such vectors are called *deep holes*. The covering radius is also the smallest integer  $R$  such that the union of the Hamming spheres of radius  $R$  centred at the codewords is the whole space.

For a code  $C$  with minimum distance  $d$ , the integer

$$e = \lfloor (d - 1)/2 \rfloor$$

is called the *packing radius* or the *error-correcting capability* of the code  $C$ . Notice that  $e$  is the largest integer such that the Hamming spheres of radius  $e$  centred at the codewords are disjoint. Therefore

$$|C| \leq q^n / V_q(n, e),$$

which is called the *sphere-packing bound* or *Hamming bound*.

If  $C$  has packing radius  $e$  and covering radius  $R$ , then clearly  $e \leq R$ . Moreover, if  $d$  is even, then  $e < R$ , and therefore we always have

$$d \leq 2R + 1.$$

A code  $C \subseteq Q^n$  with  $K$  codewords, minimum distance  $d$  and covering radius  $R$  is called an  $(n, K, d)_q R$  code. If  $d$  or  $R$  are not needed, we call  $C$  an  $(n, K)_q$ ,  $(n, K, d)_q$  or  $(n, K)_q R$  code. The subscript  $q$  is usually omitted if  $q = 2$ .

We denote

$$K_q(n, R) = \min\{K : \text{there is an } (n, K)_q R \text{ code}\}$$

for  $0 \leq R \leq n$ . An  $(n, K)_q R$  code with cardinality  $K = K_q(n, R)$  is called *optimal*. An  $(n, K, d)_q R$  code  $C \subseteq Q^n$  is called *maximal* if  $R \leq d - 1$ , or equivalently, if for every  $\mathbf{x} \in Q^n$  the code  $C \cup \{\mathbf{x}\}$  has minimum distance strictly less than  $d$ . We also denote

$$t_q(n, K) = \min\{R : \text{there is an } (n, K)_q R \text{ code}\}$$

and

$$A_q(n, d) = \max\{K : \text{there is an } (n, K, d)_q \text{ code}\}.$$

We usually consider the case  $q = 2$  and omit the subscript  $q$ .

Assume that  $C$  is an  $(n, K)_q R$  code. Because each codeword  $R$ -covers  $V_q(n, R)$  vectors in the space, we know that  $KV_q(n, R) \geq q^n$ . We have therefore proved the inequality

$$K_q(n, R) \geq q^n / V_q(n, R),$$

which is called the *sphere-covering bound*. The *density* of  $C$  is the quotient

$$\mu(C) = \frac{KV_q(n, R)}{q^n}. \quad (2.1.4)$$

The code  $C$  is *perfect* if it attains the sphere-covering bound with equality, i.e., has density 1. In that case the Hamming spheres of radius  $R$  centred at the codewords are disjoint and cover the whole space.

Usually it is convenient to choose an alphabet  $Q$  with some algebraic structure, like addition and multiplication. For example, we can take

$$\mathbb{Z}_q = \text{the set of integers modulo } q,$$

endowed with the usual addition and multiplication. If  $p$  is a prime, every element in  $\mathbb{Z}_p$  has a multiplicative inverse, and so  $\mathbb{Z}_p$  is a *field*, which we also denote by  $\mathbb{F}_p$ . Informally, a field is a set where addition, subtraction, multiplication and division by a nonzero element are defined and satisfy the usual rules. More generally, a finite field of  $q$  elements exists whenever  $q$  is a prime power, and for each prime power  $q$  such a field is essentially unique. We denote

$$\mathbb{F}_q = \text{the finite field of } q \text{ elements},$$

and

$$\mathbb{F} = \mathbb{F}_2 = \{0, 1\} = \text{the finite field of two elements.}$$

The exact definition and basic properties of finite fields are discussed in Section 2.5.

The *complement*  $\bar{\mathbf{x}}$  of a binary vector  $\mathbf{x} \in \mathbb{F}^n$  is obtained by changing all the zeros to ones and vice versa. In the same way as  $\mathbf{0} = 0^n = (0, 0, \dots, 0)$  we denote  $\mathbf{1} = 1^n = (1, 1, \dots, 1)$ . More generally,  $0^i 1^j$ , for instance, denotes a vector beginning with  $i$  zeros and ending with  $j$  ones. We also use the notations  $\mathbf{e}_1 = 10^{n-1}$ ,  $\mathbf{e}_2 = 010^{n-2}, \dots, \mathbf{e}_n = 0^{n-1}1$ .

If our alphabet is  $\mathbb{Z}_q$  or  $\mathbb{F}_q$ , we can define the sum and difference of two vectors  $\mathbf{x} = (x_1, x_2, \dots, x_n)$  and  $\mathbf{y} = (y_1, y_2, \dots, y_n)$  as

$$\mathbf{x} + \mathbf{y} = (x_1 + y_1, x_2 + y_2, \dots, x_n + y_n)$$

and

$$\mathbf{x} - \mathbf{y} = (x_1 - y_1, x_2 - y_2, \dots, x_n - y_n),$$

and their *componentwise product* as

$$\mathbf{x} * \mathbf{y} = (x_1 y_1, x_2 y_2, \dots, x_n y_n).$$

We then have the obvious formula

$$d(\mathbf{x}, \mathbf{y}) = w(\mathbf{x} - \mathbf{y}). \quad (2.1.5)$$

In the binary case  $\mathbf{x} + \mathbf{y} = \mathbf{x} - \mathbf{y}$  and

$$d(\mathbf{x}, \mathbf{y}) = w(\mathbf{x} + \mathbf{y}). \quad (2.1.6)$$

For two sets  $A, B \subseteq \mathbb{Z}_q^n$  or  $A, B \subseteq \mathbb{F}_q^n$  we denote

$$A + B = \{\mathbf{a} + \mathbf{b} : \mathbf{a} \in A, \mathbf{b} \in B\}.$$

For  $\mathbf{x} \in \mathbb{Z}_q^n$  or  $\mathbf{x} \in \mathbb{F}_q^n$  the set

$$\mathbf{x} + A = \{\mathbf{x} + \mathbf{a} : \mathbf{a} \in A\}$$

is called a *translate* of  $A$ . Clearly, a code and its translate have the same covering radius. More generally, two equivalent codes have the same covering radius.

In  $\mathbb{F}_q^n$  we can also define a *scalar multiplication*: if  $\mathbf{x} = (x_1, x_2, \dots, x_n) \in \mathbb{F}_q^n$  and  $\alpha \in \mathbb{F}_q$ , then

$$\alpha \mathbf{x} = (\alpha x_1, \alpha x_2, \dots, \alpha x_n).$$

A code  $C \subseteq \mathbb{F}_q^n$  is called *linear* if all the pairwise sums and scalar multiples of codewords belong to the code. This means that  $C$  is a linear subspace of

$\mathbb{F}_q^n$ . Thus, we can find a basis consisting of, say  $k$ , linearly independent codewords  $\mathbf{g}_1, \mathbf{g}_2, \dots, \mathbf{g}_k$ . The  $k \times n$  matrix

$$\mathbf{G} = \mathbf{G}(C) = \begin{pmatrix} \mathbf{g}_1 \\ \mathbf{g}_2 \\ \vdots \\ \mathbf{g}_k \end{pmatrix}$$

is called a *generator matrix* of  $C$ . The codewords of  $C$  are exactly the  $q^k$  linear combinations of the rows of  $\mathbf{G}$ , and the code is said to have *dimension*  $k$ . A linear code  $C \subseteq \mathbb{F}_q^n$  with dimension  $k$ , minimum distance  $d$  and covering radius  $R$  is called an  $[n, k, d]_q R$  code. If  $d$  or  $R$  are not needed, we call  $C$  an  $[n, k]_q$ ,  $[n, k, d]_q$  or  $[n, k]_q R$  code. We denote

$$t_q[n, k] = \min\{R : \text{there is an } [n, k]_q R \text{ code}\}$$

and

$$k_q[n, R] = \min\{k : \text{there is an } [n, k]_q R \text{ code}\}.$$

For error-correcting codes we have the function

$$a_q[n, d] = \max\{k : \text{there is an } [n, k, d]_q \text{ code}\}.$$

In all the previous notations the subscript  $q$  is usually omitted if  $q = 2$ . The notions of *optimal code* and *maximal code* extend easily to the linear case.

Note that when we use the term “nonlinear”, it is the common shorthand for unrestricted codes — they may even be linear!

Clearly, permuting the coordinates of all the codewords does not change the parameters of the code. Apart from the order of the coordinates, we can always put the generator matrix in the form  $(\mathbf{I}_k, \mathbf{P})$  using the gaussian elimination method. Here  $\mathbf{I}_k$  stands for the  $k \times k$  identity matrix.

If  $\mathbf{x}, \mathbf{y} \in \mathbb{F}_q^n$ , their *scalar product*  $\langle \mathbf{x}, \mathbf{y} \rangle$  is defined by

$$\langle \mathbf{x}, \mathbf{y} \rangle = x_1 y_1 + x_2 y_2 + \dots + x_n y_n.$$

The vectors  $\mathbf{x}$  and  $\mathbf{y}$  are called *orthogonal* if  $\langle \mathbf{x}, \mathbf{y} \rangle = 0$ .

When  $q = 2$ , we have

$$w(\mathbf{x} + \mathbf{y}) = w(\mathbf{x}) + w(\mathbf{y}) - 2w(\mathbf{x} * \mathbf{y}). \quad (2.1.7)$$

Therefore in a binary linear code either all or exactly half of the codewords are even. Indeed, if the code  $C$  has at least one odd codeword  $\mathbf{c}$ , then  $C_o = \mathbf{c} + C_e$  by the previous formula and  $C_o$  is an  $[n, k - 1]$  code.

The *dual*  $C^\perp$  of a linear code  $C \subseteq \mathbb{F}_q^n$  consists of all the vectors  $\mathbf{x} \in \mathbb{F}_q^n$  such that  $\langle \mathbf{x}, \mathbf{c} \rangle = 0$  for all  $\mathbf{c} \in C$ . Assume that  $\mathbf{G} = \mathbf{G}(C) = (\mathbf{I}_k, \mathbf{P})$ . Clearly,

for each  $\mathbf{x}_2 \in \mathbb{F}_q^{n-k}$  there is a unique  $\mathbf{x}_1 \in \mathbb{F}_q^k$  such that the vector  $(\mathbf{x}_1, \mathbf{x}_2)$  is orthogonal to all the rows of  $\mathbf{G}$ . Hence the dimension of the dual code is  $n-k$ . The minimum distance of  $C^\perp$  is called the *dual distance*  $d^\perp$  of the code  $C$ . Let  $\mathbf{H} = (-\mathbf{P}^T, \mathbf{I}_{n-k})$ . A routine check shows that  $\mathbf{G}\mathbf{H}^T$  is the all-zero matrix and therefore  $C^\perp$  has generator matrix  $\mathbf{H}$ . Any matrix  $\mathbf{H} = \mathbf{H}(C)$  which is a generator matrix of  $C^\perp$  is called a *parity check matrix* of  $C$ . Clearly  $(C^\perp)^\perp = C$ . Therefore if  $\mathbf{H}$  is any parity check matrix of  $C$ , the code  $C$  can also be defined as

$$C = \{\mathbf{x} \in \mathbb{F}^n : \mathbf{H}\mathbf{x}^T = \mathbf{0}\}.$$

For every  $\mathbf{x} \in \mathbb{F}^n$ , we call the vector  $\mathbf{H}\mathbf{x}^T \in \mathbb{F}^{n-k}$  the *syndrome* of  $\mathbf{x}$ . Hence the code consists of the vectors with syndrome equal to  $\mathbf{0}$ .

By (2.1.5), the minimum distance of a linear code is the smallest nonzero weight of a codeword, i.e., the *minimum weight* of a nonzero vector  $\mathbf{x} \in \mathbb{F}_q^n$  such that  $\mathbf{H}\mathbf{x}^T = \mathbf{0}$ . In particular, in the binary case we have the following theorem.

**Theorem 2.1.8** *Let  $C$  be a binary  $[n, k]$  code with parity check matrix  $\mathbf{H}$ . The minimum distance of  $C$  is the smallest positive integer  $d$  such that the sum of some  $d$  columns of  $\mathbf{H}$  is  $\mathbf{0}$ .*  $\square$

The covering radius of a linear code can also be defined in terms of the parity check matrix.

**Theorem 2.1.9** *Let  $C$  be a binary  $[n, k]$  code with parity check matrix  $\mathbf{H}$ . The covering radius of  $C$  is the smallest integer  $R$  such that every binary  $(n-k)$ -tuple can be written as the sum of at most  $R$  columns of  $\mathbf{H}$ .*

**Proof.** Let  $\mathbf{x} \in \mathbb{F}^n$  be arbitrary and  $\mathbf{s} = \mathbf{H}\mathbf{x}^T$ . If the sum of columns  $i_1, i_2, \dots, i_t$  equals  $\mathbf{s}$ , then the vector obtained by adding 1 to the coordinates  $i_1, i_2, \dots, i_t$  in  $\mathbf{x}$  belongs to the code  $C$ , and vice versa. This shows that  $d(\mathbf{x}, C)$  is the smallest number of columns of  $\mathbf{H}$  adding to  $\mathbf{s}$ , and our claim follows.  $\square$

**Example 2.1.10** The binary  $[n, n-1]$  code  $C$  with parity check matrix

$$\mathbf{H} = \begin{pmatrix} 1 & 1 & \dots & 1 \end{pmatrix}$$

consists of all the even words of length  $n$ . It is called the *even weight code* and is denoted by  $\mathbb{E}^n$ . Its covering radius is equal to 1. The dual code  $C^\perp$

generated by  $\mathbf{H}$  is called the *repetition code*. It has parity check matrix

$$\mathbf{H}(C^\perp) = \begin{pmatrix} 1 & 1 & & & \\ 1 & & 1 & & \\ \vdots & & & \ddots & \\ 1 & & & & 1 \\ 1 & & & & 1 \end{pmatrix},$$

which is also a generator matrix of  $C$ . From the definition it is clear that the covering radius of  $C^\perp$ , which only consists of the words  $\mathbf{0}$  and  $\mathbf{1}$ , is equal to  $\lfloor n/2 \rfloor$ . This can also be deduced from Theorem 2.1.9: every binary  $(n-1)$ -tuple can be written as a sum of at most  $\lfloor n/2 \rfloor$  columns of  $\mathbf{H}(C^\perp)$ , and any  $(n-1)$ -tuple of weight  $\lfloor n/2 \rfloor$  cannot be written as a sum of fewer than  $\lfloor n/2 \rfloor$  columns of  $\mathbf{H}(C^\perp)$ .  $\square$

More generally, if  $C$  is a linear  $[n, k]_q R$  code with parity check matrix  $\mathbf{H}$ , its covering radius is the smallest  $R$  such that every  $\mathbf{s} \in \mathbb{F}_q^{n-k}$  can be written as a  $(n-k)$ -tuple of  $\mathbf{s}$  as a  $(\mathbb{F}_q)$ -linear combination of at most  $R$  columns of  $\mathbf{H}$ .

Notice that if we know that every element in  $\mathbb{F}_q^m$  can be written as a linear combination of (at most  $R$ ) columns of an  $m \times n$  matrix  $\mathbf{A}$  over  $\mathbb{F}_q$  and  $m \leq n$ , then the matrix  $\mathbf{A}$  has full rank, i.e., its rows are linearly independent.

If  $C$  is an  $[n, k]_q R$  code, the translate

$$\mathbf{x} + C = \{\mathbf{x} + \mathbf{c} : \mathbf{c} \in C\}$$

is called a *coset* of  $C$ . A vector of minimum weight in a coset is called a *coset leader* and its weight the *coset weight*. Decoding involves electing one coset leader per coset. The winner is called an *elected coset leader*. Clearly, the coset weight of  $-\mathbf{x} + C$  is  $d(\mathbf{x}, C)$  by (2.1.5).

**Theorem 2.1.11** *The covering radius of a linear code is the largest of its coset weights.*  $\square$

The space  $\mathbb{F}_q^n$  can be partitioned into  $q^{n-k}$  cosets of an  $[n, k]_q$  code  $C$ , called the *standard partition of the space*. Two vectors belong to the same coset if and only if they have the same syndrome.

The *Voronoi region*  $V(\mathbf{0})$  of an  $[n, k, d]_q R$  code  $C$  is defined as:

$$V(\mathbf{0}) = \{\mathbf{x} \in \mathbb{F}_q^n : d(\mathbf{x}, C) = w(\mathbf{x})\}. \quad (2.1.12)$$

Clearly, the maximum weight of a vector in  $V(\mathbf{0})$  is  $R$ . The elected coset leaders are put in bijection with the syndromes of the received vectors, and

this ensures maximum likelihood decoding. Let  $L$  denote a set of elected coset leaders, with  $|L| = q^{n-k}$ . One has

$$B_{\lfloor(d-1)/2\rfloor}(\mathbf{0}) \subseteq L \subseteq V(\mathbf{0}) \subseteq B_R(\mathbf{0}). \quad (2.1.13)$$

**Theorem 2.1.14** (i) If there is a binary  $(n, K)R$  code and  $R \leq R' \leq n$ , then there also exists a binary  $(n, K')R'$  code with  $K' \leq K$ .

(ii) If, furthermore,  $R'$  satisfies the condition  $K + V(n, R' - 1) \leq 2^n$ , then there exists a binary  $(n, K)R'$  code.

**Proof.** (i) Change 1's to 0's in the codewords of a binary  $(n, K)R$  code, one at a time (the order does not matter). Eventually, when all the 1's have been changed to 0's, the code consists of only the all-zero word and has covering radius  $n$ . Each one-bit change alters the covering radius by at most one. Hence at some stage the covering radius is exactly  $R'$ .

(ii) By (i), there is an  $(n, K')R'$  code  $C$  with  $K' \leq K$ . Let  $\mathbf{x}$  be a deep hole. If  $K \leq 2^n - V(n, R' - 1)$  then we can take  $K - K'$  more vectors from the set  $\mathbb{F}^n \setminus B_{R'-1}(\mathbf{x})$  as codewords without decreasing the covering radius.  $\square$

The previous theorem shows that we could equivalently define  $K(n, R)$  as the smallest possible cardinality of a code of length  $n$  and covering radius *at most*  $R$ .

The covering radius of a code with a single codeword equals the length of the code. Therefore  $K(R, R) = 1$  and  $K(n, R) \geq 2$  when  $n > R$ . Clearly,  $K(n, R) = 2$  whenever  $R < n \leq 2R + 1$ , because the code  $C^\perp$  in Example 2.1.10 has covering radius  $\lfloor n/2 \rfloor \leq R$ .

**Theorem 2.1.15** (i) If there is a binary  $[n, k]R$  code and  $R \leq R' \leq n$ , then there also exists a binary  $[n, k']R'$  code with  $k' \leq k$ .

(ii) If, furthermore,  $R' \leq n - k$ , then there exists a binary  $[n, k]R'$  code.

**Proof.** (i) Change 1's to 0's in the  $k \times n$  generator matrix, one at a time. When there are only 0's left, the matrix generates a code with covering radius  $n$ . Each one-bit change in the generator matrix alters at most one bit in each codeword, and therefore at each step the covering radius changes by at most one. At some stage the covering radius is exactly  $R'$ .

(ii) Assume that  $C$  is an  $[n, k]R$  code, and let  $i$  be the number of words of weight one in  $C$ . Up to the order of the coordinates the code has a generator matrix  $\mathbf{G}$  of the form

$$\begin{pmatrix} \mathbf{I}_i & \mathbf{0} \\ \mathbf{0} & * \end{pmatrix}.$$

The first  $i$  rows of  $\mathbf{G}$  have weight one. All the other rows and all their nontrivial linear combinations have weight at least two. Change now 1's to 0's in the last row until the number of words of weight one in the code increases. Notice that the resulting code  $C'$  still has dimension  $k$  because all the nontrivial linear combinations of the last  $k - i$  rows have weight at least one (changing one bit in the generator matrix changes each codeword in at most one bit). We now replace  $C$  by  $C'$  and apply the same process to  $C'$ . Eventually we obtain a code with  $k$  codewords of weight one, which has covering radius  $n - k$ . Each one-bit change in the matrix changes the covering radius by at most one, and therefore at some stage we have a code with covering radius  $R'$ .  $\square$

Theorem 2.1.15 shows that we could equivalently define  $k[n, R]$  as the smallest dimension  $k$  of any binary linear code of length  $n$  and covering radius *at most*  $R$ . Although formulated in the binary case, Theorems 2.1.14 and 2.1.15 immediately generalize to the nonbinary case.

We also consider *mixed codes*, i.e., assume that  $Q_1, Q_2, \dots, Q_n$  are  $n$  alphabets, not necessarily of the same size, and that  $C \subseteq Q_1 \times Q_2 \times \dots \times Q_n$ . Usually we choose  $Q_i = \mathbb{Z}_{q_i}$  and write  $C \subseteq \mathbb{Z}_{q_1} \mathbb{Z}_{q_2} \dots \mathbb{Z}_{q_n}$  for short.

## 2.2 The MacWilliams identities

In this section we introduce the MacWilliams transform. It is an important tool in the analysis of possible distance distributions of codes. Moreover, it can be used to study the weight structure of the cosets. This topic is treated in more detail in Chapter 8. Here the proofs are given only for the binary case, which makes the presentation simpler.

We start with characters. Let  $\mathbf{x}$  and  $\mathbf{y}$  be two vectors in  $\mathbb{F}^n$ . We define the *additive character*  $\psi$  on  $\mathbb{F}^n$  as

$$\psi_{\mathbf{x}}(\mathbf{y}) = (-1)^{\langle \mathbf{x}, \mathbf{y} \rangle}.$$

The *projection*  $\mathbf{p}_{\mathbf{x}}(\mathbf{y})$  of  $\mathbf{y}$  on  $\mathbf{x}$  is the vector of length  $w(\mathbf{x})$  obtained from  $\mathbf{y}$  by deleting all the positions of  $\mathbf{y}$  not belonging to  $\text{supp}(\mathbf{x})$ . The projection of a set  $G \subseteq \mathbb{F}^n$  on  $\mathbf{x} \in \mathbb{F}^n$  is

$$P_{\mathbf{x}}(G) = \{\mathbf{p}_{\mathbf{x}}(\mathbf{g}) : \mathbf{g} \in G\},$$

i.e., the set of projections of the vectors in  $G$ . Note that the character equals 1 if  $\mathbf{p}_{\mathbf{x}}(\mathbf{y})$  is even, and is  $-1$  otherwise. Evidently, for all  $\mathbf{x}, \mathbf{y}, \mathbf{z} \in \mathbb{F}^n$  we have

$$\psi_{\mathbf{x}}(\mathbf{y} + \mathbf{z}) = \psi_{\mathbf{x}}(\mathbf{y}) \psi_{\mathbf{x}}(\mathbf{z}). \quad (2.2.1)$$

For arbitrary  $G \subseteq \mathbb{F}^n$  and  $\mathbf{x} \in \mathbb{F}^n$  define

$$\psi_{\mathbf{x}}(G) = \sum_{\mathbf{g} \in G} \psi_{\mathbf{x}}(\mathbf{g}). \quad (2.2.2)$$

To make this definition more intuitive, notice that this expression just calculates the difference between the number of even and odd vectors in the projection of  $G$  on  $\mathbf{x}$ .

Let  $C \subseteq \mathbb{F}^n$  be a binary linear code. Its *weight distribution*  $\mathcal{A}(C) = \mathcal{A} = (\mathcal{A}_0, \mathcal{A}_1, \dots, \mathcal{A}_n)$  is a vector of dimension  $n + 1$ , where

$$\mathcal{A}_i = |\{\mathbf{c} \in C : w(\mathbf{c}) = i\}|,$$

i.e., the  $i$ -th component of  $\mathcal{A}(C)$  is the number of codewords of weight  $i$  in  $C$ .

The *distance distribution*  $\mathcal{B}(C) = \mathcal{B} = (\mathcal{B}_0, \mathcal{B}_1, \dots, \mathcal{B}_n)$  is defined by

$$\mathcal{B}_i = \frac{1}{|C|} |\{\mathbf{c}_1, \mathbf{c}_2 \in C : d(\mathbf{c}_1, \mathbf{c}_2) = i\}|,$$

i.e., the  $i$ -th component of  $\mathcal{B}(C)$  is the average number of codewords being at distance  $i$  from a codeword of  $C$ . In the case of linear codes the vectors  $\mathcal{A}$  and  $\mathcal{B}$  coincide, a fact that does not hold in general for nonlinear codes.

If  $C$  is a linear code, the distance distribution  $\mathcal{B}(C^\perp)$  of the dual code  $C^\perp$  is denoted by  $\mathcal{B}^\perp$  and is called the *dual spectrum* of  $C$ . The following theorem shows that  $\mathcal{B}^\perp$  is uniquely determined by  $\mathcal{B}$ .

**Theorem 2.2.3 (MacWilliams identities)** *For a linear code  $C$  of length  $n$*

$$\mathcal{B}_j^\perp = \frac{1}{|C|} \sum_{i=0}^n \mathcal{B}_i P_j^n(i), \quad (2.2.4)$$

where

$$P_j^n(i) = \sum_{\ell=0}^j (-1)^\ell \binom{i}{\ell} \binom{n-i}{j-\ell},$$

is the Krawtchouk polynomial of degree  $j$ .

**Proof.** By linearity, the projection of  $C$  on any vector  $\mathbf{x} \in \mathbb{F}^m$ ,  $m \leq n$ , contains only even vectors, or the same number of even and odd vectors. Moreover,  $P_{\mathbf{x}}(C)$  consists of only even vectors if and only if  $\mathbf{x} \in C^\perp$ . Thus,

$$\psi_{\mathbf{x}}(C) = \begin{cases} |C| & \text{if } \mathbf{x} \in C^\perp, \\ 0 & \text{if } \mathbf{x} \notin C^\perp. \end{cases}$$

Furthermore, if  $S_j$  stands for the set of  $n$ -tuples of weight  $j$ , we have

$$\sum_{\mathbf{x} \in S_j} \psi_{\mathbf{x}}(C) = |C| \mathcal{B}_j^{\perp}. \quad (2.2.5)$$

On the other hand, the same sum can be estimated in a different way, namely,

$$\begin{aligned} \sum_{\mathbf{x} \in S_j} \psi_{\mathbf{x}}(C) &= \sum_{\mathbf{x} \in S_j} \sum_{\mathbf{c} \in C} \psi_{\mathbf{x}}(\mathbf{c}) \\ &= \sum_{\mathbf{c} \in C} \sum_{\mathbf{x} \in S_j} \psi_{\mathbf{x}}(\mathbf{c}). \end{aligned} \quad (2.2.6)$$

The inner sum in the last expression does not depend on the particular choice of  $\mathbf{c}$ , but only on the weight  $w(\mathbf{c})$ . If  $w(\mathbf{c}) = i$ , then each of the  $\binom{i}{\ell} \binom{n-i}{j-\ell}$  vectors of weight  $j$  with exactly  $\ell$  1's in common with  $\mathbf{c}$  contributes  $(-1)^{\ell}$  to the inner sum. Continuing (2.2.6) we get

$$\begin{aligned} \sum_{\mathbf{x} \in S_j} \psi_{\mathbf{x}}(C) &= \sum_{i=0}^n \sum_{\mathbf{c} \in C, w(\mathbf{c})=i} \sum_{\mathbf{x} \in S_j} \psi_{\mathbf{x}}(\mathbf{c}) \\ &= \sum_{i=0}^n \mathcal{B}_i \sum_{\ell=0}^j (-1)^{\ell} \binom{i}{\ell} \binom{n-i}{j-\ell} \\ &= \sum_{i=0}^n \mathcal{B}_i P_j^n(i). \end{aligned}$$

Comparing the result with (2.2.5) we get the claim.  $\square$

If  $C$  is a nonlinear  $(n, K)$  code, we may formally define the MacWilliams transform of the  $n+1$ -tuple  $\mathcal{B}(C)$ , using expression (2.2.4). In general, the result of the transform,  $\mathcal{B}^{\perp}$ , does not correspond to the distance distribution of any code. Nevertheless, an interpretation can be given to some values appearing in the transform. Notice that  $P_0^n(i) = 1$ , and

$$\mathcal{B}_0^{\perp} = \frac{1}{|C|} \sum_{i=0}^n \mathcal{B}_i P_0^n(i) = 1.$$

However, several first components of  $\mathcal{B}^{\perp}$  with positive index, could be zero. Define the *dual distance*  $d^{\perp}(C) = d^{\perp}$  of the code  $C$  as the minimum nonzero index of a nonzero component of  $\mathcal{B}^{\perp}$ . For linear codes, this is just the minimum distance of the dual code,  $d(C^{\perp})$ . Let  $\mathbf{C}$  be the  $K \times n$  array having as its rows all the codewords of  $C$ .

**Theorem 2.2.7** (i)  $\mathcal{B}_j^\perp \geq 0$  for  $j \in [0, n]$ ;

(ii) any set of  $r \leq d^\perp - 1$  columns of  $\mathbf{C}$  contains each  $r$ -tuple exactly  $K/2^r$  times, and  $d^\perp$  is the largest integer with this property.

**Proof.** As in the previous proof, we see that

$$\begin{aligned}
 \mathcal{B}_j^\perp &= \frac{1}{|C|} \sum_{i=0}^n \mathcal{B}_i P_j(i) \\
 &= \frac{1}{|C|^2} \sum_{i=0}^n \sum_{\mathbf{a}, \mathbf{b} \in C, w(\mathbf{a}+\mathbf{b})=i} P_j(i) \\
 &= \frac{1}{|C|^2} \sum_{i=0}^n \sum_{\mathbf{a}, \mathbf{b} \in C, w(\mathbf{a}+\mathbf{b})=i} \sum_{\mathbf{y} \in S_j} \psi_{\mathbf{y}}(\mathbf{a} + \mathbf{b}) \\
 &= \frac{1}{|C|^2} \sum_{\mathbf{y} \in S_j} \sum_{\mathbf{a} \in C} \sum_{\mathbf{b} \in C} \psi_{\mathbf{y}}(\mathbf{a} + \mathbf{b}) \\
 &= \frac{1}{|C|^2} \sum_{\mathbf{y} \in S_j} |\psi_{\mathbf{y}}(C)|^2 \geq 0,
 \end{aligned}$$

and (i) is proved. Moreover,  $\mathcal{B}_j^\perp = 0$  means that  $\psi_{\mathbf{y}}(C) = 0$  for every  $\mathbf{y} \in S_j$ . For  $j = 1$  this gives that every column in  $\mathbf{C}$  has  $K/2$  zeros and  $K/2$  ones.

If  $\mathcal{B}_2^\perp = \mathcal{B}_1^\perp = 0$ , in any two columns all four 2-tuples appear exactly  $K/4$  times each. Indeed, consider two arbitrary columns of  $\mathbf{C}$ . Let  $a_{00}, a_{01}, a_{10}, a_{11}$  stand for the number of occurrences of 00, 01, 10 and 11, respectively, and let  $\mathbf{y} \in S_2$  be a vector with its ones in the corresponding coordinates. Then, solving the system

$$a_{00} - a_{01} - a_{10} + a_{11} = 0,$$

$$a_{00} + a_{01} = a_{10} + a_{11} = a_{00} + a_{10} = a_{01} + a_{11} = K/2,$$

where the first equality follows from  $\psi_{\mathbf{y}}(C) = 0$ , concludes the case  $j = 2$ .

Clearly, the same can be done up to  $d^\perp - 1$ . On the other hand, when  $j = d^\perp$  there exists a vector  $\mathbf{y} \in S_{d^\perp}$  such that  $\psi_{\mathbf{y}}(C) \neq 0$ .  $\square$

Arrays with the property that all  $r \leq s$  columns contain all possible  $r$ -tuples an equal number of times are called *orthogonal arrays of strength s*. Thus, a code with dual distance  $d^\perp$  is an orthogonal array of strength  $d^\perp - 1$ .

## 2.3 Krawtchouk polynomials

Krawtchouk polynomials play a special role in the MacWilliams transform. Actually, Krawtchouk polynomials can be defined for nonbinary alphabets as

well. In what follows, we use an extended definition of the binomial coefficient: for  $x$  real and  $m$  integer,

$$\binom{x}{m} = \begin{cases} \frac{x(x-1)\dots(x-m+1)}{m!} & \text{if } m > 0, \\ 1 & \text{if } m = 0, \\ 0 & \text{otherwise,} \end{cases}$$

where  $m! = m(m-1)(m-2)\dots 1$  and  $0! = 1$ .

**Definition 2.3.1** *The  $q$ -ary Krawtchouk polynomials  $P_k^n(x)$  (of degree  $k$ ) are defined by the following generating function:*

$$\sum_{k=0}^{\infty} P_k^n(x) z^k = (1-z)^x (1+(q-1)z)^{n-x}. \quad (2.3.2)$$

Usually  $n$  is fixed, and is omitted if no confusion arises. An explicit expression for Krawtchouk polynomials is given by

$$P_k^n(x) = \sum_{j=0}^k (-1)^j (q-1)^{k-j} \binom{x}{j} \binom{n-x}{k-j}. \quad (2.3.3)$$

From now on, we consider only binary Krawtchouk polynomials ( $q = 2$ ). Features of nonbinary Krawtchouk polynomials are very similar to those of their binary counterparts.

The properties listed below can be derived by straightforward calculations using (2.3.2). There are several explicit expressions for Krawtchouk polynomials :

$$P_k^n(x) = \sum_{j=0}^k (-1)^j \binom{x}{j} \binom{n-x}{k-j} \quad (2.3.4)$$

$$= \sum_{j=0}^k (-2)^j \binom{x}{j} \binom{n-j}{k-j} \quad (2.3.5)$$

$$= \sum_{j=0}^k (-1)^j 2^{k-j} \binom{n-x}{k-j} \binom{n-k+j}{j}. \quad (2.3.6)$$

A remarkable property of Krawtchouk polynomials is that they satisfy a linear inductive relation in every variable:

$$(k+1)P_{k+1}^n(x) = (n-2x)P_k^n(x) - (n-k+1)P_{k-1}^n(x), \quad (2.3.7)$$

$$(n-x)P_k^n(x+1) = (n-2k)P_k^n(x) - xP_k^n(x-1) \quad (2.3.8)$$

$$(n - k + 1)P_k^{n+1}(x) = (3n - 2k - 2x + 1)P_k^n(x) - 2(n - x)P_k^{n-1}(x). \quad (2.3.9)$$

The sum of the first Krawtchouk polynomials is also a Krawtchouk polynomial for smaller  $n$ :

$$L_e^n(x) = \sum_{i=0}^e P_i^n(x) = P_e^{n-1}(x-1). \quad (2.3.10)$$

$L_e^n(x)$  will play an important role in the sequel and is called the *Lloyd polynomial*.

The first Krawtchouk polynomials are

$$P_0(x) = 1, \quad P_1(x) = n - 2x, \quad P_2(x) = \frac{(n - 2x)^2 - n}{2}, \quad (2.3.11)$$

$$P_3(x) = \frac{(n - 2x)((n - 2x)^2 - 3n + 2)}{6}.$$

Hereafter are listed several values of Krawtchouk polynomials:

$$P_k(0) = \binom{n}{k}, \quad P_k(1) = (1 - 2k/n) \binom{n}{k} \quad (2.3.12)$$

$$P_k(n/2) = 0, \text{ for } k \text{ odd}; \quad P_k(n/2) = (-1)^{k/2} \binom{n/2}{k/2}, \text{ for } k \text{ even}. \quad (2.3.13)$$

If  $P_k(x) = \sum_{i=0}^k c_i x^i$  then

$$c_k = (-2)^k / k!, \quad c_{k-1} = (-2)^{k-1} n / (k-1)!. \quad (2.3.14)$$

The following relations, derived from the definition of Krawtchouk polynomials by rearranging binomial coefficients, reflect some symmetry with respect to their parameters:

$$\binom{n}{x} P_k(x) = \binom{n}{k} P_x(k), \quad (\text{for a nonnegative integer } x); \quad (2.3.15)$$

$$P_k(x) = (-1)^k P_k(n-x), \quad (2.3.16)$$

$$P_k(x) = (-1)^x P_{n-k}(x), \quad (\text{for an integer } x, 0 \leq x \leq n). \quad (2.3.17)$$

**Theorem 2.3.18** *The following orthogonality relations hold:*

$$\sum_{i=0}^n \binom{n}{i} P_k(i) P_\ell(i) = \delta_{k\ell} \binom{n}{k} 2^n, \quad (2.3.19)$$

$$\sum_{i=0}^n P_k(i) P_i(\ell) = \delta_{k\ell} 2^n. \quad (2.3.20)$$

**Proof.** By (2.3.2) the left hand side of (2.3.19) is the coefficient of  $z^k y^i$  in

$$\begin{aligned} & \sum_{i=0}^n \binom{n}{i} (1-z)^i (1+z)^{n-i} (1-y)^i (1+y)^{n-i} \\ &= \sum_{i=0}^n \binom{n}{i} ((1-z)(1-y))^i ((1+z)(1+y))^{n-i} \\ &= ((1-z)(1-y) + (1+z)(1+y))^n \\ &= 2^n (1+zy)^n, \end{aligned}$$

and (2.3.20) then follows from (2.3.15).  $\square$

**Theorem 2.3.21** *Every polynomial  $\alpha(x)$  of degree  $s$  possesses a unique Krawtchouk expansion:*

$$\alpha(x) = \sum_{k=0}^s \alpha_k P_k(x), \quad (2.3.22)$$

where the coefficients are

$$\alpha_k = 2^{-n} \sum_{i=0}^n \alpha(i) P_i(k). \quad (2.3.23)$$

**Proof.** The uniqueness follows from the fact that each Krawtchouk polynomial  $P_k(x)$  is of degree  $k$ . By (2.3.20),

$$\begin{aligned} 2^{-n} \sum_{i=0}^n \alpha(i) P_i(k) &= 2^{-n} \sum_{i=0}^n \sum_{j=0}^s \alpha_j P_j(i) P_i(k) \\ &= \sum_{j=0}^s \alpha_j \left( 2^{-n} \sum_{i=0}^n P_j(i) P_i(k) \right) = \alpha_k \end{aligned}$$

proving (2.3.23).  $\square$

In particular, (2.3.12) yields

$$\alpha_0 = 2^{-n} \sum_{i=0}^n \alpha(i) \binom{n}{i}. \quad (2.3.24)$$

Krawtchouk polynomials satisfy the Christoffel-Darboux formula

$$\frac{P_{k+1}(x)P_k(y) - P_k(x)P_{k+1}(y)}{y-x} = \frac{2}{k+1} \binom{n}{k} \sum_{i=0}^k \frac{P_i(x)P_i(y)}{\binom{n}{i}}. \quad (2.3.25)$$

Recall from the proof of the MacWilliams identities that if  $\mathbf{u} \in \mathbb{F}^n$  is a fixed vector of weight  $s$ , then

$$P_k(s) = \sum_{\mathbf{y} \in \mathbb{F}^n, w(\mathbf{y})=k} (-1)^{\langle \mathbf{u}, \mathbf{y} \rangle}. \quad (2.3.26)$$

Indeed, each of the  $\binom{s}{j} \binom{n-s}{k-j}$  vectors  $\mathbf{y}$  with exactly  $j$  1's in common with  $\mathbf{u}$  contributes  $(-1)^j$  to the sum.

Krawtchouk polynomials satisfy the following multiplication rule.

**Theorem 2.3.27**

$$P_k(x)P_i(x) = \sum_{j=\max\{0, k+i-n\}}^{\min\{k, i\}} a(k, i, j)P_{k+i-2j}(x), \quad (2.3.28)$$

where

$$a(k, i, j) = \binom{k+i-2j}{k-j} \binom{n-k-i+2j}{j}.$$

**Proof.** Assume that  $n > k + i$ , and let  $\mathbf{u} \in \mathbb{F}^n$  be a fixed vector of weight  $s$ . Then

$$\begin{aligned} P_k(s)P_i(s) &= \sum_{w(\mathbf{y})=k} (-1)^{\langle \mathbf{u}, \mathbf{y} \rangle} \sum_{w(\mathbf{z})=i} (-1)^{\langle \mathbf{u}, \mathbf{z} \rangle} \\ &= \sum_{w(\mathbf{y})=k, w(\mathbf{z})=i} (-1)^{\langle \mathbf{u}, \mathbf{y} + \mathbf{z} \rangle}. \end{aligned}$$

If  $\mathbf{v}$  is a fixed vector of weight  $k + i - 2j$ , then the equation  $\mathbf{v} = \mathbf{y} + \mathbf{z}$  has  $a(k, i, j)$  solutions such that  $w(\mathbf{y}) = k$  and  $w(\mathbf{z}) = i$ . Indeed,  $\mathbf{v} + \mathbf{y}$  has weight  $i$  if and only if  $\mathbf{v}$  and  $\mathbf{y}$  have exactly  $k - j$  1's in common. Therefore,

$$\begin{aligned} P_k(s)P_i(s) &= \sum_j a(k, i, j) \sum_{w(\mathbf{v})=k+i-2j} (-1)^{\langle \mathbf{u}, \mathbf{v} \rangle} \\ &= \sum_j a(k, i, j)P_{k+i-2j}(s). \end{aligned}$$

Clearly  $a(k, i, j) = 0$  if  $j < k+i-n$ ,  $j > i$  or  $j > k$ . Because the multiplication rule holds for all  $n > k + i$  and all nonnegative integers  $x \leq n$ , it also holds as an identity for the polynomials.  $\square$

In particular, for  $k < n/2$  we have

$$(P_k(x))^2 = \sum_{j=0}^k \binom{2(k-j)}{k-j} \binom{n-2(k-j)}{j} P_{2(k-j)}(x). \quad (2.3.29)$$

Now we present some facts about zeros of Krawtchouk polynomials. The polynomial  $P_k^n(x)$  has  $k$  different roots  $0 < x_{1,n}(k) < x_{2,n}(k) < \dots < x_{k,n}(k) < n$ . The roots are symmetric with respect to  $n/2$ , that is,

$$x_{i,n}(k) + x_{k+1-i,n}(k) = n, \quad i \in [1, k].$$

More information on the locations of the roots can be easily derived from the following identity

$$x_{1,n}(k) = n/2 - \max \left\{ \sum_{i=0}^{k-2} \omega_i \omega_{i+1} \sqrt{(i+1)(n-i)} \right\}, \quad (2.3.30)$$

where the maximum is taken over all  $\omega_i$  subject to  $\sum_{i=0}^{k-1} \omega_i^2 = 1$ .

In particular, for  $k \leq n/2$  we get

$$\begin{aligned} x_{1,n}(k) &\geq n/2 - \sqrt{(k-1)(n-k+2)} \max \left\{ \sum_{i=0}^{k-2} \omega_i \omega_{i+1} \right\} \\ &\geq n/2 - \sqrt{(k-1)(n-k+2)} \sqrt{\sum_{i=0}^{k-2} \omega_i^2 \sum_{i=1}^{k-1} \omega_i^2} \\ &\geq n/2 - \sqrt{(k-1)(n-k+2)}. \end{aligned} \quad (2.3.31)$$

An upper bound is given by

$$x_{1,n}(k) \leq n/2 - \sqrt{k(n-k)} + k^{1/6} \sqrt{n-k} \quad \text{for } k \leq [n/2]. \quad (2.3.32)$$

The roots of Krawtchouk polynomials for small  $k$  can be approximated by the corresponding roots of Hermite polynomials: if  $n-k \rightarrow \infty$  then the zeros of  $P_k^n(x)$  approach

$$n/2 + \frac{\sqrt{n-k-1}}{2} h_i(k), \quad (2.3.33)$$

where  $h_1(k) < \dots < h_k(k)$  are the roots of the Hermite polynomial  $H_k(z)$ .

## 2.4 Hamming spheres

In this section we discuss some basic properties related to Hamming spheres. We first give some estimates for the size  $V(n, i)$  of a Hamming sphere.

The (binary) *entropy function*  $H(x)$  is defined by

$$H(x) = -x \log_2 x - (1-x) \log_2(1-x)$$

where  $0 \leq x \leq 1$ . The following two lemmas can be obtained using Stirling's formula

$$\sqrt{2\pi} n^{n+\frac{1}{2}} e^{-n+\frac{1}{12n}-\frac{1}{360n^3}} < n! < \sqrt{2\pi} n^{n+\frac{1}{2}} e^{-n+\frac{1}{12n}}. \quad (2.4.1)$$

**Lemma 2.4.2** Suppose that  $0 < \lambda < 1$  and  $\lambda n$  is an integer. Then

$$\frac{2^{nH(\lambda)}}{\sqrt{8n\lambda(1-\lambda)}} \leq \binom{n}{\lambda n} \leq \frac{2^{nH(\lambda)}}{\sqrt{2\pi n\lambda(1-\lambda)}}. \quad (2.4.3)$$

**Proof.** See, e.g., [464, p. 309].  $\square$

**Lemma 2.4.4** Suppose that  $0 < \lambda < \frac{1}{2}$  and  $\lambda n$  is an integer. Then

$$\frac{2^{nH(\lambda)}}{\sqrt{8n\lambda(1-\lambda)}} \leq V(n, \lambda n) \leq 2^{nH(\lambda)}. \quad (2.4.5)$$

**Proof.** See, e.g., [464, p. 310].  $\square$

We next consider the cardinalities of the intersections and unions of two and three Hamming spheres.

**Lemma 2.4.6** If the pairwise distances between  $\mathbf{c}_1, \mathbf{c}_2, \mathbf{c}_3 \in \mathbb{F}^n$  are  $d_1, d_2, d_3$ ,  $d_1 \leq d_2 \leq d_3$  then

$$d_1 + d_2 \geq d_3, 2n \geq d_1 + d_2 + d_3, \text{ and } d_1 + d_2 + d_3 \text{ is even.} \quad (2.4.7)$$

If (2.4.7) holds for nonnegative integers  $d_1, d_2, d_3$ ,  $d_1 \leq d_2 \leq d_3$ , then there are three vectors in  $\mathbb{F}^n$  having pairwise distances  $d_1, d_2, d_3$ .

**Proof.** Suppose  $\mathbf{c}_1, \mathbf{c}_2, \mathbf{c}_3 \in \mathbb{F}^n$  have pairwise distances  $d_1, d_2, d_3$ . Without loss of generality we may assume that  $\mathbf{c}_1 = 0^n$ ,  $\mathbf{c}_2 = 1^x 1^y 0^z 0^v$ ,  $\mathbf{c}_3 = 1^x 0^y 1^z 0^v$  and that  $d(\mathbf{c}_i, \mathbf{c}_j) = d_{6-i-j}$ ,  $i \neq j$ . Then  $x+y = d_3$ ,  $x+z = d_2$ ,  $y+z = d_1$ , and  $2x = -d_1 + d_2 + d_3$ ,  $2y = d_1 - d_2 + d_3$ ,  $2z = d_1 + d_2 - d_3$  and  $2n - 2v = d_1 + d_2 + d_3$ . Therefore  $d_1 + d_2 \geq d_3$  and  $d_1 + d_2 + d_3$  is even and at most  $2n$ . Conversely, given  $d_1, d_2$  and  $d_3$ ,  $0 \leq d_1 \leq d_2 \leq d_3$  satisfying (2.4.7), we define  $x, y, z$  and  $\mathbf{c}_1, \mathbf{c}_2, \mathbf{c}_3 \in \mathbb{F}^n$  by the previous equations.  $\square$

**Theorem 2.4.8** If  $r, s \in \{0, 1, \dots, n\}$ ,  $\mathbf{c}_1, \mathbf{c}_2, \mathbf{c}_3, \mathbf{c}_4 \in \mathbb{F}^n$ , and  $d(\mathbf{c}_1, \mathbf{c}_2) \leq d(\mathbf{c}_3, \mathbf{c}_4)$ , then

$$|B_r(\mathbf{c}_1) \cap B_s(\mathbf{c}_2)| \geq |B_r(\mathbf{c}_3) \cap B_s(\mathbf{c}_4)|.$$

Furthermore, if  $d(\mathbf{c}_3, \mathbf{c}_4) = 1 + d(\mathbf{c}_1, \mathbf{c}_2)$  and  $r + s + d(\mathbf{c}_1, \mathbf{c}_2)$  is odd, equality holds.

**Proof.** It is clearly sufficient to consider the case  $d(\mathbf{c}_3, \mathbf{c}_4) = 1 + d(\mathbf{c}_1, \mathbf{c}_2)$ .

Assume that  $\mathbf{c}_1 = \mathbf{c}_3 = 0^n$ ,  $\mathbf{c}_2 = 01^i 0^{n-i-1}$ ,  $\mathbf{c}_4 = 1^{i+1} 0^{n-i-1}$ . If  $\mathbf{x} \in B_r(\mathbf{c}_1) = B_r(\mathbf{c}_3)$  belongs to  $B_s(\mathbf{c}_4)$  but not to  $B_s(\mathbf{c}_2)$ , it begins with 1 and satisfies  $d(\mathbf{x}, \mathbf{c}_2) = s + 1$ ,  $d(\mathbf{x}, \mathbf{c}_4) = s$ . Changing the first coordinate of  $\mathbf{x}$  to 0 gives a vector  $\mathbf{x}'$  such that  $d(\mathbf{x}', \mathbf{c}_2) = s$ ,  $d(\mathbf{x}', \mathbf{c}_4) = s + 1$ , and  $d(\mathbf{x}', \mathbf{c}_1) \leq r - 1$ , i.e., a vector in  $B_{r-1}(\mathbf{c}_1)$  that belongs to  $B_s(\mathbf{c}_2)$  but not to  $B_s(\mathbf{c}_4)$ , proving the first claim.

Conversely, if  $\mathbf{y} \in B_{r-1}(\mathbf{c}_1)$  belongs to  $B_s(\mathbf{c}_2) \setminus B_s(\mathbf{c}_4)$ , then changing the first coordinate from 0 to 1 in  $\mathbf{y}$  gives a vector  $\mathbf{y}' \in B_r(\mathbf{c}_1)$  that belongs to  $B_s(\mathbf{c}_4) \setminus B_s(\mathbf{c}_2)$ . Therefore, equality holds, unless there is a vector  $\mathbf{y}$  such that  $d(\mathbf{y}, \mathbf{c}_1) = r$ ,  $d(\mathbf{y}, \mathbf{c}_2) = s$ ,  $d(\mathbf{y}, \mathbf{c}_4) = s + 1$ , which by the previous lemma requires that  $d(\mathbf{y}, \mathbf{c}_1) + d(\mathbf{y}, \mathbf{c}_2) + d(\mathbf{c}_1, \mathbf{c}_2) = r + s + d(\mathbf{c}_1, \mathbf{c}_2)$  is even.  $\square$

Of course, as we see from the proof, equality holds in some other cases as well.

If  $n \geq 2r + 1$  and  $a_i$  denotes the cardinality  $|B_r(\mathbf{c}_1) \cap B_r(\mathbf{c}_2)|$  when  $i = d(\mathbf{c}_1, \mathbf{c}_2)$ , then it is easy to verify that

$$a_0 > a_1 = a_2 > a_3 = a_4 > \dots > a_{2r-1} = a_{2r} > a_{2r+1} = \dots = a_n = 0.$$

Because

$$|B_r(\mathbf{c}_1) \cup B_s(\mathbf{c}_2)| = V(n, r) + V(n, s) - |B_r(\mathbf{c}_1) \cap B_s(\mathbf{c}_2)|,$$

we immediately obtain the corresponding statement about the union of two Hamming spheres.

**Theorem 2.4.9** *If  $r, s \in \{0, 1, \dots, n\}$ ,  $\mathbf{c}_1, \mathbf{c}_2, \mathbf{c}_3, \mathbf{c}_4 \in \mathbb{F}^n$ , and  $d(\mathbf{c}_1, \mathbf{c}_2) \leq d(\mathbf{c}_3, \mathbf{c}_4)$ , then*

$$|B_r(\mathbf{c}_1) \cup B_s(\mathbf{c}_2)| \leq |B_r(\mathbf{c}_3) \cup B_s(\mathbf{c}_4)|.$$

*Furthermore, if  $d(\mathbf{c}_3, \mathbf{c}_4) = 1 + d(\mathbf{c}_1, \mathbf{c}_2)$  and  $r + s + d(\mathbf{c}_1, \mathbf{c}_2)$  is odd, equality holds.*  $\square$

Consider now three Hamming spheres.

**Theorem 2.4.10** *Assume that  $r, s, t \in \{0, 1, \dots, n\}$ ,  $\mathbf{c}_1, \mathbf{c}_2, \mathbf{c}_3, \mathbf{c}'_1, \mathbf{c}'_2, \mathbf{c}'_3 \in \mathbb{F}^n$ , and  $d(\mathbf{c}_i, \mathbf{c}_j) \leq d(\mathbf{c}'_i, \mathbf{c}'_j)$  for all  $i$  and  $j$ . Then*

$$|B_r(\mathbf{c}_1) \cap B_s(\mathbf{c}_2) \cap B_t(\mathbf{c}_3)| \geq |B_r(\mathbf{c}'_1) \cap B_s(\mathbf{c}'_2) \cap B_t(\mathbf{c}'_3)|.$$

**Proof.** First consider the case  $d(\mathbf{c}'_1, \mathbf{c}'_2) = d(\mathbf{c}_1, \mathbf{c}_2)$ ,  $d(\mathbf{c}'_2, \mathbf{c}'_3) = d(\mathbf{c}_2, \mathbf{c}_3)$  and  $d(\mathbf{c}'_1, \mathbf{c}'_3) = d(\mathbf{c}_1, \mathbf{c}_3) + 2$ . We may assume that  $\mathbf{c}_1 = \mathbf{c}'_1$  and  $\mathbf{c}_2 = \mathbf{c}'_2$ . Let  $\mathbf{c}_1, \mathbf{c}_2, \mathbf{c}_3$  be as in the figure

$$\begin{aligned}\mathbf{c}_1 &= \mathbf{c}'_1 = 0 \ 0 \ 00\dots0 \ 00\dots0 \ 00\dots0 \ 00\dots0 \\ \mathbf{c}_2 &= \mathbf{c}'_2 = 0 \ 1 \ 11\dots1 \ 11\dots1 \ 00\dots0 \ 00\dots0 \\ \mathbf{c}_3 &= 0 \ 0 \ 00\dots0 \ 11\dots1 \ 11\dots1 \ 00\dots0 \\ \mathbf{c}'_3 &= 1 \ 1 \ 00\dots0 \ 11\dots1 \ 11\dots1 \ 00\dots0\end{aligned}$$

Because there also exists a vector  $\mathbf{c}'_3$  of weight  $w(\mathbf{c}_3) + 2$  such that  $d(\mathbf{c}'_3, \mathbf{c}_2) = d(\mathbf{c}_3, \mathbf{c}_2)$ , we know that  $\mathbf{c}'_3$  has exactly one more 1 in common with  $\mathbf{c}_2$  than  $\mathbf{c}_3$  and therefore there is a coordinate (the first coordinate in the figure) in which  $\mathbf{c}_2$  and  $\mathbf{c}_3$  both have 0 and a coordinate (the second coordinate in the figure) in which  $\mathbf{c}_2$  has 1 and  $\mathbf{c}_3$  has 0. But then we can choose  $\mathbf{c}'_3$  as in the figure. If now  $\mathbf{x} \in B_r(\mathbf{c}_1) \cap B_s(\mathbf{c}_2)$  belongs to  $B_t(\mathbf{c}'_3) \setminus B_t(\mathbf{c}_3)$ , then  $x_1 = x_2 = 1$  and changing the first two coordinates in  $\mathbf{x}$  gives a vector  $\mathbf{x}' \in B_{r-2}(\mathbf{c}_1) \cap B_s(\mathbf{c}_2)$  that belongs to  $B_t(\mathbf{c}_3) \setminus B_t(\mathbf{c}'_3)$  (because  $d(\mathbf{x}', \mathbf{c}_3) = d(\mathbf{x}, \mathbf{c}'_3)$  and  $d(\mathbf{x}', \mathbf{c}'_3) = d(\mathbf{x}, \mathbf{c}_3)$ ). This completes the proof in this case.

Second, assume that  $d(\mathbf{c}'_1, \mathbf{c}'_2) = d(\mathbf{c}_1, \mathbf{c}_2)$ ,  $d(\mathbf{c}'_1, \mathbf{c}'_3) = d(\mathbf{c}_1, \mathbf{c}_3) + 1$ , and  $d(\mathbf{c}'_2, \mathbf{c}'_3) = d(\mathbf{c}_2, \mathbf{c}_3) + 1$ , and let  $\mathbf{c}_1 = \mathbf{c}'_1$ ,  $\mathbf{c}_2 = \mathbf{c}'_2$ , and  $\mathbf{c}_3$  be as in the figure

$$\begin{aligned}\mathbf{c}_1 &= \mathbf{c}'_1 = 0 \ 00\dots0 \ 00\dots0 \ 00\dots0 \ 00\dots0 \\ \mathbf{c}_2 &= \mathbf{c}'_2 = 0 \ 11\dots1 \ 11\dots1 \ 00\dots0 \ 00\dots0 \\ \mathbf{c}_3 &= 0 \ 00\dots0 \ 11\dots1 \ 11\dots1 \ 00\dots0 \\ \mathbf{c}'_3 &= 1 \ 00\dots0 \ 11\dots1 \ 11\dots1 \ 00\dots0\end{aligned}$$

By the assumptions there is a coordinate (the first coordinate in the figure) in which  $\mathbf{c}_2$  and  $\mathbf{c}_3$  both have 0, and we may choose  $\mathbf{c}'_3$  as in the figure. If  $\mathbf{x} \in B_r(\mathbf{c}_1) \cap B_s(\mathbf{c}_2)$  belongs to  $B_t(\mathbf{c}'_3) \setminus B_t(\mathbf{c}_3)$ , then changing the first coordinate in  $\mathbf{x}$  from 1 to 0 gives a vector  $\mathbf{x}' \in B_{r-1}(\mathbf{c}_1) \cap B_{s-1}(\mathbf{c}_2)$  that belongs to  $B_t(\mathbf{c}_3) \setminus B_t(\mathbf{c}'_3)$ , proving the second case.

By Lemma 2.4.6, we may apply the second case a suitable number of times to obtain vectors  $\mathbf{c}''_1, \mathbf{c}''_2, \mathbf{c}''_3$  such that at most one of the differences  $d(\mathbf{c}'_i, \mathbf{c}'_j) - d(\mathbf{c}''_i, \mathbf{c}''_j)$  is nonzero and if there is a nonzero one, it is positive and even. But then the result follows by applying the first case a suitable number of times.  $\square$

An easy modification of the previous proof yields the corresponding statement about the union of three Hamming spheres.

**Theorem 2.4.11** *Assume that  $r, s, t \in \{0, 1, \dots, n\}$ ,  $\mathbf{c}_1, \mathbf{c}_2, \mathbf{c}_3, \mathbf{c}'_1, \mathbf{c}'_2, \mathbf{c}'_3 \in \mathbb{F}^n$ , and  $d(\mathbf{c}_i, \mathbf{c}_j) \leq d(\mathbf{c}'_i, \mathbf{c}'_j)$  for all  $i$  and  $j$ . Then*

$$|B_r(\mathbf{c}_1) \cup B_s(\mathbf{c}_2) \cup B_t(\mathbf{c}_3)| \leq |B_r(\mathbf{c}'_1) \cup B_s(\mathbf{c}'_2) \cup B_t(\mathbf{c}'_3)|.$$

**Proof.** We proceed in the same way as in the previous proof. If in the first case  $\mathbf{x} \notin B_r(\mathbf{c}_1) \cup B_s(\mathbf{c}_2)$  belongs to  $B_t(\mathbf{c}_3) \setminus B_t(\mathbf{c}'_3)$ , then  $x_1 = x_2 = 0$  and changing the first two coordinates in  $\mathbf{x}$  gives a vector  $\mathbf{x}' \notin B_r(\mathbf{c}_1) \cup B_s(\mathbf{c}_2)$  that belongs to  $B_t(\mathbf{c}'_3) \setminus B_t(\mathbf{c}_3)$ . If in the second case  $\mathbf{x} \notin B_r(\mathbf{c}_1) \cup B_s(\mathbf{c}_2)$  belongs to  $B_t(\mathbf{c}_3) \setminus B_t(\mathbf{c}'_3)$ , then changing the first coordinate in  $\mathbf{x}$  from 0 to 1 gives a vector  $\mathbf{x}' \notin B_r(\mathbf{c}_1) \cup B_s(\mathbf{c}_2)$  that belongs to  $B_t(\mathbf{c}'_3) \setminus B_t(\mathbf{c}_3)$ .  $\square$

**Example 2.4.12** Let

$$\begin{aligned}\mathbf{c}_1 &= \mathbf{c}'_1 = 000000\dots0 \\ \mathbf{c}_2 &= \mathbf{c}'_2 = 110000\dots0 \\ \mathbf{c}_3 &= \mathbf{c}'_3 = 101000\dots0 \\ \mathbf{c}_4 &= 011000\dots0 \\ \mathbf{c}'_4 &= 100100\dots0.\end{aligned}$$

For these binary vectors of length  $n$ ,  $d(\mathbf{c}_i, \mathbf{c}_j) = d(\mathbf{c}'_i, \mathbf{c}'_j) = 2$  for all  $i \neq j$ . However,  $|\cap_{i=1}^4 B_2(\mathbf{c}_i)| = 4$  whereas  $|\cap_{i=1}^4 B_2(\mathbf{c}'_i)| = n+1$ . Therefore the cardinality of the intersection is no longer necessarily determined by the pairwise distances of the centres when the number of spheres is four (or more), and the same is true for the union.

The code  $C = \{\mathbf{c}_1, \mathbf{c}_2, \mathbf{c}_3, \mathbf{c}_4\}$  has covering radius  $n-2$ , whereas the code  $C' = \{\mathbf{c}'_1, \mathbf{c}'_2, \mathbf{c}'_3, \mathbf{c}'_4\}$  has covering radius  $n-1$ . This shows that the covering radius is not uniquely determined by the pairwise distances between the four codewords.  $\square$

Although there exist some essential differences, the geometries of the Hamming and euclidean spaces are in many respects similar. One of the most crucial properties is that the sphere is the set of maximal size among the sets of given diameter (Theorem 2.4.16). The *diameter* of a set  $S \subseteq \mathbb{F}^n$  is defined by

$$\text{diam}(S) = \max_{\mathbf{x}, \mathbf{y} \in S} d(\mathbf{x}, \mathbf{y}).$$

A set  $S \subseteq \mathbb{F}^n$  is said *hereditary* if

$$\mathbf{x} \in S \text{ and } \text{supp}(\mathbf{y}) \subseteq \text{supp}(\mathbf{x}) \Rightarrow \mathbf{y} \in S.$$

A simple property on the diameter of a hereditary set is the following:

**Lemma 2.4.13** *For any two elements  $s_1$  and  $s_2$  of a hereditary set  $S$ ,*

$$|\text{supp}(s_1) \cup \text{supp}(s_2)| \leq \text{diam}(S).$$

**Proof.** The vector  $s_1 \setminus s_2$ , with support  $\text{supp}(s_1) \setminus \text{supp}(s_2)$ , belongs to  $S$  by heredity, and has disjoint support with  $s_2$ ; thus  $|\text{supp}(s_1) \cup \text{supp}(s_2)| = d(s_1 \setminus s_2, s_2)$  is upperbounded by the diameter of  $S$ .  $\square$

Any sphere centred at  $\mathbf{0}$  is hereditary. The Voronoi region  $V(\mathbf{0})$ , defined by (2.1.12), which actually coincides with the set of coset leaders, is hereditary as well. This does not necessarily hold for a set of elected coset leaders. However, we have the following

**Theorem 2.4.14** *In a binary linear code, a set of elected coset leaders can be chosen hereditary.*

**Proof.** Let  $C(0) \cup C(1) \cup \dots \cup C(2^{n-k} - 1)$  be the partition of  $\mathbb{F}^n$  into the cosets of an  $[n, k]$  code  $C$ . For any vector  $\mathbf{x} \in \mathbb{F}^n$ , define the weight  $\omega(\mathbf{x}) = \sum_{i \in \text{supp}(\mathbf{x})} 2^i$ . This induces a linear order  $\omega$  on  $\mathbb{F}^n$ :  $\mathbf{x} <_{\omega} \mathbf{y}$  if and only if  $\omega(\mathbf{x}) < \omega(\mathbf{y})$ . In each coset  $C(i)$ , we elect, among the coset leaders, the vector, say  $s_i$ , preceding all the others with respect to  $\omega$ . Set  $L = \{s_i : 0 \leq i \leq 2^{n-k} - 1\}$ . Assume that  $L$  is not hereditary: let  $\mathbf{x} \in \mathbb{F}^n \setminus L$  and  $s_i \in L$  be such that  $\text{supp}(\mathbf{x}) \subset \text{supp}(s_i)$ . Observe that  $\mathbf{x}$  is a coset leader by the heredity of the Voronoi region. Then  $s_i = \mathbf{x} + (s_i + \mathbf{x})$ , with  $\text{supp}(\mathbf{x} + s_i) \cap \text{supp}(\mathbf{x}) = \emptyset$ . Consequently,  $\omega(s_i) = \omega(\mathbf{x}) + \omega(\mathbf{x} + s_i)$ . Let  $s_j$  be the elected coset leader of the coset containing  $\mathbf{x}$ :  $\mathbf{x} + s_j = \mathbf{c} \in C$ ,  $w(s_j) = w(\mathbf{x})$  and  $s_j <_{\omega} \mathbf{x}$ . We conclude by noting that  $\omega(\mathbf{c} + s_i) = \omega(\mathbf{x} + s_i + s_j) \leq \omega(\mathbf{x} + s_i) + \omega(s_j) < \omega(\mathbf{x} + s_i) + \omega(\mathbf{x}) = \omega(s_i)$ , and similarly  $w(\mathbf{c} + s_i) = w(s_i)$ , contradicting the way  $s_i$  was elected.  $\square$

Let us split the elements of a set  $S$  in two sets  $S_0^{(i)}$  and  $S_1^{(i)}$ , according to whether their  $i$ -th component is 0 or 1. Define a set of transformations  $\tau_i$  by

$$\tau_i(s) = \begin{cases} s + \mathbf{e}_i, & \text{if } s \in S_1^{(i)} \text{ and } s + \mathbf{e}_i \notin S_0^{(i)} \\ s, & \text{otherwise.} \end{cases}$$

Notice that performing  $\tau_i$  can only decrease the weight.

**Lemma 2.4.15** *A set  $S$  is one-to-one mapped by  $\tau_i$  onto a set with smaller or equal diameter. If  $S$  is stable under all  $\tau_i$ 's, then  $S$  is hereditary.*

**Proof.** We first check injectivity: let  $s_1$  and  $s_2$  be two distinct elements of  $S$ ,  $s'_1$  and  $s'_2$  their respective images under  $\tau_i$ . There is something to prove only if exactly one element, say  $s_2$ , moves; thus  $s'_1 = s_1$  and  $s'_2 = s_2 + \mathbf{e}_i$ . If  $s'_2 = s'_1$ , then  $s_2 + \mathbf{e}_i = s_1$ , and  $s_2$  should not have moved. Thus  $s'_2 \neq s'_1$ .

Now  $d(s'_1, s'_2) = d(s_1, s_2 + \mathbf{e}_i) = d(s_1, s_2) - 1$ , if  $s_1 \in S_0^{(i)}$ . If  $s_1 \in S_1^{(i)}$ , then  $s_1^* := s_1 + \mathbf{e}_i \in S_0^{(i)}$  (otherwise,  $s_1$  would have moved). But then,

$d(s'_1, s'_2) = d(s_1^*, s_2) \leq \text{diam}(S)$ . Thus the diameter cannot increase. Heredity can be rephrased as

$$s \in S_1^{(i)} \Rightarrow s + e_i \in S_0^{(i)}, \text{ for all } i.$$

This property is clearly satisfied if  $S$  is stable under every  $\tau_i$ .  $\square$

**Theorem 2.4.16 (Kleitman theorem)** *Let  $B \subseteq \mathbb{F}^n$ ,  $n \geq 2r + 1$ , be a set of diameter  $2r$ . Then  $|B| \leq V(n, r)$ .*

**Proof.** Let  $B$  be a set of diameter  $2r$  in  $\mathbb{F}^n$ . Apply the transformations  $\tau_i$  coordinatewise until  $B$  stabilizes to some  $B^*$ . Combining Lemmas 2.4.15 and 2.4.13,  $B^*$  is a hereditary set of size  $|B|$ , with diameter at most  $2r$  and

$$|\text{supp}(a) \cup \text{supp}(b)| \leq 2r \quad (2.4.17)$$

for all  $a, b \in B^*$ . In particular,  $0 \in B^*$  and any element in  $B^*$  has weight at most  $2r$ .

This is already sufficient for an asymptotic version of Theorem 2.4.16.

**Theorem 2.4.18** *For  $n$  large enough with respect to  $r$ , the largest subset of  $\mathbb{F}^n$  with diameter  $2r$  is realized by a sphere of radius  $r$ .*

**Proof.** Let  $S$  be such a set, and  $S^*$  its stabilized version under the  $\tau_i$ 's. Take an element  $s_1 \in S^*$  of maximal weight  $r + k$ . Assume  $k > 0$  (otherwise there is nothing to prove). For any  $s_2 \in S^*$ ,  $\text{supp}(s_2)$  is the disjoint union of  $\text{supp}(s_2) \cap \text{supp}(s_1)$  and  $\text{supp}(s_2) \setminus \text{supp}(s_1)$ , the latter of size at most  $r - k$  by (2.4.17) applied to  $s_1, s_2 \setminus s_1 \in S^*$ . Thus the number of such  $s_2$ 's is upperbounded by

$$2^{r+k} \sum_{i=0}^{r-k} \binom{n-r-k}{i} = o(V(n, r)).$$

$\square$

We now end the proof of Theorem 2.4.16. We apply another set of transformations  $\sigma_i$  to  $B^*$ , with the goal of “pushing 1's to the left”. Split again the elements of  $B^*$  in two: the set  $B_{01}^{(i)}$  of vectors with a 0 in position  $i - 1$  and 1 in position  $i$ , and its complement in  $B^*$ . Define  $\sigma_i$  by

$$\sigma_i(a) = \begin{cases} a + e_{i-1} + e_i, & \text{if } a \in B_{01}^{(i)} \text{ and } a + e_{i-1} + e_i \notin B^* \\ a, & \text{otherwise.} \end{cases}$$

Apply these transformations coordinatewise until  $B^*$  stabilizes to some  $B''$ . Analogously to the previous case one easily checks that  $B''$  is a hereditary set (it remains so after each  $\sigma_i$ ) of size  $|B|$  and diameter at most  $2r$ . Moreover, along with any vector  $\mathbf{a}$  the set  $B''$  contains all the vectors obtained from  $\mathbf{a}$  by interchanging any number of 1's with 0's, each 0 lying to the left of the corresponding 1 in  $\mathbf{a}$ .

For  $\mathbf{a} \in B''$ , assume that  $w(\mathbf{a}) = r + k$  where  $k > 0$ . Then the following property (P) holds: at most  $r - k$  of these 1's can be associated to distinct 0's in  $\mathbf{a}$ , each 0 lying to the left of the corresponding 1. Indeed, if there were  $r - k + 1$  such 1's, the vector  $\mathbf{b}$  obtained by interchanging the 1's with the 0's would also belong to  $B''$ , and  $d(\mathbf{a}, \mathbf{b}) = 2(r - k + 1)$ . Then

$$\begin{aligned} |\text{supp}(\mathbf{a}) \cup \text{supp}(\mathbf{b})| &= d(\mathbf{a}, \mathbf{b}) + |\text{supp}(\mathbf{a} * \mathbf{b})| \\ &= 2(r - k + 1) + w(\mathbf{a}) - (r - k + 1) > 2r \end{aligned}$$

would hold, contradicting (2.4.17).

We now define a last set of transformations: split  $B''$  into  $B_l'' = \{\mathbf{a} \in B'' : w(\mathbf{a}) \leq r\}$  and  $B_h'' = \{\mathbf{a} \in B'' : w(\mathbf{a}) = r + k, 0 < k \leq r\}$  (for “light” and “heavy”). At the end of the following procedure,  $B_l''$  is unchanged, and  $B_h''$  is transformed into  $A'$ , with

$$|A'| = |B_h''|, A' \cap B_l'' = \emptyset, A' \subseteq B_r(\mathbf{0}).$$

To every  $\mathbf{a}$  in  $B_h''$ , associate the corresponding vectors  $\mathbf{a}'$  and  $\mathbf{a}''$  as follows. The vector  $\mathbf{a}'$  has 0's in all positions where  $\mathbf{a}$  has 1's. To fill the 1's in  $\mathbf{a}'$  we start from the rightmost 1 in  $\mathbf{a}$  and set 1 in  $\mathbf{a}'$  in the first position to the left of this 1 where  $\mathbf{a}$  has 0. If there is no such 0 we assume that the positions with indices  $n$  and less are to the left of the first coordinate. We proceed in the same manner with the next  $r - k$  (to the left) nonzero positions of  $\mathbf{a}$ , adding in each step a new 1 to  $\mathbf{a}'$ . Clearly  $w(\mathbf{a}') = r - k + 1$ . Since  $\mathbf{a}$  and  $\mathbf{a}'$  have disjoint supports,  $d(\mathbf{a}, \mathbf{a}') = 2r + 1$ , and thus  $\mathbf{a}' \notin B''$ .

Let  $i$  be the number of steps for constructing  $\mathbf{a}'$  when the inserted 1 has index less than the index of the corresponding 1 in  $\mathbf{a}$ , and let  $\mathbf{a}''$  be the vector we get after the  $i$ -th step. By the property (P),  $\mathbf{a}''$  is always defined; evidently,  $w(\mathbf{a}'') = i$ . Notice that  $i$  actually may be deduced from  $\mathbf{a}'$  since  $i$  is the maximal number of 1's in  $\mathbf{a}'$  which can be paired with distinct 0's of  $\mathbf{a}'$ , each 0 lying to the right of the corresponding 1; and, given  $\mathbf{a}'$ , we may determine  $\mathbf{a}''$ . From  $\mathbf{a}''$ , moreover, we may recover  $\mathbf{a}$ , by inserting  $i$  1's in the places as close as possible to the right of the 1's in  $\mathbf{a}''$ ; the remaining 1's in  $\mathbf{a}$  are inserted in the first  $r + k - i$  left hand places which are not 1's of  $\mathbf{a}''$  or already 1's in  $\mathbf{a}$ .

So, we have constructed a one-to-one mapping from  $\mathbf{a}$  to  $\mathbf{a}'$ , and therefore, a one-to-one mapping from  $B$  into a subset of  $B_r(\mathbf{0})$ .  $\square$

**Example 2.4.19** Let  $n = 11$ ,  $r = 4$ ,  $k = 1$ , and consider how the vector  $\mathbf{a} \in B_h''$  given below is transformed:

$\mathbf{a}$	10110000011	
	0*00*****00	Step 0
	0*00****100	Step 1
	0*00***1100	Step 2
	0100***1100	Step 3
	0100**11100	Step 4
$\mathbf{a}'$	01000011100.	

Here  $i = 3$  and  $\mathbf{a}'' = 01000011100$  can be deduced from  $\mathbf{a}'$ . Now  $\mathbf{a}$  can be recovered from  $\mathbf{a}''$  by putting three 1's immediately to the right of the 1's in  $\mathbf{a}''$ :  $\mathbf{a} = *01****0011$ , then 1's in the two leftmost positions where  $\mathbf{a}$  and  $\mathbf{a}''$  have no 1's:  $\mathbf{a} = 10110000011$ .  $\square$

Note that for  $q$  large enough, Theorem 2.4.16 does not hold: choose  $B = \mathbb{F}_q^{2r} \oplus \mathbf{0}^{n-2r}$ . Then,  $B$  clearly has diameter  $2r$ , and as a function of  $q$ :

$$|B| = q^{2r} > V_q(n, r) = O(q^r).$$

## 2.5 Finite fields

In this section we only briefly go through some basic definitions and results about finite fields that are required later. For a more thorough discussion, see, e.g., the references in the Notes.

**Definition 2.5.1** Let  $G$  be a nonempty set and  $\circ$  be a binary operation defined on  $G$ . The pair  $(G, \circ)$  is a group if the following three properties hold:

(i)  $(a \circ b) \circ c = a \circ (b \circ c)$  for all  $a, b, c \in G$ .

(ii) There is an identity element  $e$  such that  $e \circ a = a \circ e = a$  for all  $a \in G$ .

(iii) For every  $a \in G$  there exists an inverse  $a^{-1} \in G$  such that  $a \circ a^{-1} = a^{-1} \circ a = e$ .

If, furthermore,

(iv)  $a \circ b = b \circ a$  for all  $a, b \in G$ ,

the group is called abelian or commutative.

We often use the notation of ordinary multiplication or addition for the group operation. Using the multiplicative notation, we write  $a^n = a \cdot a \cdot \dots \cdot a$  ( $n$  factors  $a$ ), and in the additive notation  $na = a + a + \dots + a$  ( $n$  summands  $a$ ). If  $n$  is negative, we define  $a^n = (a^{-1})^{-n}$  and  $na = (-n)(-a)$  respectively.

**Definition 2.5.2** A group  $(G, \cdot)$  is called cyclic if there is an element  $a \in G$  such that every  $b \in G$  is of the form  $a^j$  for some  $j \in \mathbb{Z}$ . Such an element is called a generator of the group.

**Definition 2.5.3** Let  $R$  be a nonempty set and  $+$  and  $\cdot$  be two binary operations defined on  $R$ . The triple  $(R, +, \cdot)$  is a ring if

- (i)  $(R, +)$  is an abelian group,
- (ii)  $(a \cdot b) \cdot c = a \cdot (b \cdot c)$  for all  $a, b, c \in R$ ,
- (iii) there is an element  $1 \in R$  such that  $1 \cdot a = a \cdot 1 = a$  for all  $a \in R$ ,
- (iv)  $a \cdot (b + c) = a \cdot b + a \cdot c$  and  $(a + b) \cdot c = a \cdot c + b \cdot c$  for all  $a, b, c \in R$ .

The ring  $(R, +, \cdot)$  is called commutative if

- (v)  $a \cdot b = b \cdot a$  for all  $a, b \in R$ .

The identity element of  $(R, +)$  is denoted by 0.

**Definition 2.5.4** A ring  $(F, +, \cdot)$  is called a field if the pair  $(F \setminus \{0\}, \cdot)$  is an abelian group.

We denote  $F^* = F \setminus \{0\}$ . As with the usual multiplication, we often omit the symbol  $\cdot$  and simply write  $ab$  instead of  $a \cdot b$ .

The ring of integers modulo  $n$  is denoted by  $\mathbb{Z}_n$ . When  $n$  is a prime,  $\mathbb{Z}_n$  is a field.

The smallest integer  $p$  such that  $p1 = 1 + 1 + \dots + 1 = 0$  is called the characteristic of the field. The characteristic of a finite field is always a prime. In a field  $F$  with characteristic  $p$

$$(a + b)^p = a^p + b^p$$

for all  $a, b \in F$ , because all the binomial coefficients  $\binom{p}{i}$ ,  $0 < i < p$ , are divisible by  $p$ .

**Definition 2.5.5** If  $(F, +, \cdot)$  is a field, the set of polynomials over  $F$  defined by

$$F[x] = \{a_0 + a_1x + \dots + a_mx^m : m = 0, 1, \dots; a_i \in F, 0 \leq i \leq m\}$$

together with the addition

$$\left( \sum a_i x^i \right) + \left( \sum b_i x^i \right) = \sum (a_i + b_i) x^i$$

and multiplication

$$\left( \sum a_i x^i \right) \left( \sum b_j x^j \right) = \sum \left( \sum_{i+j=k} a_i b_j \right) x^k$$

forms a ring  $(F[x], +, \cdot)$  called the polynomial ring over  $F$ .

A polynomial  $a_0 + a_1x + \dots + a_mx^m \in F[x]$  with  $m \geq 1$  and  $a_m \neq 0$  is called *irreducible* if it cannot be written as a product of two polynomials in  $F[x]$  both of degree less than  $m$ .

**Theorem 2.5.6** *If  $p$  is a prime, then for every  $m \geq 1$  there exists an irreducible polynomial  $g(x) \in \mathbb{Z}_p[x]$  of degree  $m$ .*  $\square$

**Theorem 2.5.7** *If  $p$  is a prime and  $g(x)$  is an irreducible polynomial of degree  $m$  in  $\mathbb{Z}_p[x]$ , then the residue classes*

$$a(x) + \langle g(x) \rangle := \{a(x) + s(x)g(x) : s(x) \in \mathbb{Z}_p[x]\},$$

where  $a(x) \in \mathbb{Z}_p[x]$ , together with the usual addition

$$(a(x) + \langle g(x) \rangle) + (b(x) + \langle g(x) \rangle) = (a(x) + b(x)) + \langle g(x) \rangle$$

and multiplication

$$(a(x) + \langle g(x) \rangle)(b(x) + \langle g(x) \rangle) = a(x)b(x) + \langle g(x) \rangle$$

form a finite field with  $p^m$  elements.  $\square$

The characteristic of this field is  $p$ . Consequently, for every prime  $p$  and every integer  $m \geq 1$  there exists a finite field with  $q = p^m$  elements, which is denoted by  $\mathbb{F}_q$ . It can be shown that for each such  $q$  there is a unique field with  $q$  elements (up to isomorphism). The field  $\mathbb{F}_q$  is a vector space over  $\mathbb{F}_p$ . If we choose a basis for  $\mathbb{F}_q$  over  $\mathbb{F}_p$ , every element of  $\mathbb{F}_q$  can be written uniquely as an  $\mathbb{F}_p$ -linear combination of the basis elements.

**Example 2.5.8** The polynomial  $g(x) = x^4 + x + 1 \in \mathbb{Z}_2[x]$  is irreducible, and can be used to construct the finite field of 16 elements. The residue classes  $a(x) + \langle g(x) \rangle$  are represented by polynomials in  $\mathbb{Z}_2[x]$  of degree less than four. If we denote the residue class  $x + \langle g(x) \rangle$  by  $\alpha$ , then all the elements of the field are  $0, 1, \alpha, \alpha + 1, \alpha^2, \alpha^2 + 1, \alpha^2 + \alpha, \alpha^2 + \alpha + 1, \alpha^3, \alpha^3 + 1, \alpha^3 + \alpha, \alpha^3 + \alpha + 1, \alpha^3 + \alpha^2, \alpha^3 + \alpha^2 + 1, \alpha^3 + \alpha^2 + \alpha, \alpha^3 + \alpha^2 + \alpha + 1$ . Addition in the field is easy. For example,

$$(\alpha^3 + \alpha^2 + 1) + (\alpha^2 + \alpha + 1) = \alpha^3 + \alpha,$$

because the characteristic is two. Multiplication of any two elements is almost as easy. For instance,

$$(\alpha^3 + \alpha^2 + 1)(\alpha^2 + \alpha + 1) = \alpha^5 + \alpha + 1.$$

Table 2.1: The field of 16 elements.

0	= 0	= 0000
$1 = \alpha^{15}$	= 1	= 0001
$\alpha$	= $\alpha$	= 0010
$\alpha^2$	= $\alpha^2$	= 0100
$\alpha^3$	= $\alpha^3$	= 1000
$\alpha^4$	= $\alpha + 1$	= 0011
$\alpha^5$	= $\alpha^2 + \alpha$	= 0110
$\alpha^6$	= $\alpha^3 + \alpha^2$	= 1100
$\alpha^7$	= $\alpha^3 + \alpha + 1$	= 1011
$\alpha^8$	= $\alpha^2 + 1$	= 0101
$\alpha^9$	= $\alpha^3 + \alpha$	= 1010
$\alpha^{10}$	= $\alpha^2 + \alpha + 1$	= 0111
$\alpha^{11}$	= $\alpha^3 + \alpha^2 + \alpha$	= 1110
$\alpha^{12}$	= $\alpha^3 + \alpha^2 + \alpha + 1$	= 1111
$\alpha^{13}$	= $\alpha^3 + \alpha^2 + 1$	= 1101
$\alpha^{14}$	= $\alpha^3 + 1$	= 1001

To see which of the sixteen elements listed above this is, we use the fact that  $\alpha^4 = \alpha + 1$  and hence  $\alpha^5 = \alpha(\alpha + 1) = \alpha^2 + \alpha$ . Consequently  $\alpha^5 + \alpha + 1 = \alpha^2 + 1$ . In this way it is easy to verify that all the nonzero elements of the field are powers of  $\alpha$  as shown in Table 2.1.

Using this table the multiplication is even easier: to multiply  $\alpha^3 + \alpha^2 + 1$  and  $\alpha^2 + \alpha + 1$ , we check from the table that  $\alpha^3 + \alpha^2 + 1 = \alpha^{13}$  and  $\alpha^2 + \alpha + 1 = \alpha^{10}$ , and hence their product is  $\alpha^{23} = \alpha^8 = \alpha^2 + 1$ .  $\square$

**Theorem 2.5.9** *The multiplicative group  $(\mathbb{F}_q^*, \cdot)$  of  $\mathbb{F}_q$  is cyclic.*  $\square$

A generator of the multiplicative group of  $\mathbb{F}_q$  is called a *primitive element* of the field. If  $\alpha$  is a primitive element of the field  $\mathbb{F}_q$ , then  $\alpha^{q-1} = 1$ . Consequently, the elements of the finite field  $\mathbb{F}_q$  are the  $q$  roots of the equation  $x^q = x$ . If  $k > 0$  is not divisible by  $q - 1$ , then

$$\sum_{a \in \mathbb{F}_q} a^k = \sum_{i=0}^{q-2} \alpha^{ik} = \frac{\alpha^{k(q-1)} - 1}{\alpha^k - 1} = 0. \quad (2.5.10)$$

Let  $(G, \cdot)$  be a finite abelian group and 1 the identity element of  $G$ . A *character* of  $G$  is a mapping  $\varphi$  from  $G$  to the set of complex numbers with

norm 1 such that

$$\varphi(ab) = \varphi(a)\varphi(b) \text{ for all } a \in G, b \in G.$$

The mapping  $\varphi$  such that  $\varphi(a) = 1$  for all  $a \in G$  is called the *trivial character*. For the trivial character, the sum  $\sum_{a \in G} \varphi(a)$  equals the cardinality of the group.

**Theorem 2.5.11** *If  $\varphi$  is a nontrivial character of an abelian group  $G$ , then*

$$\sum_{a \in G} \varphi(a) = 0.$$

**Proof.** There is an element  $b$  of  $G$  such that  $\varphi(b) \neq 1$ . When  $a$  runs through  $G$ , so does  $ba$ . Hence

$$(1 - \varphi(b)) \sum_{a \in G} \varphi(a) = \sum_{a \in G} \varphi(a) - \sum_{a \in G} \varphi(ba) = 0.$$

□

The characters of the additive and multiplicative groups of a finite field are called *additive* and *multiplicative characters*, respectively.

In the field  $\mathbb{F}_q$ , where  $q = p^m$ , the *trace function*  $Tr$  is defined by

$$Tr(x) = x + x^p + x^{p^2} + \dots + x^{p^{m-1}} \text{ for all } x \in \mathbb{F}_q.$$

The trace function satisfies the property

$$Tr(a + b) = Tr(a) + Tr(b) \text{ for all } a, b \in \mathbb{F}_q$$

and it is a surjective mapping from  $\mathbb{F}_q$  to  $\mathbb{F}_p$ . Let

$$e(x) = e^{2\pi i Tr(x)/p} \text{ for all } x \in \mathbb{F}_q.$$

For every  $a \in \mathbb{F}_q$ , the function

$$\psi_a(x) = e(ax) \text{ for all } x \in \mathbb{F}_q$$

is an additive character of  $\mathbb{F}_q$ . When  $a$  runs through all the nonzero elements of  $\mathbb{F}_q$ , the functions  $\psi_a$  run through all the  $q - 1$  different nontrivial additive characters of the field  $\mathbb{F}_q$ .

## 2.6 Families of error-correcting codes

Surprisingly, the theory of covering codes has quite a small intersection with the theory of error-correcting codes. However, sometimes error-correcting codes are used as building blocks for constructing covering codes. As well, in Chapters 9 and 10 we address the problem of estimating the covering radii of some classes of error-correcting codes. In this section we survey the most efficient known classes of codes.

The essential parameters of codes are alphabet, length, cardinality (or dimension for linear codes), minimum distance and covering radius. Since covering radius is our main interest, its detailed study is postponed to subsequent chapters!

There are several methods to construct new codes from given ones. We present a few of them, in their binary version. Assume that  $C$  is an  $(n, K, d)$  or  $[n, k, d]$  code.

**Shortening:** For a linear code, choose one coordinate and take the subcode of  $C$  consisting of the codewords having 0 in this position. Deleting the chosen coordinate in every codeword of the subcode gives a linear code  $C^\circ$  with parameters  $[n-1, \geq k-1, \geq d]$ . For a nonlinear code, pick the largest of the two subcodes of  $C$  with either 0 or 1 in this coordinate. The resulting code  $C^\circ$  is an  $(n-1, \geq \lceil K/2 \rceil, \geq d)$  code.

**Puncturing:** If  $d \geq 2$ , deleting one coordinate gives an  $(n-1, K, \geq d-1)$  or  $[n-1, k, \geq d-1]$  code  $C^*$ .

**Extending:** For  $d$  odd, adding the overall parity check (sum modulo 2 of all the symbols) to every codeword results in the code  $\widehat{C}$  having parameters  $(n+1, K, d+1)$  or  $[n+1, k, d+1]$ .

Now we consider several essential classes of error-correcting codes. All these codes are binary or presented in their binary form, except the Reed-Solomon and the ternary Golay codes. In what follows,  $q = 2^m$ , except for the Reed-Solomon codes where  $q = p^m$ ,  $p$  prime.

**Cyclic codes:** A binary linear code  $C$  of length  $n$  is *cyclic* if for every  $\mathbf{c} = (c_0, c_1, \dots, c_{n-1}) \in C$ , the vector  $(c_{n-1}, c_0, \dots, c_{n-2})$  is also a codeword. In what follows we identify the vector  $\mathbf{a} = (a_0, a_1, \dots, a_{n-1})$  and the polynomial in  $\mathbb{F}[x]$   $a(x) = a_0 + a_1x + \dots + a_{n-1}x^{n-1}$ .

**The primitive case:** Assume that  $n = q - 1$  and  $\alpha$  is a primitive element of the field  $\mathbb{F}_q$ . Remember that two elements  $\alpha$  and  $\beta$  in  $\mathbb{F}_q$  are *conjugates* if for some integer  $\ell$ ,  $\alpha = \beta^{2^\ell}$ . Pick a subset  $\mathbb{N} = \{\alpha^{i_1}, \alpha^{i_2}, \dots, \alpha^{i_s}\}$  of  $\mathbb{F}_q$  not containing two conjugate elements.

Then all the binary polynomials of degree at most  $q - 2$  whose set of roots contains  $\aleph$  (and the conjugates of elements in  $\aleph$ ), constitute a *primitive cyclic code*. To see that the code is cyclic, notice that the polynomial  $x^n - 1$  has all nonzero elements of  $\mathbb{F}_q$  as its roots, and so  $xc(x) \pmod{x^n - 1}$  has the same set of nonzero roots as  $c(x)$ . But  $xc(x) \pmod{x^n - 1}$  is the cyclic shift of  $c(x)$ .

By definition, the cyclic code  $C$  consists of all binary words  $\mathbf{c}$  of length  $n = q - 1$  satisfying  $\mathbf{H}\mathbf{c}^T = \mathbf{0}$ , where

$$\mathbf{H} = \begin{pmatrix} 1 & \alpha^{i_1} & \alpha^{2i_1} & \dots & \alpha^{(n-1)i_1} \\ 1 & \alpha^{i_2} & \alpha^{2i_2} & \dots & \alpha^{(n-1)i_2} \\ \vdots & \dots & \dots & \dots & \dots \\ 1 & \alpha^{i_s} & \alpha^{2i_s} & \dots & \alpha^{(n-1)i_s} \end{pmatrix}. \quad (2.6.1)$$

The matrix  $\mathbf{H}$  is called a parity check matrix over  $\mathbb{F}_q$ . To obtain the binary parity check matrix, replace every element of  $\mathbb{F}_q$  by the corresponding binary column vector of size  $m$ . The length of the code is thus  $n = 2^m - 1$ , and its dimension is at least  $n - ms$  (the rows of  $\mathbf{H}$  may be dependent!). The problem of estimating the minimum distance is difficult in general, but, as we shall see later, easy for some particular choices of  $\aleph$ .

**The nonprimitive case:** Let  $\beta'$  be a nonprimitive element of  $\mathbb{F}_q$ . Then  $\beta'$  is conjugate to  $\beta = \alpha^h$  for some factor  $h$  of  $q - 1$ ,  $h > 1$ , where  $\alpha$  is a suitable primitive element and

$$\beta^{(q-1)/h} = 1.$$

Let all the degrees of  $\alpha$  in  $\aleph$  be multiples of  $h$ ,

$$\begin{aligned} \aleph &= \{\alpha^{hi_1}, \alpha^{hi_2}, \dots, \alpha^{hi_s}\} \\ &= \{\beta^{i_1}, \beta^{i_2}, \dots, \beta^{i_s}\}. \end{aligned}$$

Then the matrix

$$\mathbf{H}(C) = \begin{pmatrix} 1 & \beta^{i_1} & \beta^{2i_1} & \dots & \beta^{(n-1)i_1} \\ 1 & \beta^{i_2} & \beta^{2i_2} & \dots & \beta^{(n-1)i_2} \\ \vdots & \dots & \dots & \dots & \dots \\ 1 & \beta^{i_s} & \beta^{2i_s} & \dots & \beta^{(n-1)i_s} \end{pmatrix} \quad (2.6.2)$$

where  $n = (2^m - 1)/h$ , defines a *nonprimitive cyclic code*. It has length  $n$  and dimension  $k \geq n - ms$ .

**Hamming codes:** The parity check matrix of the *Hamming code*  $\mathcal{H}_m$  consists of all nonzero columns of size  $m$  in some order. The parameters of  $\mathcal{H}_m$  are

$$[n = 2^m - 1, k = 2^m - m - 1, d = 3].$$

The codes  $\mathcal{H}_m$  are perfect. If we define  $\aleph = \{\alpha\}$ , for some primitive  $\alpha \in \mathbb{F}_q$ , then we get the Hamming codes in a cyclic form.

The *extended Hamming codes* have parameters

$$[n = 2^m, k = 2^m - m - 1, d = 4],$$

the *shortened Hamming codes* have parameters

$$[n, k = n - \lfloor \log_2 n \rfloor - 1, d = 3],$$

and the *extended shortened Hamming codes* are

$$[n + 1, k = n - \lfloor \log_2 n \rfloor - 1, d = 4]$$

codes. All these codes have the largest minimum distance among linear codes with the same length and dimension.

**Reed-Muller codes:** The *Reed-Muller code*  $\mathcal{RM}(r, m)$  of order  $r$ ,  $r = 0, 1, \dots, m$ , has parameters

$$[n = 2^m, k = \sum_{i=0}^r \binom{m}{i}, d = 2^{m-r}].$$

For a definition, see Section 9.1. The dual code of  $\mathcal{RM}(r, m)$  is  $\mathcal{RM}(m - r - 1, m)$ . The Reed-Muller codes constitute a family of nested codes, namely,

$$\mathcal{RM}(0, m) \subset \mathcal{RM}(1, m) \subset \dots \subset \mathcal{RM}(m, m).$$

Particular cases of Reed-Muller codes coincide with some of aforementioned codes:

$\mathcal{RM}(0, m)$  is the repetition  $[2^m, 1, 2^m]$  code;

$\mathcal{RM}(m - 2, m)$  is the extended Hamming code;

$\mathcal{RM}(m - 1, m)$  is the even weight  $[2^m, 2^m - 1, 2]$  code;

$\mathcal{RM}(m, m)$  is the  $[2^m, 2^m, 1]$  code consisting of all possible words of length  $2^m$ .

**First order Reed-Muller codes:** The codes  $\mathcal{RM}(1, m)$  form a class of codes having parameters

$$[n = 2^m, k = m + 1, d = 2^{m-1}].$$

These codes contain 0, 1 and  $2^{m+1} - 2$  codewords of weight  $2^{m-1}$ .

**Punctured Reed-Muller codes:** The code  $\mathcal{RM}^*(r, m)$  can be presented in a cyclic form. The set of zeros  $\mathbb{N}$  consists of all  $\alpha^i$ ,  $1 \leq i \leq 2^m - 2$ , such that  $w_2(i)$ , the number of ones in the binary expansion of  $i$ , satisfies the inequality

$$1 \leq w_2(i) \leq m - r - 1.$$

The parameters of  $\mathcal{RM}^*(r, m)$  are

$$[n = 2^m - 1, k = \sum_{i=0}^r \binom{m}{i}, d = 2^{m-r} - 1].$$

**Simplex codes:** The *simplex codes*  $\mathcal{SIM}_m$  can be obtained by shortening the code  $\mathcal{RM}(1, m)$ , and have parameters

$$[n = 2^m - 1, k = m, d = 2^{m-1}].$$

All nonzero codewords in  $\mathcal{SIM}_m$  have the same weight  $2^{m-1}$ . These are cyclic codes with

$$\mathbb{N} = \mathbb{F}_q^* \setminus \{\alpha^1, \alpha^2, \alpha^4, \dots\}.$$

The codes  $\mathcal{SIM}_m$  are the duals of the Hamming codes  $\mathcal{H}_m$  and have generator matrices consisting of all the nonzero columns of size  $m$ .

**Primitive BCH codes:** The (narrow-sense) *primitive BCH codes*  $\mathcal{BCH}(e, m)$  are cyclic codes with

$$\mathbb{N} = \{\alpha^1, \alpha^3, \dots, \alpha^{2e-1}\}.$$

Their parameters are

$$[n = 2^m - 1, k \geq n - me, d \geq 2e + 1].$$

The BCH codes constitute a nested family of codes:

$$\mathcal{BCH}(e + 1, m) \subseteq \mathcal{BCH}(e, m).$$

The BCH codes contain punctured Reed-Muller codes as subcodes, namely, for every  $e \leq 2^i - 1$

$$\mathcal{RM}^*(m - i - 1, m) \subseteq \mathcal{BCH}(e, m).$$

If  $2e - 2 < 2^{\lceil m/2 \rceil}$ , then the dimension of  $\mathcal{BCH}(e, m)$  is exactly  $n - me$ .

**Nonprimitive BCH codes:** If  $n = (2^m - 1)/h$  and  $\beta$  is an  $n$ -th root of unity in  $\mathbb{F}_q$ , then a (narrow-sense) *nonprimitive BCH code*  $\mathcal{BCH}_h(e, m)$  is defined

as a nonprimitive cyclic code with  $\mathbb{N} = \{\beta^1, \beta^3, \dots, \beta^{2e-1}\}$ . Its parameters are

$$[n = (2^m - 1)/h, k \geq n - me, d \geq 2e + 1].$$

**Duals of BCH codes:** Let  $\alpha \in \mathbb{F}_q$  be a primitive element. Then  $\mathcal{BCH}^\perp(e, m)$  consists of all vectors

$$(Tr(f(0)), Tr(f(1)), Tr(f(\alpha)), \dots, Tr(f(\alpha^{q-2}))),$$

where  $f(x) \in \mathbb{F}_q[x]$  is of the form

$$f(x) = a_1x + a_2x^3 + \dots + a_ex^{2e-1}.$$

The minimum distance of  $\mathcal{BCH}^\perp(e, m)$  can be estimated by using the Carlitz-Uchiyama bound, namely,

$$d(\mathcal{BCH}^\perp(e, m)) \geq 2^{m-1} - (e-1)2^{m/2}.$$

**Reed-Solomon codes:** These are  $q$ -ary codes, with  $q = p^m$ ,  $p$  prime. One way of defining the *Reed-Solomon code*  $\mathcal{RS}(k, q)$  is by its polynomial representation: for every  $q$ ,  $\mathcal{RS}(k, q)$  consists of vectors

$$(f(1), f(\alpha), f(\alpha^2), \dots, f(\alpha^{q-2})),$$

where  $f(x) \in \mathbb{F}_q[x]$  runs through all polynomials of degree at most  $k-1$ . This code has parameters

$$[n = q - 1, k, d = n - k + 1]_q.$$

If we add an extra coordinate containing  $f(0)$ , we get the *extended Reed-Solomon code* with parameters

$$[n = q, k, d = n - k + 1]_q.$$

It is possible to further extend the Reed-Solomon code, thus getting the *doubly extended Reed-Solomon code* with parameters

$$[n = q + 1, k, d = n - k + 1]_q.$$

If  $q = 2^m$ , there exist *triply extended Reed-Solomon codes* with parameters

$$[n = q + 2, k = 3, d = q]_q,$$

and

$$[n = q + 2, k = q - 1, d = 4]_q.$$

For every  $n < q-1$ , there exist *shortened Reed-Solomon codes* with parameters

$$[n, k, d = n - k + 1]_q.$$

All these codes achieve maximum possible minimum distance for given length and size by the Singleton bound:

**Theorem 2.6.3 (Singleton bound)** *For every  $(n, K, d)_q$  code,*

$$d \leq n - \log_q K + 1.$$

**Proof.** Puncturing an  $(n, K, d)_q$  code  $d-1$  times yields a code of length  $n-d+1$ , minimum distance at least one and cardinality  $K$ .  $\square$

Codes achieving the Singleton bound are called *maximum distance separable* (MDS), so the Reed-Solomon codes are MDS.

The Reed-Solomon and extended Reed-Solomon codes constitute a nested family of codes, namely,

$$\mathcal{RS}(k, q) \subset \mathcal{RS}(k+1, q).$$

**Quadratic residue codes:** The *quadratic residue code*  $\mathcal{QR}(p)$  is a cyclic code of length  $p = 8m \pm 1$ , where  $p$  is a prime. Pick a minimal field of characteristic 2 containing a  $p$ -th root of unity, say  $\alpha$ . Then choose

$$\aleph = \{\alpha^i : \text{there exists } x \in \mathbb{Z}_p \text{ such that } x^2 = i \pmod{p}\}.$$

The  $\mathcal{QR}(p)$  codes have parameters

$$[n = p, k = \frac{1}{2}(p+1), d \geq \sqrt{p}].$$

**Self-dual codes:** A binary linear code  $C$  is called *self-dual* if  $C = C^\perp$ . Such codes have even lengths and parameters  $[n, n/2, d]$ . If all the weights of a self-dual code  $C$  are divisible by 4, then it is called a self-dual code of *Type II*, otherwise of *Type I*. Codes of Type II, also called *doubly-even* self-dual codes, have lengths that are multiples of 8.

**Goppa codes:** Let  $g(x) \in \mathbb{F}_q[x]$  be a polynomial of degree  $e$  with no multiple zeros. Denote by  $L$  the subset  $\{\alpha_1, \alpha_2, \dots, \alpha_n\}$  of  $\mathbb{F}_q$  consisting of the nonzeros of  $g(x)$ . Then the *Goppa code*  $\mathcal{GOP}(L, g)$  with parameters

$$[n, k \geq n - me, d \geq 2e + 1],$$

consists of the codewords  $(a_1, a_2, \dots, a_n)$  satisfying

$$\sum_{i=1}^n \frac{a_i}{x - \alpha_i} \equiv 0 \pmod{g(x)}.$$

A parity check matrix of  $\mathcal{GOP}(L, g)$  is

$$\mathbf{H} = \begin{pmatrix} 1/g(\alpha_1) & 1/g(\alpha_2) & \dots & 1/g(\alpha_n) \\ \alpha_1/g(\alpha_1) & \alpha_2/g(\alpha_2) & \dots & \alpha_n/g(\alpha_n) \\ \dots & \dots & \dots & \dots \\ \alpha_1^{e-1}/g(\alpha_1) & \alpha_2^{e-1}/g(\alpha_2) & \dots & \alpha_n^{e-1}/g(\alpha_n) \end{pmatrix}. \quad (2.6.4)$$

If  $g(x)$  is irreducible then the code is called an *irreducible Goppa code*. Since  $g(x)$  in this case has no zeros in  $\mathbb{F}_q$ , we may take  $L = \mathbb{F}_q$ , thus getting codes with parameters

$$[n = 2^m, k \geq n - me, d \geq 2e + 1].$$

**Golay codes:** These are perfect binary  $[23, 12, 7]$  and ternary  $[11, 6, 5]_3$  codes. They are nonprimitive cyclic codes. For example, the binary Golay code is defined by picking a 23-rd root of unity  $\beta$  in  $\mathbb{F}_{2^{11}}$ . Then we may choose  $\aleph = \{\beta\}$  to get the cyclic Golay code. The binary Golay code is also a quadratic residue code. The extended Golay code is self-dual.

Some nonlinear codes have better parameters than any linear codes. We describe three such classes.

**Hadamard codes:** A  $\pm 1$ -matrix  $\mathbf{H}_n^\pm$  is a *Hadamard  $n \times n$  matrix* if

$$\mathbf{H}_n^\pm (\mathbf{H}_n^\pm)^T = n \mathbf{I}_n.$$

Hadamard matrices conjecturally exist for every  $n$  being a multiple of 4.

A *Hadamard code*  $\mathcal{HD}_n$  consists of the rows of  $\mathbf{H}_n^\pm$  and their complements after substitutions  $1 \rightarrow 0$  and  $-1 \rightarrow 1$ . The parameters of  $\mathcal{HD}_n$  are

$$(n, K = 2n, d = n/2).$$

The code  $\mathcal{RM}(1, m)$  is a Hadamard code for  $n = 2^m$  (see Section 9.1, where we use the Kronecker power of  $\mathbf{H}_2^\pm$ ). We define here  $\mathbf{A} \otimes \mathbf{B}$ , the *Kronecker product* of two square matrices  $\mathbf{A} = (a_{i,j})$  and  $\mathbf{B}$  of dimension  $n_A$  and  $n_B$ , respectively:  $\mathbf{A} \otimes \mathbf{B}$  is the square matrix of dimension  $n_A n_B$  obtained from  $\mathbf{A}$  by replacing every entry  $a_{i,j}$  by  $a_{i,j} \mathbf{B}$ .

**Preparata codes:** Assume that  $m \geq 4$  is even. The *Preparata code*  $\mathcal{P}_m$  has parameters

$$(n = 2^m, K = 2^{n-2m}, d = 6).$$

The *punctured Preparata code*  $\mathcal{P}_m^*$  is an  $(n = 2^m - 1, K = 2^{n-2m+1}, d = 5)$  code. The following result turns out to be useful in constructing coverings.

**Theorem 2.6.5** *The Hamming code  $\mathcal{H}_m$  is a partition of  $2^{m-1}$  cosets of the punctured Preparata code  $\mathcal{P}_m^*$ .*  $\square$

**Nordstrom-Robinson code:** The code  $\mathcal{P}_4$  is called the *Nordstrom-Robinson code*  $\mathcal{NR}$ , and has parameters  $(16, 2^8, 6)$ . The union of eight cosets of  $\mathcal{NR}$  constitutes the extended Hamming  $[16, 11, 4]$  code.

**Goethals codes:** Assume that  $m \geq 6$  is even. The *Goethals code*  $\mathcal{GOE}_m$  has parameters

$$(n = 2^m, K = 2^{n-3m+1}, d = 8).$$

We have described some very efficient families of error-correcting codes. There are also many other ways of constructing good codes. In Tables 2.2 and 2.3 we summarize the current knowledge about the parameters of best known error-correcting codes of small lengths. Along with constructive existence bounds, the tables also give nonexistence bounds restricting our expectations on possible further improvements of known constructions.

## 2.7 Designs, constant weight codes, graphs

Codes are in a natural way connected to many combinatorial objects, like designs.

**Definition 2.7.1** *A collection  $\mathcal{D}$  of distinct  $k$ -subsets, called blocks, of the set  $S = \{1, 2, \dots, v\}$  is called a  $t$ -( $v, k, \lambda$ ) design if every  $t$ -subset of  $S$  is contained in exactly  $\lambda$  blocks.*

**Definition 2.7.2** *A  $t$ -( $v, k, 1$ ) design is called a Steiner system and is denoted by  $S(t, k, v)$ .*

For given  $t, v, k, \lambda$ , there may not exist any  $t$ -( $v, k, \lambda$ ) design. It is then natural to require that each  $t$ -subset is contained in *at least*  $\lambda$  blocks.

**Definition 2.7.3** *A collection  $\mathcal{D}$  of  $k$ -subsets, called blocks, of the set  $S = \{1, 2, \dots, v\}$  is called a  $t$ -( $v, k, \lambda$ ) covering design if every  $t$ -subset of  $S$  is contained in *at least*  $\lambda$  blocks.*

In particular, a covering design with  $t = 2$  is called a *pair covering design*. A lower bound on the minimal cardinality  $F(v, k)$  of a  $2$ -( $v, k, 1$ ) covering design is given by the Schönheim bound

$$F(v, k) \geq L(v, k) := \lceil \frac{v}{k} \lceil \frac{v-1}{k-1} \rceil \rceil.$$

Table 2.2: Upper and lower bounds on  $A(n, d)$ .

$n$	$d = 4$	$d = 6$	$d = 8$	$d = 10$
6	4	2	1	1
7	8	2	1	1
8	16	2	2	1
9	20	4	2	1
10	40	6	2	2
11	72–76	12	2	2
12	144–152	24	4	2
13	256	32	4	2
14	512	64	8	2
15	1024	128	16	4
16	2048	256	32	4
17	2720–3276	256–340	36–37	6
18	5312–6552	512–680	64–72	10
19	10496–13104	1024–1288	128–144	20
20	20480–26208	2048–2372	256–279	40
21	36864–43690	2560–4096	512	42–48
22	73728–87380	4096–6942	1024	48–88
23	147456–173784	8192–13774	2048	68–150
24	294912–344636	16384–24106	4096	128–280

$$A(n, 2) = 2^{n-1};$$

$$A(n, d) = A(n+1, d+1) \text{ for } d \text{ odd.}$$

Table 2.3: Upper and lower bounds on  $a[n, d]$ .

$n$	$d = 6$	$d = 8$	$d = 10$
6	1	0	0
7	1	0	0
8	1	1	0
9	2	1	0
10	2	1	1
11	3	1	1
12	4	2	1
13	4	2	1
14	5	3	1
15	6	4	2
16	7	5	2
17	8	5	2
18	9	6	3
19	9	7	3
20	10	8	4
21	11	9	5
22	12	10	5
23	13	11	6
24	14	12	7
25	14	12	7
26	15	12	8
27	16	13	9
28	17	14	10
29	18	14–15	10–11
30	19	15–16	11–12
31	20	16–17	12–13
32	21	17–18	13–14

$a[n+1, 4] = n-1 - \lfloor \log_2 n \rfloor$  (achieved by extended shortened Hamming codes);  
 $a[n, d] = a[n+1, d+1]$  for  $d$  odd.

Indeed, assume that  $\mathcal{D}$  is a  $2-(v, k, 1)$  covering design consisting of some  $k$ -subsets of the set  $\{1, 2, \dots, v\}$ , and count in two ways the number of pairs  $(i, B)$  such that  $1 \leq i \leq v$ ,  $B \in \mathcal{D}$ ,  $i \in B$ . For a fixed  $B$ , there are  $k$  such pairs. For a fixed  $i$ , there are at least  $\lceil (v-1)/(k-1) \rceil$  such pairs. Therefore  $|\mathcal{D}|k \geq v\lceil (v-1)/(k-1) \rceil$ , proving the bound.

Several families of exact values are known:

- Fort and Hedlund [240] have shown that  $F(v, 3) = L(v, 3)$  for all  $v \geq 3$ .
- Mills [485], [486] has shown that

$$F(v, 4) = \begin{cases} L(v, 4), & \text{if } v \geq 4, v \neq 7, 9, 10, 19, \\ L(v, 4) + 1 & \text{if } v = 7, 9, 10, \\ L(v, 4) + 2 & \text{if } v = 19. \end{cases}$$

- The values of  $F(v, k)$  are known for  $v \leq 3k$ ; see Mills [487].

A code is called a *constant weight code* if all its codewords have the same weight  $w$ . For tables of the best currently known error-correcting constant weight codes, see Brouwer, Shearer, Sloane and W. D. Smith [95]. In the context of covering codes it is natural to study binary constant weight codes of length  $n$  and constant weight  $w$  such that every binary vector of weight  $u$  is within Hamming distance  $d$  from at least one codeword. The minimal cardinality of such a code is denoted by  $K(n, w, u, d)$ . For a comprehensive study of such codes we refer to Etzion, Wei and Zhang [226]. When  $u < w$  and  $d = w - u$  this leads to the definition of a covering design with  $v = n$ ,  $k = w$ ,  $t = u$  and  $\lambda = 1$ . For the case  $u > w$  and  $d = u - w$ , see Section 19.5.

A *graph*  $\Gamma$  is a pair  $(V, E)$  where  $V$  is a finite set of *vertices* and  $E \subseteq \{\{u, v\} : u, v \in V, u \neq v\}$  is the set of *edges*. The *degree*  $d(v)$  of a vertex  $v$  is the number of vertices adjacent to  $v$ . If  $G$  is a graph with  $V = \{1, 2, \dots, n\}$ , its *adjacency matrix*  $\mathbf{A}$  is the  $n \times n$  matrix  $\mathbf{A} = (a_{ij})$  where  $a_{ij} = 1$  if  $\{i, j\} \in E$  and  $a_{ij} = 0$  otherwise. A *path* of length  $k$  from  $v_1 \in V$  to  $v_{k+1} \in V$  is a sequence  $v_1 v_2 \dots v_{k+1}$  where  $\{v_i, v_{i+1}\} \in E$  for all  $i = 1, 2, \dots, k$  and  $v_i \neq v_j$  whenever  $i \neq j$ . The *graphic distance* between two vertices is the length of the shortest path connecting them. The *chromatic number* of a graph is the minimal number of colours needed to colour the vertices in such a way that no two adjacent vertices have the same colour. The *independence number* of a graph is the maximal size of a subset of  $V$  such that no two vertices in the subset are adjacent.

A *hypergraph* is a pair  $(V, E)$  where  $V$  is a finite set of *vertices* and  $E \subseteq 2^V$  the elements of which are called *edges* or *hyperedges*. Here  $2^V$  denotes the set of all subsets of  $V$ . If every edge is of size  $b$ , the hypergraph is called *b-uniform*. For  $b = 2$ , the definition reduces to that of a graph. If every vertex belongs to the same number  $\Delta$  of edges,  $(V, E)$  is called  $\Delta$ -*regular*. A *transversal* is a set intersecting every hyperedge.

Table 2.4: Bounds on  $F(v, k)$ .

$v \setminus k$	3	4	5	6	7	8	9	10	11	12
3	1									
4	3	1								
5	4	3	1							
6	6	3	3	1						
7	7	5	3	3	1					
8	11	6	4	3	3	1				
9	12	8	5	3	3	3	1			
10	17	9	6	4	3	3	3	1		
11	19	11	7	6	4	3	3	3	1	
12	24	12	9	6	5	3	3	3	3	1
13	26	13	10	7	6	4	3	3	3	3
14	33	18	12	7	6	5	4	3	3	3
15	35	19	13	10	7	6	4	3	3	3
16	43	20	15	10	8	6	5	4	3	3
17	46	26	16	12	9	7	6	5	4	3
18	54	27	18	12	10	7	6	5	4	3
19	57	31	19	14–15	11	9	7	6	5	4
20	67	35	21	16	12	9	7	6	6	4
21	70	37	21	17	13	11	7	7	6	5
22	81	39	27	19	13	11	9	7	6	6
23	85	46	28	20–21	15–16	12	10	8	7	6
24	96	48	30	21–22	17	12	11	8	7	6
25	100	50	30	23	18	13	11	10	7	7
26	113	59	37	24	19–20	13	12	10	8	7
27	117	61	38	27	20	16–17	12	11	9	7
28	131	63	40–43	28	21–22	17–18	13–14	11	10	7
29	136	73	42–44	29–31	22–24	18	14	12	10	9
30	150	75	48	31	24–25	19	15	13	11	9
31	155	78	50	31	26	20	15–18	13	12	10
32	171	88	52–54	38	28–31	20	15–19	13–15	12	10

Table 2.4 has been obtained from Todorov [654], Mills and Mullin [489] and D. M. Gordon, Kuperberg and Patashnik [261], which the reader is referred to for detailed references.

## 2.8 Notes

§2.1 If we use a code for correcting errors, and always decode to the nearest codeword, the covering radius is the maximum weight of a correctable error pattern. Of course, there can be several nearest codewords, and we then have to choose one of them. The *Newton radius*, studied in Helleseth and Kløve [298] and Helleseth, Kløve and Levenshtein [299], is the largest weight of a *uniquely* decodable error. In the case when the Newton radius equals the covering radius, the code is said *uniquely decodable* (UD); see van Lint [438, 3.7.13] for an example. A study of UD codes can be found in Cohen, Rifá and Zémor [168], where the question is raised whether there exist linear binary UD codes apart from direct sums of perfect codes. For  $R = 1$ , UD codes are considered in Weichsel [683] under the name of perfect dominating sets.

Minkes [490] has written a covering radius extension of GUAVA, a share library package that implements coding theory algorithms. GUAVA is written in the computer algebra language GAP. It is distributed as a part of GAP through anonymous ftp from [samson.math.rwth-aachen.de](http://samson.math.rwth-aachen.de) (Internet number 137.226.152.6), directory /pub/gap/.

§2.2 The MacWilliams transform first appeared in MacWilliams [462]. For its generalizations see MacWilliams and Sloane [464, Chap. 5]. Theorem 2.2.7 is by Delsarte [194].

§2.3 Szegő [631] contains extensive information about general orthogonal polynomials. A nice introduction to Krawtchouk polynomials is in van Lint [438, §1.2], MacWilliams and Sloane [464, §5.7], and Nikiforov, Suslov and Uvarov [503]. For properties of Krawtchouk polynomials, see van Tilborg [651], Best [73], Bannai [46], Levenshtein [419], Krasikov and Litsyn [388]. Expression (2.3.30) is by Levenshtein [419], (2.3.32) by Levenshtein [417] and estimates by roots of Hermite polynomials are due to Szegő [631]. Integer roots of Krawtchouk polynomials have received a special attention due to their relation to several problems in combinatorics, e.g., the existence of perfect codes, the graph reconstruction problem, etc. For further investigations, see Bannai [44], Best [73], L. Chihara and D. Stanton [136], Habsieger and D. Stanton [273], Krasikov and Litsyn [388]. Hong [307] proved that every nonbinary ( $q \geq 3$ ) Krawtchouk polynomial of degree greater than two has at least one noninteger root. Upper bounds on the absolute values of Krawtchouk polynomials, especially in a range close to  $n/2$ , are derived in Sidelnikov [584], Kasami, Fujiwara and Lin [367], Sharapudinov [582], Solé [601], Krasikov and Litsyn [387].

§2.4 Theorem 2.4.8 is from van Wee [675], cf. also Honkala [308] and Struik [628]. Theorem 2.4.10 is proved in van Wee [675] in the case  $d(\mathbf{c}'_1, \mathbf{c}'_2) = d(\mathbf{c}_1, \mathbf{c}_2)$ ,  $d(\mathbf{c}'_2, \mathbf{c}'_3) = d(\mathbf{c}_2, \mathbf{c}_3)$  and  $d(\mathbf{c}'_1, \mathbf{c}'_3) \equiv d(\mathbf{c}_1, \mathbf{c}_3) \pmod{2}$ , and in the

case  $r = s = t$  in Honkala [308]. There are also cases when equality holds in Theorem 2.4.10: for example, if  $r = s = t$  and  $\lceil d(\mathbf{c}_i, \mathbf{c}_j)/2 \rceil = \lceil d(\mathbf{c}'_i, \mathbf{c}'_j)/2 \rceil$  for all  $i, j$ ; see [308]. The number of points in a union of three spheres with the same radius is studied in [308].

In the nonbinary case, even the number of points in the intersection of three Hamming spheres is not determined by the pairwise distances between the centres: take, for instance,  $\mathbf{c}_1 = \mathbf{c}'_1 = 000000$ ,  $\mathbf{c}_2 = \mathbf{c}'_2 = 111100$ ,  $\mathbf{c}_3 = 110011$ ,  $\mathbf{c}'_3 = 222200$  and  $r = s = t = 2$ . Theorem 2.4.8 generalizes to the nonbinary case; see van Wee [680].

Theorem 2.4.14 was first proved by Slepian and Moore (see Peterson and Weldon [534]). The proof given here follows Cohen, Dornstetter and Godlewski [147].

Theorem 2.4.16 was conjectured by Erdős and proved by Kleitman [379].

**§2.5** Sources for finite fields are Berlekamp [68], Lidl and Niederreiter [424], MacWilliams and Sloane [464], McEliece [478], Menezes, Blake, Gao, Mullin, Vanstone and Yaghoobian [482], Shparlinski [583] and Schmidt [571].

**§2.6** Textbooks in coding theory are, e.g., Berlekamp [68], Blake and Mullin [83], van Lint [433], [438], MacWilliams and Sloane [464], Peterson and Weldon [534], Pless [542] and van Tilborg [653].

The  $q$ -ary Hamming codes are defined in Section 11.1. For more on the Golay codes, see also Section 11.1.

Table 2.2 is an update of Table II of Brouwer, Shearer, Sloane and W. D. Smith [95] (lower bounds) and Best, Brouwer, MacWilliams, Odlyzko and Sloane [75]. Table 2.3 is an extract of Brouwer and Verhoeff [96] (also available at Internet address <http://www.win.tue.nl/win/math/dw/voorlincod.html>), see for earlier results Verhoeff [672] and Helgert and Stinaff [293].

The updates to Table 2.2 are the following: van Pul [545] proved that  $A(18, 8) \leq 72$ ,  $A(21, 10) \leq 48$  and  $A(22, 10) \leq 88$ ; Klein, Litsyn and Vardy [378], see also Litsyn and Vardy [446], showed that  $A(11, 4) \leq 76$ ,  $A(12, 4) \leq 152$ .

As for the lower bounds, we were informed by Etzion (1991) on an improvement for  $A(18, 4)$ . The  $(17, 5312, 3)$  code is constructed in the following way. The vectors of length 10 and weight 5 can be partitioned into eight subcodes  $S_5(i)$ ,  $i = 0, 1, \dots, 7$ , of sizes 36, 36, 34, 34, 29, 29, 27, 27, such that every subcode has minimum distance four (see the partition  $\pi(10, 5)$  in the Appendix Table of Brouwer, Shearer, Sloane and W. D. Smith [95, p. 1366]). The vectors of length 10 and weight two can be partitioned into nine subcodes  $S_2(i)$ ,  $i = 0, 1, \dots, 8$ , of size five, each having minimum distance four.

Let  $S(i) = S_2(i) \cup S_5(i) \cup \overline{S}_2(i)$  for  $i = 0, 1, \dots, 7$ . Clearly  $d(S(i)) = 3$  and  $d(\cup S(i)) = 2$ . Let

$$\mathbb{F}^7 = \mathcal{H}_3(0) \cup \mathcal{H}_3(1) \cup \dots \cup \mathcal{H}_3(7)$$

be a partition of  $\mathbb{F}^7$  into the cosets of the Hamming code  $\mathcal{H}_3$ . Then

$$C = \{\mathbf{c} = (\mathbf{c}_1, \mathbf{c}_2) : \mathbf{c}_1 \in S(i), \mathbf{c}_2 \in \mathcal{H}_3(i), \text{ for } i = 0, 1, \dots, 7\}$$

is the claimed code.

In fact, the same construction had been used by Romanov [561] to construct a  $(16, 2720, 3)$  code, using seven subcodes of length 9 and size 24 defined by Steiner triple systems  $S(2, 3, 9)$  and their complements, and one subcode of size two consisting of  $1^9$  and  $0^9$ . It exploits the fact that 84 vectors of length 9 and weight three can be partitioned into seven subcodes, each of them being the incidence vectors of a Steiner system  $S(2, 3, 9)$ .

For tables of lower bounds on  $A(n, d)$  for  $n \leq 512$  and  $d \leq 30$ , see MacWilliams and Sloane [464] and Litsyn [442] (also available at Internet address <http://www.eng.tau.ac.il/litsyn/>).

**§2.7** The Schönheim bound given here is a special case of the general bound for covering designs; see [572]. For an excellent survey on covering designs, see Mills and Mullin [489].

On graphs and hypergraphs, see Berge [65] and [66].

This Page Intentionally Left Blank

# Chapter 3

# Constructions

In this and the next two chapters we discuss various methods of producing codes with small covering radius. Given the length and cardinality — or the dimension if the code is required to be linear — we want to find a code with covering radius as small as possible. Alternatively, we fix the length and the covering radius and wish to find a code with as small a number of codewords as possible.

We present several constructions that produce codes from scratch, e.g., the piecewise constant code method. There are also many techniques of combining known codes in an efficient way to build new, larger codes, e.g., the  $(u, u + v)$  construction.

We begin with some easy well-known constructions, like addition of a parity check bit, puncturing and direct sum, and discuss how they affect the covering radius. The piecewise constant code method provides codes with a simple, elegant structure which makes it easy to determine the covering radius. Section 3.4 describes variations on the  $(u, u + v)$  construction. We often choose one of the component codes in a particular way, e.g., so that it consists of all the vectors of given weights. The covering radius of a linear code can be found using its parity check matrix. The matrix construction gives us codes for which the covering radius can be found in a similar fashion. This construction is particularly suitable in connection with different computer search methods. Cascading is discussed in Section 3.6.

Constructions which are specific to the linear case are considered in Chapter 5.

Like in the whole book, the emphasis is on binary codes. However, many constructions work in the same way in the binary and nonbinary cases. Several interesting constructions that yield optimal nonbinary codes are studied in Section 3.7.

Many good covering codes have been found using computer search meth-

ods, and we have included a section about local search techniques, in particular simulated annealing and taboo search.

The amalgamated direct sum construction and normality, as well as the blockwise direct sum construction, are discussed in the next chapter.

Lower bounds are studied and tables of the best known lower and upper bounds are given in Chapters 6 and 7 for nonlinear and linear codes, respectively.

### 3.1 Puncturing and adding a parity check bit

One of the simplest constructions is puncturing.

**Theorem 3.1.1** *If  $C$  is an  $(n, K)_q R$  code, then the punctured code  $C^* = \{(c_1, c_2, \dots, c_{n-1}) : (c_1, c_2, \dots, c_n) \in C\}$  has covering radius  $R - 1$  or  $R$ .*  $\square$

**Example 3.1.2** It is not difficult to verify that the binary code  $C = \{10001, 01111, 00000, 11110\}$  has covering radius 2. Puncturing the last coordinate gives the code  $C^* = \{1000, 0111, 0000, 1111\}$  with covering radius 1. If we further puncture the last coordinate of  $C^*$  we obtain the code  $\{100, 011, 000, 111\}$  which still has covering radius 1.  $\square$

If we add a parity check  $-\sum_{i=1}^n c_i$  to each codeword  $\mathbf{c} = (c_1, c_2, \dots, c_n)$  of a  $q$ -ary code, the covering radius remains the same or increases by one. For binary codes we denote the parity check bit by

$$\pi(\mathbf{c}) = \begin{cases} 0 & \text{if } w(\mathbf{c}) \text{ is even,} \\ 1 & \text{if } w(\mathbf{c}) \text{ is odd.} \end{cases}$$

Adding a parity check bit to a binary code always increases the covering radius by one.

**Theorem 3.1.3** *If a binary code  $C$  has covering radius  $R$ , then the extended code  $\widehat{C} = \{(\mathbf{c}, \pi(\mathbf{c})) : \mathbf{c} \in C\}$  has covering radius  $R + 1$ .*

**Proof.** Let  $\mathbf{x}$  be a vector such that  $d(\mathbf{x}, C) = R$ . If  $R$  is even (respectively, odd), then for every  $\mathbf{c} \in C$  such that  $d(\mathbf{x}, \mathbf{c}) = R$ , the integers  $w(\mathbf{x})$  and  $w(\mathbf{c})$  have the same (respectively, opposite) parity, because  $R = w(\mathbf{c} + \mathbf{x}) = w(\mathbf{c}) + w(\mathbf{x}) - 2w(\mathbf{x} * \mathbf{c})$ . Therefore  $d((\mathbf{x}, \pi(\mathbf{x}) + 1), \widehat{C}) = R + 1$  (respectively,  $d((\mathbf{x}, \pi(\mathbf{x})), \widehat{C}) = R + 1$ ).  $\square$

In particular, if we puncture a binary even weight code the covering radius decreases by one.

**Example 3.1.4** If  $C$  is a binary code of length  $n$ , and  $C' = \{(c_1 + c_2 + \dots + c_n, c_2, c_3, \dots, c_n) : (c_1, c_2, \dots, c_n) \in C\}$ , then  $C$  and  $C'$  have the same covering radius, because they have equivalent extended codes.  $\square$

## 3.2 Direct sum

One of the most basic constructions is the direct sum.

**Theorem 3.2.1** *Assume that  $C_1$  has covering radius  $R_1$  and  $C_2$  has covering radius  $R_2$ . Then their direct sum*

$$C_1 \oplus C_2 = \{(\mathbf{c}_1, \mathbf{c}_2) : \mathbf{c}_1 \in C_1, \mathbf{c}_2 \in C_2\}$$

*has covering radius  $R_1 + R_2$ .*

**Proof.** The result is immediate because  $d((\mathbf{x}, \mathbf{y}), C_1 \oplus C_2) = d(\mathbf{x}, C_1) + d(\mathbf{y}, C_2)$ .  $\square$

If  $C_1$  and  $C_2$  are linear, so is  $C_1 \oplus C_2$ . The previous theorem leads to a number of simple formulas for the covering radius functions, like the following ones obtained by choosing  $C_2 = \{0, 1\}$ .

**Corollary 3.2.2**  $K(n+1, R) \leq 2K(n, R)$ .  $\square$

**Corollary 3.2.3**  $t[n+1, k+1] \leq t[n, k]$ .  $\square$

It is an open problem whether  $K(n+2, R+1) \leq K(n, R)$  for all  $R \neq n$ . Similarly for linear codes, it is not known if  $k[n+2, R+1] \leq k[n, R]$  holds for all  $R \neq n$ . We shall discuss these inequalities again in Chapter 4. Using the direct sum construction we can show that both inequalities hold if  $R$  is fixed and  $n$  is large enough.

**Theorem 3.2.4** *For fixed  $R$  there is a constant  $n(R)$  such that*

$$K(n+2, R+1) \leq K(n, R)$$

*and*

$$k[n+2, R+1] \leq k[n, R]$$

*for all  $n \geq n(R)$ .*

**Proof.** Assume that  $R$  is fixed. By the sphere-covering bound

$$2^{k[n,R]} \geq K(n, R) \geq \frac{2^n}{\sum_{i=0}^R \binom{n}{i}}$$

and

$$2^{k[n+2,R+1]} \geq K(n+2, R+1).$$

It is therefore sufficient to show that for large  $n$

$$2^{n-k[n+2,R+1]} \geq \sum_{i=0}^R \binom{n}{i}.$$

Choose an integer  $m$  such that  $2^m \leq (n+2)/(R+1) < 2^{m+1}$ , and form the direct sum

$$C = \mathcal{H}_m \oplus \mathcal{H}_m \oplus \dots \oplus \mathcal{H}_m \oplus \mathbb{F}^{n+2-(R+1)(2^m-1)},$$

where the  $[2^m - 1, 2^m - 1 - m]1$  Hamming code  $\mathcal{H}_m$  occurs  $R+1$  times. The resulting code  $C$  is an  $[n+2, n+2-(R+1)m]R+1$  code. Therefore

$$2^{n-k[n+2,R+1]} \geq 2^{(R+1)m-2} > \frac{1}{4} \left( \frac{n+2}{2R+2} \right)^{R+1} \geq \sum_{i=0}^R \binom{n}{i},$$

when  $n$  is large enough.  $\square$

### 3.3 Piecewise constant codes

Partition the length  $n$  as  $n = n_1 + n_2 + \dots + n_t$ , and partition each codeword  $\mathbf{c}$  in the same way, as  $\mathbf{c} = (\mathbf{c}_1, \mathbf{c}_2, \dots, \mathbf{c}_t)$ , where the length of  $\mathbf{c}_i$  is  $n_i$ . The code  $C$  is a *piecewise constant code* if it has the following property: if  $C$  contains any vector with

$$w(\mathbf{c}_1) = w_1, w(\mathbf{c}_2) = w_2, \dots, w(\mathbf{c}_t) = w_t,$$

then it contains all such vectors.

**Example 3.3.1** Figure 3.1 shows a piecewise constant code of length 5 corresponding to the partition  $5 = 2 + 3$ .

00	000
00	111
10	000
01	000
11	011
11	101
11	110

Figure 3.1: A  $(5, 7)1$  piecewise constant code.

		$w_2$				
		0	1	2	3	
		0	(1)	3	3	(1)
$w_1$		1	(2)	6	6	2
		2	1	3	(3)	1

Figure 3.2: Two-dimensional representation of the above  $(5, 7)1$  piecewise constant code.

The code consists of seven codewords corresponding to the weights  $(w_1, w_2) = (0, 0), (0, 3), (1, 0), (2, 2)$ . In fact, this is the same code as in (1.1.3) except that the last three coordinates have been complemented.

Any piecewise constant code of length 5 partitioned as  $5 = 2 + 3$  can be represented by a subset of the two-dimensional 3 by 4 array of cells shown in Figure 3.2. The cell  $(i, j)$  represents all the vectors with  $(w_1, w_2) = (i, j)$  and the number in the cell gives the number of such words in  $\mathbb{F}^5$ . The circled entries represent the code in the previous figure.

In general a piecewise constant code of length  $n = n_1 + \dots + n_t$  can be illustrated by a similar  $t$ -dimensional array. The *Manhattan distance* between two cells  $(w_1, \dots, w_t)$  and  $(w'_1, \dots, w'_t)$  is  $|w_1 - w'_1| + \dots + |w_t - w'_t|$ . The covering radius of the code is easy to check: it is the smallest Manhattan distance between any cell and the code.

The code in Figure 3.1 is optimal; see Example 1.1.1. □

**Example 3.3.2** The code of length  $3 + 3$  represented by Figure 3.3 is a  $(6, 12)1$  code. It is optimal, cf. Table 6.1. □

		$w_2$			
		0	1	2	3
		0	1	2	3
$w_1$	0	1	(3)	3	1
	1	3	9	9	(3)
	2	(3)	9	9	3
		3	1	3	(3)
					1

Figure 3.3: Two-dimensional representation of a  $(6, 12)1$  piecewise constant code.

In the final example of this section we use both a Steiner system and a piecewise constant code.

**Example 3.3.3** We construct an  $(11, 192)1$  code. Take first as codewords the 66 blocks of the Steiner system  $S(4, 5, 11)$  and their complements, i.e., the blocks of the Steiner system  $S(5, 6, 12)$  with one coordinate deleted. These 132 words cover all the vectors in  $\mathbb{F}^{11}$  of weight 4, 5, 6 and 7. To cover the vectors of the remaining weights we use a piecewise constant code. Partition the length as  $11 = 5 + 6$  and take as codewords all vectors  $(\mathbf{c}_1, \mathbf{c}_2)$ , where  $\mathbf{c}_1 \in \mathbb{F}^5$  and  $\mathbf{c}_2 \in \mathbb{F}^6$ , such that  $(w(\mathbf{c}_1), w(\mathbf{c}_2))$  is  $(1, 0)$ ,  $(2, 0)$  or  $(0, 2)$ , and their complements. These 60 new codewords cover all the vectors in  $\mathbb{F}^{11}$  of weight less than 4 or greater than 7.  $\square$

### 3.4 Variations on the $(\mathbf{u}, \mathbf{u} + \mathbf{v})$ construction

A useful alternative to the direct sum is provided by the  $(\mathbf{u}, \mathbf{u} + \mathbf{v})$  construction.

**Theorem 3.4.1** Assume that  $C_1 \subseteq \mathbb{Z}_q^n$  has covering radius  $R_1$  and  $C_2 \subseteq \mathbb{Z}_q^n$  has covering radius  $R_2$ . Then the code  $\{(\mathbf{u}, \mathbf{u} + \mathbf{v}) : \mathbf{u} \in C_1, \mathbf{v} \in C_2\}$  has covering radius at most  $R_1 + R_2$ .

**Proof.** Given any  $(\mathbf{a}, \mathbf{b}) \in \mathbb{Z}_q^{2n}$ , we can choose a codeword  $\mathbf{u} \in C_1$  such that  $d(\mathbf{u}, \mathbf{a}) \leq R_1$  and a codeword  $\mathbf{v} \in C_2$  such that  $d(\mathbf{v}, \mathbf{b} - \mathbf{u}) \leq R_2$ . Then  $d((\mathbf{u}, \mathbf{u} + \mathbf{v}), (\mathbf{a}, \mathbf{b})) = d(\mathbf{u}, \mathbf{a}) + d(\mathbf{v}, \mathbf{b} - \mathbf{u}) \leq R_1 + R_2$ .  $\square$

In exactly the same way we can prove the following generalization.

**Theorem 3.4.2** Assume that  $C_1 \subseteq \mathbb{Z}_q^{n_1}$  has covering radius  $R_1$ ,  $C_2 \subseteq \mathbb{Z}_q^{n_2}$  has covering radius  $R_2$ , and  $f : \mathbb{Z}_q^{n_1} \rightarrow \mathbb{Z}_q^{n_2}$  is any function. Then the code  $\{(\mathbf{u}, f(\mathbf{u}) + \mathbf{v}) : \mathbf{u} \in C_1, \mathbf{v} \in C_2\}$  has covering radius at most  $R_1 + R_2$ .  $\square$

For instance, if  $n_1 \geq n_2$ , then the code

$$\{(\mathbf{u}_0, \mathbf{u}_1, \mathbf{u}_1 + \mathbf{v}) : \mathbf{u}_0 \in \mathbb{Z}_q^{n_1 - n_2}, (\mathbf{u}_0, \mathbf{u}_1) \in C_1, \mathbf{v} \in C_2\}$$

has covering radius at most  $R_1 + R_2$ .

In contrast to the direct sum, the  $(\mathbf{u}, \mathbf{u} + \mathbf{v})$  construction may produce a code with covering radius smaller than  $R_1 + R_2$ . In the following theorem  $C_1$  is the binary even weight code of length  $n + 1$  and  $C_2$  a binary code of length  $n$  and covering radius 1. According to the previous theorem, the covering radius of the resulting code is at most 2; we show it is 1.

**Theorem 3.4.3** Let  $C$  be an  $(n, K)_1$  code. Then the code

$$C' = \{(\pi(\mathbf{u}), \mathbf{u}, \mathbf{u} + \mathbf{v}) : \mathbf{u} \in \mathbb{F}^n, \mathbf{v} \in C\},$$

where  $\pi(\mathbf{u})$  denotes a parity check bit, is a  $(2n + 1, 2^n K)_1$  code.

**Proof.** Let  $\mathbf{w} = (x, \mathbf{y}, \mathbf{z}) \in \mathbb{F}^{2n+1}$  be arbitrary, where  $\mathbf{y}, \mathbf{z} \in \mathbb{F}^n$ . There is a codeword  $\mathbf{v} \in C$  such that  $d(\mathbf{v}, \mathbf{y} + \mathbf{z}) \leq 1$ . If  $d(\mathbf{v}, \mathbf{y} + \mathbf{z}) = 0$  or  $\pi(\mathbf{y}) = x$ , then the word  $\mathbf{c} = (\pi(\mathbf{y}), \mathbf{y}, \mathbf{y} + \mathbf{v}) \in C'$  satisfies  $d(\mathbf{c}, \mathbf{w}) \leq 1$ . Otherwise, change  $\mathbf{y}$  in one coordinate to obtain a vector  $\mathbf{y}'$  such that  $\mathbf{y}' + \mathbf{z} = \mathbf{v} \in C$ . Then  $\pi(\mathbf{y}') = x$  and  $\mathbf{c}' = (\pi(\mathbf{y}'), \mathbf{y}', \mathbf{y}' + \mathbf{v}) \in C'$  and  $d(\mathbf{c}', \mathbf{w}) \leq 1$ .  $\square$

**Example 3.4.4** Many of the best known upper bounds on  $K(n, 1)$  have been obtained using Theorem 3.4.3. For instance, the bound  $K(9, 1) \leq 62$  implies that  $K(19, 1) \leq 31744$ , which is the current record.  $\square$

Theorem 3.4.3 easily generalizes to nonbinary codes. If  $C \subseteq \mathbb{Z}_q^n$  is an  $(n, K)_q 1$  code, then

$$C' = \{(y, \mathbf{u}, \mathbf{u} + \mathbf{v}) : \mathbf{u} \in \mathbb{Z}_q^n, \mathbf{v} \in C, y \in \mathbb{Z}_q \text{ and } y \neq \sum_{i=1}^n u_i\}$$

is a  $(2n + 1, (q - 1)q^n K)_q 1$  code.

We now show how Theorem 3.4.3 can be generalized to  $R > 1$ . Yet another generalization is discussed in the next section (Theorem 3.5.3).

**Theorem 3.4.5** Suppose that a nonempty set

$$W = \{w_1, w_2, \dots, w_s\} \subseteq \{0, 1, 2, \dots, n+1\}$$

with  $w_1 < w_2 < \dots < w_s$  and a nonnegative integer  $R \leq n$  satisfy the conditions

$$w_1 \leq \frac{1}{2}(R+1), \quad w_s \geq n+1 - \frac{1}{2}(R+1),$$

$$w_{i+1} - w_i \leq R+1 \text{ for } i = 1, 2, \dots, s-1.$$

Denote by  $S_w$  the set of all binary vectors of length  $n+1$  and weight  $w$ . If

$$C_1 = \bigcup_{w \in W} S_w$$

and  $C_2$  is an  $(n, K)R$  code, then the code

$$C = \{(x_0, \mathbf{x}, \mathbf{x} + \mathbf{y}) : x_0 \in \mathbb{F}, \mathbf{x} \in \mathbb{F}^n, (x_0, \mathbf{x}) \in C_1, \mathbf{y} \in C_2\}$$

is a  $(2n+1, K \sum_{i=1}^s \binom{n+1}{w_i})R$  code.

**Proof.** We first prove that for every  $\mathbf{z} = (a_0, \mathbf{a}, \mathbf{b}) \in \mathbb{F}^{2n+1}$  with  $a_0 \in \mathbb{F}, \mathbf{a} \in \mathbb{F}^n$  and  $\mathbf{b} \in \mathbb{F}^n$  we have

$$d(\mathbf{z}, C_0^{(1)}) + d(\mathbf{z}, C_1^{(1)}) \leq 2R+1, \quad (3.4.6)$$

where  $C_a^{(1)} = \{\mathbf{c} \in C : c_1 = a\}$  for  $a = 0, 1$ . Clearly,  $C_0^{(1)} \neq \emptyset$  and  $C_1^{(1)} \neq \emptyset$ . We may assume that  $a_0 = 0$ . Otherwise, define  $\mathbf{z}' = (0, \mathbf{a}, \mathbf{b})$  and note that

$$\begin{aligned} d(\mathbf{z}, C_0^{(1)}) + d(\mathbf{z}, C_1^{(1)}) &= (d(\mathbf{z}', C_0^{(1)}) + 1) + (d(\mathbf{z}', C_1^{(1)}) - 1) \\ &= d(\mathbf{z}', C_0^{(1)}) + d(\mathbf{z}', C_1^{(1)}). \end{aligned}$$

By the definition of  $C_2$  there is a word  $\mathbf{c} \in C_2$  such that  $h = d(\mathbf{a} + \mathbf{b}, \mathbf{c}) \leq R$ . For any  $\mathbf{x}' = (x_0, \mathbf{x}) \in C_1$  define

$$\begin{aligned} D(\mathbf{x}') &= d((0, \mathbf{a}, \mathbf{b}), (x_0, \mathbf{x}, \mathbf{x} + \mathbf{c})) \\ &= d(0, x_0) + d(\mathbf{a}, \mathbf{x}) + d(\mathbf{b} + \mathbf{c}, \mathbf{x}). \end{aligned}$$

Let  $j$  be the number of coordinates where both  $\mathbf{a}$  and  $\mathbf{b} + \mathbf{c}$  have 1:

$$\begin{array}{rcl} \mathbf{a} & = & 111\dots 1 \quad 000\dots 0 \quad 111\dots 1 \quad 000\dots 0 \\ \mathbf{b} + \mathbf{c} & = & \underbrace{111\dots 1}_j \quad \underbrace{111\dots 1 \quad 000\dots 0}_h \quad 000\dots 0. \end{array}$$

It is now sufficient to find two vectors  $\mathbf{x}', \mathbf{x}'' \in C_1$ , one beginning with 0 and the other with 1, such that  $D(\mathbf{x}') + D(\mathbf{x}'') \leq 2R + 1$ .

For each  $w \in W$  and  $t = 0, 1$  choose a vector  $\mathbf{u}_t(w) = (u_{t,0}, u_{t,1}, \dots, u_{t,n}) \in S_w$  as follows. If  $j < w$ , set  $u_{t,0} = t$ ,  $u_{t,i} = 1$  whenever  $a_i = b_i + c_i = 1$  and as many of the remaining 1's in  $\mathbf{u}_t(w)$  as possible are in such coordinates  $i$  where  $a_i \neq b_i + c_i$ . If  $j \geq w$ , we choose  $\mathbf{u}_t(w)$  in such a way that  $u_{t,0} = t$  and  $a_i = b_i + c_i = 1$  whenever  $u_{t,i} = 1$ . Notice that  $\mathbf{u}_0(w)$  is not defined for  $w = n + 1$  and  $\mathbf{u}_1(w)$  for  $w = 0$ . We show that we can pick  $\mathbf{x}'$  and  $\mathbf{x}''$  from the collection of vectors just defined.

One of the following three cases occurs.

*Case 1:* There are  $w, w' \in W$  such that  $w \leq j < w'$  and  $w' - w \leq R + 1$ . If  $w' - j \leq h$ , then  $w' \leq h + j < n + 1$ ,  $\mathbf{u}_0(w')$  and  $\mathbf{u}_1(w')$  are both defined and  $D(\mathbf{u}_t(w')) = h + t \leq R + t$  for  $t = 0, 1$ . Hence  $D(\mathbf{u}_0(w')) + D(\mathbf{u}_1(w')) \leq 2R + 1$ . If  $w' - j > h$ , then  $D(\mathbf{u}_1(w')) = 1 + h + 2(w' - j - h - 1) = 2(w' - j) - h - 1$  and  $D(\mathbf{u}_0(w)) = 2(j - w) + h$ . Hence  $D(\mathbf{u}_1(w')) + D(\mathbf{u}_0(w)) = 2(w' - w) - 1 \leq 2(R + 1) - 1 = 2R + 1$ .

*Case 2:* We have  $0 \leq j < w_1$ . Since  $w_1 \leq (R + 1)/2 < n + 1$ ,  $\mathbf{u}_0(w_1)$  is defined. If  $w_1 - j \leq h$ , then as in Case 1 we have  $D(\mathbf{u}_t(w_1)) = h + t \leq R + t$  for  $t = 0, 1$  and  $D(\mathbf{u}_0(w_1)) + D(\mathbf{u}_1(w_1)) \leq 2R + 1$ . If  $w_1 - j > h$ , then  $D(\mathbf{u}_t(w_1)) = t + h + 2(w_1 - j - h - t) = 2(w_1 - j) - h - t \leq 2(R + 1)/2 - t = R + 1 - t$  for  $t = 0, 1$ , and again  $D(\mathbf{u}_0(w_1)) + D(\mathbf{u}_1(w_1)) \leq 2R + 1$ .

*Case 3:* We have  $w_s \leq j \leq n - h$ . Since  $w_s \geq n + 1 - (R + 1)/2 > 0$ ,  $\mathbf{u}_1(w_s)$  is defined. We have  $D(\mathbf{u}_t(w_s)) = t + 2(j - w_s + t) + h \leq 2(n - h - w_s) + h + 3t = 2(n + 1 - w_s) - h - 2 + 3t \leq 2(R + 1)/2 - 2 + 3t = R - 1 + 3t$  for  $t = 0, 1$  and  $D(\mathbf{u}_0(w_s)) + D(\mathbf{u}_1(w_s)) \leq 2R + 1$ .

This proves that (3.4.6) holds for all  $\mathbf{z} \in \mathbb{F}^{2n+1}$ , and consequently, the covering radius of  $C$  is at most  $R$ . Because  $C_2$  has covering radius  $R$ , we can choose  $\mathbf{a}, \mathbf{b} \in \mathbb{F}^n$  such that  $d(\mathbf{a} + \mathbf{b}, C_2) = R$ . Then for any  $(\mathbf{x}_0, \mathbf{x}, \mathbf{x} + \mathbf{y}) \in C$  we have

$$\begin{aligned} d((0, \mathbf{a}, \mathbf{b}), (\mathbf{x}_0, \mathbf{x}, \mathbf{x} + \mathbf{y})) &\geq d(\mathbf{a}, \mathbf{x}) + d(\mathbf{b}, \mathbf{x} + \mathbf{y}) \\ &= d(\mathbf{a}, \mathbf{x}) + d(\mathbf{b} + \mathbf{y}, \mathbf{x}) \\ &\geq d(\mathbf{a}, \mathbf{b} + \mathbf{y}) = d(\mathbf{a} + \mathbf{b}, \mathbf{y}) \\ &\geq d(\mathbf{a} + \mathbf{b}, C_2) = R. \end{aligned}$$

Therefore the covering radius is equal to  $R$ .  $\square$

In fact, using the terminology of Chapter 4, (3.4.6) shows that the resulting code in the previous theorem is normal.

**Example 3.4.7** If  $R = 1$ ,  $W = \{0, 2, 4, \dots, 2\lfloor(n+1)/2\rfloor\}$ , then  $C_1$  has  $2^n$  codewords, and if there is an  $(n, K)1$  code  $C_2$ , then there also exists a  $(2n+1, 2^n K)1$  code. Therefore the previous theorem generalizes Theorem 3.4.3.  $\square$

**Example 3.4.8** Pick  $n+1 = 6$ ,  $R = 2$ , and choose a set  $W = \{w_1, w_2, \dots, w_s\} \subseteq \{0, 1, \dots, 6\}$ ,  $w_1 < w_2 < \dots < w_s$ , in such a way that  $w_1 \leq 1$ ,  $w_s \geq 5$ ,  $w_{i+1} - w_i \leq 3$  for  $i = 1, 2, \dots, s-1$ , and the sum  $\sum_{i=1}^s \binom{n+1}{w_i}$  is as small as possible. We can choose  $W = \{0, 3, 6\}$ ,  $W = \{0, 2, 5\}$ , or  $W = \{1, 4, 6\}$ . In each case the code  $C_1$  in the theorem consists of 22 codewords. With  $C_2$  a  $(5, 2)2$  code, the construction gives an  $(11, 44)2$  code  $C$ .  $\square$

**Example 3.4.9** Choosing  $n+1 = 4m$ ,  $R = 2m-1$ ,  $W = \{m, 3m\}$  and  $C_2 = \{0^n, 1^n\}$  produces an  $(8m-1, 4\binom{4m}{m})2m-1$  code for every  $m \geq 1$ . For instance,  $K(15, 3) \leq 112$ .  $\square$

## 3.5 Matrix construction

As we have seen in Theorem 2.1.9, there is a nice way of calculating the covering radius of a linear code using its parity check matrix. The following theorem shows that for a certain class of nonlinear codes we can calculate the covering radius in a similar fashion. All the vectors are assumed to be column vectors.

Let  $Q = \mathbb{Z}_q$  or  $Q = \mathbb{F}_q$ , and  $\mathbf{A} = (\mathbf{I}_k, \mathbf{D})$  be a  $k \times n$  matrix over  $Q$ , where  $\mathbf{I}_k$  is the  $k \times k$  identity matrix. A set  $S \subseteq Q^k$  is said to  $r$ -cover  $Q^k$  using  $\mathbf{A}$  if every  $\mathbf{x} \in Q^k$  can be represented as a sum of exactly one element of  $S$  and a  $Q$ -linear combination of at most  $r$  columns of  $\mathbf{A}$ , i.e., if given a vector  $\mathbf{x} \in Q^k$  we can find a vector  $\mathbf{y} \in Q^n$  of weight at most  $r$  and a vector  $\mathbf{s} \in S$  such that  $\mathbf{x} = \mathbf{A}\mathbf{y} + \mathbf{s}$ .

**Theorem 3.5.1** *If  $S$  is an  $r$ -covering of  $Q^k$  using  $\mathbf{A}$ , then the code*

$$C = \{\mathbf{c} \in Q^n : \mathbf{A}\mathbf{c} \in S\}$$

*has  $|S|q^{n-k}$  codewords and covering radius at most  $r$ .*

**Proof.** Suppose  $\mathbf{z} \in Q^n$ . Then  $\mathbf{A}\mathbf{z} \in Q^k$  and we can find a vector  $\mathbf{y} \in Q^n$  of weight at most  $r$  such that  $\mathbf{A}\mathbf{z} = \mathbf{A}\mathbf{y} + \mathbf{s}$  for some  $\mathbf{s} \in S$ . Then  $\mathbf{A}(\mathbf{z} - \mathbf{y}) \in S$  and hence  $\mathbf{z} - \mathbf{y} \in C$ , and  $d(\mathbf{z}, \mathbf{z} - \mathbf{y}) \leq r$ . Clearly the cardinality of  $C$  equals  $|S|q^{n-k}$ .  $\square$

Assume now that  $Q$  is the finite field  $\mathbb{F}_q$ . Then the code  $C$  in the previous theorem is a union of some cosets of the linear code whose parity check matrix is  $\mathbf{A}$ . Therefore we can without loss of generality assume that  $\mathbf{A}$  is of the form  $(\mathbf{I}_k, \mathbf{D})$ .

**Example 3.5.2** If we choose

$$\mathbf{A} = \left( \begin{array}{c|c} & \begin{array}{ccccccccc} 0010110 & 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 0110000 & 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 1100101 & 0 & 1 & 1 & 1 & 0 & 1 & 1 \\ 1011110 & 0 & 0 & 0 & 1 & 1 & 1 & 0 \\ 1111011 & 0 & 1 & 1 & 0 & 1 & 0 & 1 \\ 0000111 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0101000 & 0 & 1 & 1 & 1 & 0 & 0 & 1 \\ 0111011 & 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 0001011 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \end{array} \end{array} \right) \quad S : \begin{array}{ccccccccc} 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \end{array}$$

then it can be verified by computer that the seven column vectors in  $S$  2-cover  $\mathbb{F}^9$  using the matrix  $\mathbf{A}$ , and the previous theorem yields a code of length 16 and covering radius at most 2 with 896 codewords. In fact, the covering radius of this code equals 2 by the sphere-covering bound.  $\square$

The following result generalizes Theorem 3.4.3.

**Theorem 3.5.3** *If  $q$  is a prime power, then*

$$K_q(qn + 1, 1) \leq q^{(q-1)n} K_q(n, 1).$$

**Proof.** Assume that  $C \subseteq \mathbb{F}_q^n$  attains the bound  $K_q(n, 1)$  and let  $\alpha_1, \alpha_2, \dots, \alpha_{q-1}$  denote the nonzero elements of the field  $\mathbb{F}_q$ . We choose

$$\mathbf{A} = \left( \begin{array}{ccccc} 1 & 00\dots0 & \alpha_1\alpha_1\dots\alpha_1 & \dots & \alpha_{q-1}\alpha_{q-1}\dots\alpha_{q-1} \\ 0 & & & & \\ 0 & & \mathbf{I}_n & \mathbf{I}_n & \dots & \mathbf{I}_n \\ \vdots & & & & & \\ 0 & & & & & \end{array} \right)$$

and

$$S = \{ \begin{pmatrix} 0 \\ \mathbf{c} \end{pmatrix} : \mathbf{c} \in C \}.$$

Now  $S$  1-covers  $\mathbb{F}_q^{n+1}$  using  $\mathbf{A}$ . Indeed, given any  $\begin{pmatrix} a \\ b \end{pmatrix} \in \mathbb{F}_q^{n+1}$  we can find a word  $\mathbf{c} \in C$  such that  $d(\mathbf{c}, \mathbf{b}) \leq 1$ . If  $d(\mathbf{c}, \mathbf{b}) = 0$ , then we obtain  $\begin{pmatrix} a \\ b \end{pmatrix}$  as a sum of  $\begin{pmatrix} 0 \\ \mathbf{c} \end{pmatrix} \in S$  and a suitable multiple of the first column. If  $d(\mathbf{c}, \mathbf{b}) = 1$ , then for

some  $\alpha \in \mathbb{F}_q^*$  and  $i$ ,  $1 \leq i \leq n$ , we have  $\mathbf{b} - \mathbf{c} = \alpha \mathbf{e}_i$ , where  $\mathbf{e}_i$  denotes the  $i$ -th column of  $\mathbf{I}_n$ . We obtain  $\binom{a}{b}$  by multiplying the column  $\binom{a\alpha^{-1}}{\mathbf{e}_i}$  of  $\mathbf{A}$  by  $\alpha$  and adding it to  $\binom{0}{c} \in S$ . The claim now follows from the previous theorem.  $\square$

## 3.6 Cascading

The next construction is a special case of generalized concatenated codes. In the following theorem  $V_1$  and  $V_2$  are of the form  $\mathbb{Z}_{q_1} \mathbb{Z}_{q_2} \dots \mathbb{Z}_{q_n}$ , but possibly for different values of  $n, q_1, \dots, q_n$ .

**Theorem 3.6.1** *Suppose that the code  $A \subseteq V_1 \times \mathbb{Z}_q$  has length  $n$  and covering radius  $R$ . If the codes  $C_0, C_1, \dots, C_{q-1} \subseteq V_2$  all have covering radius at most  $R' + 1$ , and their union has covering radius at most  $R'$ , then the code obtained by replacing each word  $(a_1, \dots, a_{n-1}, a) \in A$  by all the words  $(a_1, \dots, a_{n-1}, \mathbf{c})$  where  $\mathbf{c} \in C_a$ , has covering radius at most  $R + R'$ .*

**Proof.** Let  $(\mathbf{x}, \mathbf{y}) \in V_1 \times V_2$  be arbitrary. Then  $d(\mathbf{y}, C_i) \leq R'$  for at least one  $i$  and  $d(\mathbf{y}, C_t) \leq R' + 1$  for all  $t$ . Since the covering radius of  $A$  is at most  $R$ , there is a word  $(\mathbf{c}, j) \in A$  such that  $d((\mathbf{x}, i), (\mathbf{c}, j)) \leq R$ . But then  $d((\mathbf{x}, \mathbf{y}), \{\mathbf{c}\} \oplus C_j) = d(\mathbf{x}, \mathbf{c}) + d(\mathbf{y}, C_j) \leq R + R'$  both when  $i = j$  and  $i \neq j$ .  $\square$

Of course, one may repeat the construction for several coordinates, in particular, when  $R' = 0$ .

**Example 3.6.2** By Section 11.5 (Construction M) there exists a perfect mixed code  $A$  of length 17, covering radius 2 and cardinality  $2^{11}$  with sixteen binary coordinates and one coordinate over the alphabet  $\mathbb{F}_8$ .

Let  $C \subseteq \mathbb{F}^5$  be the  $(5, 7)1$  code of Figure 3.1. Denote by  $C_0, C_1, \dots, C_7 \subseteq \mathbb{F}^5$  the eight codes of the form  $\mathbf{x} + C$  where  $\mathbf{x} = (0, 0, x_1, x_2, x_3)$ ,  $x_1, x_2, x_3 \in \mathbb{F}$ . Clearly their union is the whole space  $\mathbb{F}^5$ . The construction of the previous theorem applied to the coordinate over  $\mathbb{F}_8$  gives a binary code of length 21 and covering radius at most 2 with  $7 \cdot 2^{11}$  codewords. In fact, by the sphere-covering bound, the covering radius of this code equals 2.

If we instead let  $C \subseteq \mathbb{F}^6$  be the  $(6, 12)1$  code of Figure 3.3, and denote by  $C_0, C_1, \dots, C_7$  the codes  $\mathbf{x} + C$  where  $\mathbf{x} = (0, 0, 0, x_1, x_2, x_3)$ ,  $x_1, x_2, x_3 \in \mathbb{F}$ , we obtain a  $(22, 3 \cdot 2^{13})2$  code.  $\square$

### 3.7 Optimal short nonbinary codes

In this section we present some constructions for arbitrary  $q$ -ary codes when  $n$  is small.

**Theorem 3.7.1** *For every  $q \geq 2$  and  $t \geq 1$ ,*

$$K_q(n, n-t) = q \quad \text{if } n \geq (t-1)q + 1,$$

and

$$K_q(n, n-t) > q \quad \text{if } n \leq (t-1)q.$$

**Proof.** If  $C \subseteq \mathbb{Z}_q^n$  has fewer than  $q$  codewords, then for each  $i = 1, 2, \dots, n$  we can choose  $x_i \in \mathbb{Z}_q$  such that  $c_i \neq x_i$  for all  $c \in C$ . Then the vector  $\mathbf{x} = (x_1, x_2, \dots, x_n)$  satisfies  $d(\mathbf{x}, C) = n$ . Therefore  $K_q(n, n-t) \geq q$  for every  $t \geq 1$ .

Assume that  $n \geq (t-1)q + 1$ , and choose  $C = \{\mathbf{a} = (a, a, \dots, a) \in \mathbb{Z}_q^n : a \in \mathbb{Z}_q\}$ . In any given  $\mathbf{x} \in \mathbb{Z}_q^n$ , at least one element  $a \in \mathbb{Z}_q$  appears at least  $t$  times, and  $d(\mathbf{x}, \mathbf{a}) \leq n-t$ . Hence  $K_q(n, n-t) = q$ .

Finally, suppose that  $C \subseteq \mathbb{Z}_q^n$  has cardinality  $q$  and that  $n \leq (t-1)q$ . We can assume that (up to equivalence) each element of  $\mathbb{Z}_q$  appears in each of the first  $j$  coordinates ( $0 \leq j \leq n$ ), and that the first codeword begins with  $j$  0's, the second with  $j$  1's, and so on, the  $q$ -th codeword begins with  $j$   $(q-1)$ 's, and that for every other coordinate  $i > j$  we can find  $x_i \in \mathbb{Z}_q$  that does not appear in the  $i$ -th coordinate in any codeword. For all  $i \leq j$  define  $x_i$  by the congruence  $x_i \equiv i \pmod{q}$ . Clearly  $d(\mathbf{x}, C) = (j - \lceil j/q \rceil) + (n-j) \geq n - \lceil n/q \rceil \geq n - t + 1$ . Hence  $K_q(n, n-t) > q$  when  $n \leq (t-1)q$ .  $\square$

Trivially,  $K_q(n, 0) = q^n$  and  $K_q(n, n) = 1$ . By the previous theorem,  $K_q(n, n-1) = q$  for all  $q$  and  $n$ . In particular  $K_q(2, 1) = q$  for all  $q$ .

We can also determine the exact value of  $K_q(3, 1)$ . Choose  $Q = \{1, 2, \dots, q\}$  as our  $q$ -ary alphabet.

Assume that  $Q_1 = \{1, 2, \dots, i\} \subseteq Q$  and consider the set  $C_1 = \{(a, b, c) : a, b, c \in Q_1, a+b \equiv c \pmod{i}\}$ . Then every ordered pair of  $1, 2, \dots, i$  occurs (exactly) once in every two coordinates. Hence any vector in  $Q^3$  with at least two coordinates in  $Q_1$  is covered.

Similarly choose  $Q_2 = \{i+1, i+2, \dots, q\}$  and construct the set  $C_2 = \{(a, b, c) : a, b, c \in Q_2, a+b \equiv c \pmod{q-i}\}$ . Any vector in  $Q^3$  with at least two coordinates in the set  $Q_2$  is covered.

Hence the union of  $C_1$  and  $C_2$  has covering radius one. Choosing  $i = \lfloor q/2 \rfloor$  gives a code with  $\lceil q^2/2 \rceil$  codewords.

The optimality of this construction is proved in the following theorem.

**Theorem 3.7.2**  $K_q(3, 1) = \lceil \frac{1}{2}q^2 \rceil$ .

**Proof.** Assume on the contrary that there is a  $(3, K)_q 1$  code with  $K < q^2/2$ . Denote by  $m$  the smallest integer such that every letter in  $Q$  appears at least  $m$  times in every coordinate and there is a letter which appears exactly  $m$  times in some coordinate. Clearly,  $m < q/2$ . We may assume that there are exactly  $m$  codewords  $\mathbf{c}_1, \mathbf{c}_2, \dots, \mathbf{c}_m$  that begin with the letter  $a$ . Suppose that  $t$  of the second coordinates in these  $m$  words are distinct and that  $x \in Q$  is not among them. By the definition of  $m$ , the second coordinate in some  $s \geq tm$  codewords, is among these  $t$  letters. If  $y \in Q$  does not appear as the third coordinate in the first  $m$  codewords, then the vector  $(a, x, y)$  is not covered by these  $s$  codewords. The remaining codewords, the number of which is smaller than  $\frac{1}{2}q^2 - tm$ , do not begin with  $a$  and they each cover at most one such vector  $(a, x, y)$ . The letter  $x$  can be chosen in  $q - t$  ways and  $y$  in at least  $q - m$  ways, and thus

$$(q - t)(q - m) < \frac{1}{2}q^2 - tm,$$

or equivalently

$$(q - 2t)(q - 2m) < 0.$$

However,  $t \leq m < q/2$ , a contradiction.  $\square$

We now generalize the previous result to a class of mixed codes, and provide an alternative proof for the previous theorem.

**Lemma 3.7.3** *In an  $s \times s$  matrix of nonnegative integers, suppose that for every zero entry, the sum of the row entries plus the sum of the column entries corresponding to that zero is at least  $t$ . Then the sum of all entries in the matrix is at least*

$$s^2 - \left\lfloor \frac{(3s - t)^2}{8} \right\rfloor.$$

**Proof.** Maximize  $x$ , the number of zeros along the main diagonal, by permuting rows and columns, and write the matrix in the form

$$\mathbf{B} = (b_{ij}) = \begin{pmatrix} \mathbf{B}_{00} & \mathbf{B}_{01} \\ \mathbf{B}_{10} & \mathbf{B}_{11} \end{pmatrix},$$

where the  $x$  diagonal entries of  $\mathbf{B}_{00}$  are zeros. Let  $S_{ij}$  denote the sum of all entries in the block  $\mathbf{B}_{ij}$ .

It is not possible that  $b_{ij} = b_{ji} = 0$  for some  $1 \leq i \leq x$ ,  $x + 1 \leq j \leq s$ , because a pattern like

$$\left( \begin{array}{ccc|c} 0 & & & 0 \\ & \ddots & & \\ & & 0 & \\ \hline 0 & & & \end{array} \right)$$

implies that we can increase  $x$  by rearranging rows and columns. Consequently  $S_{01} + S_{10} \geq x(s - x)$ . None of the entries in  $\mathbf{B}_{11}$  are zeros, and therefore  $S_{11} \geq (s - x)^2$ . For each of the  $x$  zeros in the main diagonal of  $B_{00}$  we add the entries of its corresponding row and column, and get  $2S_{00} + S_{01} + S_{10} \geq xt$ . Together these three inequalities imply that

$$\begin{aligned} 2S_{00} + 2S_{01} + 2S_{10} + 2S_{11} &\geq xt + x(s - x) + 2(s - x)^2 \\ &= x^2 + (t - 3s)x + 2s^2 \\ &= \left(x + \frac{t - 3s}{2}\right)^2 - \left(\frac{t - 3s}{2}\right)^2 + 2s^2 \\ &\geq 2s^2 - \left(\frac{3s - t}{2}\right)^2 \end{aligned}$$

proving our claim.  $\square$

**Theorem 3.7.4** *Let  $S = \{1, 2, \dots, s\}$  and  $T = \{1, 2, \dots, t\}$ , and assume that  $s \leq t$ . The minimum cardinality of a mixed code  $C \subseteq S \times S \times T$  with covering radius one equals  $s^2 - \lfloor \frac{(3s-t)^2}{8} \rfloor$  if  $t \leq 3s$ , and  $s^2$  otherwise.*

**Proof.** Assume that  $C \subseteq S \times S \times T$  has covering radius one. Let  $\mathbf{B} = (b_{ij})$  be the  $s \times s$  matrix where  $b_{ij}$  is the number of codewords of the form  $(i, j, k) \in C$ . If  $b_{ij} = 0$ , all the vectors  $(i, j, z)$ , where  $z \in T$ , are covered by the codewords of the form  $(x, j, z)$  with  $x \neq i$  and  $(i, y, z)$  with  $y \neq j$ , and therefore the sum of the entries in the  $i$ -th row of  $\mathbf{B}$  plus the sum of the entries in the  $j$ -th column is at least  $t$ . The previous lemma now implies the lower bound when  $t \leq 3s$ .

If we increase  $t$ , the number of codewords needed cannot decrease, and therefore the lower bound  $s^2$  obtained for  $t = 3s$  holds for all  $t \geq 3s$ .

Notice first that the code  $S \times S \times \{1\}$  has  $s^2$  codewords and covering radius one, which proves the claim when  $t \geq 3s - 2$ . Assume that  $t < 3s - 2$ . Let  $i$  be an integer such that  $1 \leq i \leq s$ , and denote  $S_1 = \{1, 2, \dots, i\}$ ,  $S_2 = S \setminus S_1$ , and

$T_1 = \{1, 2, \dots, t-s+i\}$ ,  $T_2 = T \setminus T_1$ . The argument used in the construction leading to Theorem 3.7.2 shows that the union of the codes

$$C_1 = \{(a, b, c) : a, b \in S_1, c \in T_1, a + b \equiv c \pmod{i}\}$$

and

$$C_2 = \{(a, b, c) : a, b \in S_2, c \in T_2, a + b \equiv c \pmod{s-i}\}$$

has covering radius one. The cardinality of this union is

$$i(t-s+i) + (s-i)^2 = 2\left(i - \frac{3s-t}{4}\right)^2 + s^2 - \frac{(3s-t)^2}{8},$$

with minimum value  $s^2 - \lfloor \frac{(3s-t)^2}{8} \rfloor$ .  $\square$

The idea of the construction leading to Theorem 3.7.2 can be generalized to larger covering radii.

**Definition 3.7.5** A  $K \times n$  matrix  $\mathbf{A} = (a_{ij})$  over  $\mathbb{Z}_q$  is called  $s$ -surjective, or  $s$ -independent, if for every  $s$  columns with indices  $j_1, j_2, \dots, j_s$  and every  $(b_1, b_2, \dots, b_s) \in \mathbb{Z}_q^s$  there is a row with index  $i$  such that  $a_{i,j_t} = b_t$  for all  $t = 1, 2, \dots, s$ . We denote by  $ms_q(n, s)$  the minimum number of rows in any  $s$ -surjective matrix over  $\mathbb{Z}_q$  with  $n$  columns.

**Example 3.7.6** Consider the code  $C_1$  in the construction leading to Theorem 3.7.2. If we write the codewords as rows, the resulting matrix over  $Q_1$  is 2-surjective.  $\square$

By Theorem 3.7.1,  $K_q(n, n-2) = q$  if  $n \geq q+1$ . Consider now the case  $n = q$ .

**Theorem 3.7.7**  $K_q(q, q-2) \leq q-2 + ms_2(q, 2)$ .

**Proof.** Take as the codewords of  $C$  all the rows of a binary 2-surjective matrix with  $q$  columns and  $ms_2(q, 2)$  rows, and all the vectors  $\mathbf{a} = (a, a, \dots, a)$ , where  $a \in \{2, 3, \dots, q-1\}$ . This gives a  $q$ -ary code of length  $q$  with  $q-2 + ms_2(q, 2)$  codewords. We show that it has covering radius at most  $q-2$ . Any  $q$ -ary vector that has at least two binary coordinates is covered by the codewords obtained from the 2-surjective matrix. On the other hand, if  $\mathbf{x}$  is a  $q$ -ary vector with at most one binary coordinate, then there exists a letter  $a \in \{2, 3, \dots, q-2\}$  which occurs at least twice in  $\mathbf{x}$ , and  $d(\mathbf{x}, \mathbf{a}) \leq q-2$ .  $\square$

The values of  $ms_2(q, 2)$  are known. The columns of a binary  $K \times n$  matrix can be viewed as incidence vectors of subsets of the set  $\{1, 2, \dots, K\}$ . If we

choose as columns all the subsets that contain the element 1 and exactly  $\lfloor K/2 \rfloor - 1$  of the remaining  $K - 1$  elements, then the union of the subsets corresponding to any two such columns contains fewer than  $K$  elements, and we immediately verify that the resulting matrix is 2-surjective. We can choose  $K$  to be the smallest integer such that

$$q \leq \binom{K-1}{\lfloor K/2 \rfloor - 1},$$

and this is the best possible; see Brace and Daykin [93] and Kleitman and Spencer [380].

The following result provides upper bounds on codes over large nonprime alphabets.

**Theorem 3.7.8** *For every  $q \geq 2$  and  $t \geq 1$ ,*

$$K_{tq}(n, 1) \leq t^{n-1} K_q(n, 1).$$

**Proof.** Assume that  $C$  is a code over the alphabet  $Q = \{0, 1, \dots, q-1\}$  which attains the bound  $K_q(n, 1)$ . Clearly, the code

$$\begin{aligned} C' = \{ & (c_1 t + b_1, c_2 t + b_2, \dots, c_n t + b_n) : (c_1, c_2, \dots, c_n) \in C, \\ & 0 \leq b_i < t \text{ for all } i, b_1 + \dots + b_n \equiv 0 \pmod{t} \} \end{aligned}$$

over the alphabet  $\{0, 1, \dots, tq-1\}$  has cardinality  $t^{n-1} K_q(n, 1)$ . We claim that it has covering radius 1. Let  $\mathbf{z} = (z_1, z_2, \dots, z_n)$  be an arbitrary vector where  $z_i \in \{0, 1, \dots, tq-1\}$  for all  $i$ , and for each  $i$  write  $z_i = x_i t + y_i$ , where  $0 \leq x_i < q$  and  $0 \leq y_i < t$ . There is a codeword  $(c_1, c_2, \dots, c_n) \in C$  such that  $c_i = x_i$  for all coordinates  $i$  except possibly one. But we can freely choose  $b_i = y_i$  in  $n-1$  coordinates to obtain a codeword of  $C'$  that has distance at most 1 to  $\mathbf{z}$ .  $\square$

Using this construction we obtain another family of optimal nonbinary codes.

**Theorem 3.7.9** *If  $q$  is a prime power, then for all  $t \geq 1$*

$$K_{tq}(q+1, 1) = q^{q-1} t^q.$$

**Proof.** Applying the previous theorem to the  $q$ -ary Hamming code, we get  $K_{tq}(q+1, 1) \leq q^{q-1} t^q$ . The claim follows from the inequality

$$K_m(n, 1) \geq \frac{m^{n-1}}{n-1}$$

proved for all  $m$  and  $n \geq 2$  by Rodemich [555].  $\square$

**Theorem 3.7.10** For every  $q \geq 2$  and  $t \geq 1$ ,

$$K_{tq}(n, R) \leq ms_t(n, n - R)K_q(n, R).$$

**Proof.** The proof of Theorem 3.7.8 immediately generalizes to the case  $R \geq 1$ .  $\square$

Notice that  $ms_q(n, s) \geq q^s$ , with equality if and only if there is an  $(n, q^s, n - s + 1)_q$  MDS code. Namely, a  $q^s \times n$  matrix over  $\mathbb{Z}_q$  formed by taking as its rows the codewords of an  $(n, q^s, d)_q$  code is  $s$ -surjective if and only if  $d \geq n - s + 1$ . Indeed, two rows have the same  $s$ -tuple in some  $s$  columns if and only if the distance between the rows is at most  $n - s$ .

For example,  $ms_q(n, n - 1) = q^{n-1}$  because  $\{\mathbf{x} \in \mathbb{Z}_q^n : x_1 + x_2 + \dots + x_n = 0\}$  is an  $(n, q^{n-1}, 2)_q$  code.

**Theorem 3.7.11** If  $q$  is a prime power and  $2 \leq n \leq q + 1$ , then

$$K_{q(n-1)}(n, n - 2) = q^2(n - 1).$$

**Proof.** From Section 2.6 we know that there exists a  $[q + 1, 2, q]_q$  doubly extended Reed-Solomon code, and by puncturing we obtain an  $[n, 2, n - 1]_q$  code for all  $2 \leq n \leq q + 1$ . Theorem 3.7.10 implies that  $K_{q(n-1)}(n, n - 2) \leq ms_q(n, 2)K_{n-1}(n, n - 2) = q^2(n - 1)$ . The reverse inequality follows from the lower bound

$$K_m(n, n - 2) \geq \frac{m^2}{n - 1} \tag{3.7.12}$$

proved for all  $m$  and  $n \geq 2$  by Rodemich [555].  $\square$

The idea of Theorem 3.7.8 can be generalized to produce codes over arbitrary larger alphabets.

**Example 3.7.13** Consider the ternary  $(4, 9)1$  Hamming code over the alphabet  $\{0, 1, 2\}$  consisting of the codewords 0000, 1201, 2102, 2210, 0111, 1012, 1120, 2021, 0222. We now construct a  $(4, \cdot)1$  code over the alphabet  $Q = \{1, 2, 3, 4\}$ . In each of the last eight codewords we replace 0 with 3 and 4, thus obtaining 16 words. We then replace the all-zero codeword with all the eight words  $(x_1, x_2, x_3, x_4) \in \{3, 4\}^4$  such that  $x_1 + x_2 + x_3 + x_4 \equiv 0 \pmod{2}$ . These 24 words form a  $(4, 24)1$  code over  $Q$ . In fact, this code is optimal; see Kalbfleisch and Stanton [358].  $\square$

## 3.8 Simulated annealing and local search

When no suitable combinatorial or algebraic method is available for constructing a code with given parameters, we can instead use computer search techniques. The exhaustive search is seldom feasible, but there are a number of *local search* methods that can be employed. In this section we briefly discuss some of them, in particular simulated annealing and taboo search, and how they can be applied to finding good covering codes.

Usually the parameters  $q, n, K$  and  $r$  are fixed before the search. The objective is to find an  $(n, K)R$  code with  $R \leq r$ . If such a code is found we decrease  $K$  and try to find a smaller one.

When using the *iterative improvement* method we start with  $K$  — usually randomly chosen —  $q$ -ary vectors of length  $n$ . Such a configuration is a code, if all the  $K$  vectors are different. For each configuration we define its *neighbourhood*, which, e.g., consists of all the configurations that can be obtained by changing at most  $r$  coordinates in one vector. At each step we change the configuration to a randomly chosen one in its neighbourhood. If a better configuration is obtained, the change is accepted, otherwise not. The same process is then continued until no further improvements are possible. The quality of a configuration is measured by a *cost function*. A natural choice is to define the cost function as the number of vectors in the whole space that are not  $r$ -covered by the  $K$  vectors of the current configuration. We can use an array with  $q^n$  entries to store the number of times each  $q$ -ary vector of length  $n$  is covered. Updating this array and calculating the cost of the new configuration is easy after each change. The goal is to try to minimize the cost function value. Indeed, a configuration with cost 0 has covering radius at most  $r$ . This method is simple and efficient, but liable to get stuck in local minima. In the *steepest descent* method, instead of choosing a random neighbour, we go through the whole neighbourhood and choose the configuration with the least cost.

In *simulated annealing* we sometimes accept changes that deteriorate the configuration, thus hoping to escape from local minima. This method mimics physical annealing, slow cooling of material from a high-energy liquid state to a low-energy crystallized state. In simulated annealing, we first choose a high initial temperature  $T$  which is slowly lowered, typically by multiplying the previous temperature by a constant  $\lambda$ , where  $0.9 \leq \lambda < 1$ . At each temperature we generate a number of new configurations, e.g., a constant number. Each new configuration with a lower cost is accepted. A configuration with a higher cost is accepted with a probability

$$e^{-\Delta c/T},$$

where  $\Delta c > 0$  is the increase in cost, and  $T$  is the current temperature. At first when  $T$  is high, this probability is large, but decreases when  $T$  is

lowered. Eventually, we find a configuration with cost 0, i.e., a configuration with covering radius at most  $r$ , or anyway stop, if the cost remains the same for a fixed number of consecutive temperatures. This basic variant can be modified in a number of ways.

In *taboo search* we go through the whole neighbourhood and accept the neighbour with the smallest cost — even if this means increasing the cost. However, after accepting a configuration with a higher cost we do not wish to slide back to the local minimum in the next move. To avoid it we keep a *taboo list* of forbidden moves. In our case a taboo list may consist of the  $L$  most recently altered vectors in the configuration, and it is forbidden to change a vector which is in the taboo list. Then  $L$  denotes the number of moves that must take place before an altered vector can be altered again.

Another natural neighbourhood structure is obtained as follows. We go through the vectors in the whole space one by one, e.g., in the lexicographic order, until we find an uncovered vector  $\mathbf{x}$ . The neighbourhood consists of all configurations that can be obtained by replacing exactly one vector in the current configuration by a vector that  $r$ -covers  $\mathbf{x}$ .

Local search can also be used in connection with the matrix method of Section 3.5 to search for the matrix  $\mathbf{A}$  and the set  $S$ . First, the parameters  $q$ ,  $n$ ,  $r$ ,  $k$  and  $|S|$  are fixed. A suitable cost function is the number of vectors in  $Q^k$  that cannot be written in the form  $\mathbf{A}\mathbf{y} + \mathbf{s}$  for any  $\mathbf{y} \in Q^n$  of weight at most  $r$  and  $\mathbf{s} \in S$ . During the search we may change both  $\mathbf{A}$  and  $S$ . Alternatively, we can change only  $S$ , but go through some large collection of matrices  $\mathbf{A}$  or choose a particularly promising matrix  $\mathbf{A}$ , e.g., a parity check matrix of a good linear code. Linear covering codes can be searched by fixing  $S = \{00\dots 0\}$ .

### 3.9 Notes

§3.1 Theorem 3.1.3 is from Assmus and Pless [27]. Example 3.1.4 is from Struik [630].

§3.2 The linear case of Theorem 3.2.4 is from Cohen, Karpovsky, Mattson and Schatz [156] and the nonlinear case from Lobstein [449]; see also Cohen, Lobstein and Sloane [165].

§3.3 The discussion is from Cohen, Lobstein and Sloane [165]. The values of  $K(n, 2)$  for  $n = 2, 3, 4, 5, 7$  were already determined in Taussky and Todd [635]. For the history of the bound  $K(11, 1) \leq 192$ , see Hämäläinen and Rankinen [278].

§3.4 For Theorem 3.4.2, see Mattson [471]. Theorem 3.4.3 is due to Mollard [491] and Katsman and Litsyn [165]. The remark following Example 3.4.4

is from van Lint, Jr. [440]. Theorem 3.4.5 and the examples following it are from Honkala and Hämäläinen [322]. The bound  $K(11, 2) \leq 44$  which can be obtained from Theorem 3.4.5 was already known earlier, see Hämäläinen and Rankinen [278].

The following result related to Theorem 3.4.5 has been proved in Honkala [312]. A binary  $(n, K)R$  code  $C$  is called  $s$ -surjective, if the binary  $K \times n$  matrix formed by the codewords is  $s$ -surjective (see Definition 3.7.5). Suppose that  $C_1$  is an  $(n+R, K_1)$  code which is  $n$ -surjective, and that  $C_2$  is an  $(n, K_2)R$  code. Then the code  $C = \{(\mathbf{x}_0, \mathbf{x}, \mathbf{x} + \mathbf{y}) : \mathbf{x}_0 \in \mathbb{F}^R, \mathbf{x}, \mathbf{y} \in \mathbb{F}^n, (\mathbf{x}_0, \mathbf{x}) \in C_1, \mathbf{y} \in C_2\}$  is a  $(2n + R, K_1 K_2)R$  code. (In fact, it is only shown in [312] that the covering radius is at most  $R$ , but exactly the same argument as in the proof of Theorem 3.4.5 shows that equality holds.)

§3.5 The case  $r = 1$  of Theorem 3.5.1 is due to Blokhuis and Lam [90] who generalized a method of Kamps and van Lint [362], and the generalization to arbitrary  $r$  was independently presented in van Lint, Jr. [440] and Carnielli [130]. See also Kabatyanskii and Panchenko [355]. The theorem can be modified to mixed codes and several other covering problems; see Östergård [516] and Chapters 13, 14 and 15. Example 3.5.2 is from Hämäläinen, Honkala, Kaikkonen and Litsyn [275]. Local search methods have been used in connection with the matrix construction in several papers; see the Notes on Section 3.8.

For using Davydov's method to construct nonlinear covering codes, see the Notes of Chapter 5.

Theorem 3.5.3 is from Blokhuis and Lam [90]. In the same way as Theorem 3.5.3 we can prove that more generally, if  $q$  is a prime power, then for all  $R \geq 1$ ,  $K_q(qn + 1, R) \leq q^{(q-1)n} K_q(n, R)$ ; see van Lint, Jr. [440]. It has been shown in Honkala [315] that if  $q$  is a prime, then  $K_q(tn + 1, R) \leq \max\{1, q - (t - 1)R\} q^{(t-1)n} K_q(n, R)$ . The case when  $R = 1$  and  $n$  is of the form  $(q^k - 1)/(q - 1)$  for some  $k$ , i.e.,  $n$  is the length of a Hamming code was already proved in Blokhuis and Lam [90]. When  $R \geq 2$ , Östergård [522] proved that  $K_q(tn, R) \leq \max\{1, q - (t - 1)R\} q^{(t-1)n-1} K_q(n, R)$ . For some further improvements, see Honkala [315], Östergård [522].

When  $q = 2$  and  $R = 1$  the following observation has been used in Östergård and Kaikkonen [526]. Assume that  $S = \{\mathbf{s}_1, \mathbf{s}_2, \dots, \mathbf{s}_t\} \subseteq \mathbb{F}^k$ ,  $\mathbf{A} = (\mathbf{a}_1, \mathbf{a}_2, \dots, \mathbf{a}_n)$  and that  $S$  1-covers  $\mathbb{F}^k$  using the matrix  $\mathbf{A}$ . Since a code and its translate have the same covering radius, assume without loss of generality that  $\mathbf{s}_1 = \mathbf{0}$ . Then switch the roles of the sets  $\{\mathbf{a}_1, \dots, \mathbf{a}_n\}$  and  $\{\mathbf{s}_2, \dots, \mathbf{s}_t\}$ . Namely, the set  $\{\mathbf{0}, \mathbf{a}_1, \dots, \mathbf{a}_n\}$  1-covers  $\mathbb{F}^k$  using the matrix  $(\mathbf{s}_2, \mathbf{s}_3, \dots, \mathbf{s}_t)$ . Indeed, both properties mean that  $\{\mathbf{0}, \mathbf{a}_1, \dots, \mathbf{a}_n\} + \{\mathbf{0}, \mathbf{s}_2, \dots, \mathbf{s}_t\} = \mathbb{F}^k$ .

§3.6 The substitution construction of Theorem 3.6.1 has been used in a number of papers to construct covering codes: see, e.g., Heden [289], Kabatyanskii and Panchenko [355], Hämäläinen and Rankinen [278], Construc-

tions e and h], Östergård [511], [512] and Etzion and Greenberg [222]. Östergård calls an  $(n, K)_q R$  code  $C$  *strongly  $p$ -seminormal* if it can be partitioned into  $p$  subcodes  $C_i$  each with covering radius at most  $R + 1$ . In the terminology of Etzion and Greenberg, a *covering by coverings* of  $\mathbb{F}^n$  is a set of  $(n, \cdot)_1$  codes whose union is  $\mathbb{F}^n$ . Example 3.6.2 is from Etzion and Greenberg [222].

Theorem 3.6.1 can be generalized further. Assume that  $A \subseteq \mathbb{Z}_{q_1} \mathbb{Z}_{q_2} \dots \mathbb{Z}_{q_n}$  has covering radius  $R$ . If for each  $i$  we have a family of codes  $C_{i,j}$  of length  $n_i$ , where  $j = 1, 2, \dots, q_i$ , such that each  $C_{i,j}$  has covering radius  $R'$  and the union of these  $q_i$  codes has covering radius  $R''$ , then the code obtained by replacing each codeword  $(a_1, \dots, a_n)$  of  $A$  by all the words in the set  $C_{1,a_1} \oplus C_{2,a_2} \oplus \dots \oplus C_{n,a_n}$  has covering radius at most  $RR' + (n - R)R''$ . In this way Carnielli [128] has shown that  $K_q(tn, (n - R)(t - R')) \leq K_{K_q(t, R')}(n, R)$  when  $R < n$  and  $R' < t$ .

§3.7 The first half of Theorem 3.7.1 for  $n = 2$  is from Kalbfleisch and Stanton [358] and the general form from Carnielli [128]; the second half is from Chen and Honkala [134].

Theorem 3.7.2 is from Golomb and Posner [257] (which uses results by A. W. Hales and J. N. Franklin, and S. C. Rosen) and Kalbfleisch and Stanton [358]. See also Stanton [615]. Our proof of Theorem 3.7.2 is from [358].

Theorem 3.7.4 is from Numata [505] and the proof of the lower bound follows the one given for the case  $s = t$  in Golomb and Posner [257] and uses Lemma 3.7.3 due to J. N. Franklin and A. W. Hales [257]. Clayton [141] has used a similar technique to obtain the lower bound  $\frac{7}{8}s^2$  for 2-fold coverings of length three over  $\mathbb{F}_s$ , cf. Chapter 14. In fact, Numata [505] showed using a similar construction as in the proof of Theorem 3.7.4 that the minimum cardinality  $K$  of a code  $C \subseteq \mathbb{Z}_r \mathbb{Z}_s \mathbb{Z}_t$  with covering radius one satisfies

$$K \leq \begin{cases} rs - \lfloor \frac{(2r+s-t)^2}{8} \rfloor & \text{if } 2r + s \geq t + 2 \\ rs & \text{if } 2r + s < t + 2, \end{cases}$$

and conjectures that equality always holds. Trivially, the conjecture holds when  $t \geq rs$ . See also Östergård [516].

Theorem 3.7.7 is a special case of [516, Theorem 8]. In Example 6.7.6 it is shown that equality holds in Theorem 3.7.7 at least for  $q \leq 4$ . In general we do not know if the codes are optimal. The discussion preceding Theorem 3.7.8 belongs to the area of combinatorics of finite sets; see I. Anderson [22].

Theorem 3.7.8 is due to Stanton, Horton and Kalbfleisch [616] — the case when  $n = q + 1$  and  $q$  is a prime power is already given in Kalbfleisch and Weiland [360] — and rediscovered by Blokhuis and Lam [90]. Kalbfleisch and Weiland [360] also proved Theorem 3.7.9 when  $t = 2$ . In general the lower bound follows from Rodemich [555] as was noticed in Blokhuis and Lam [90]; see also Carnielli [128] and Clayton [141]. Theorem 3.7.10 is discussed

in Carnielli [128] in the case  $mst_t(n, n - R) = t^{n-R}$ . Apart from proving inequality (3.7.12), Rodemich [555] also showed that equality holds if and only if  $n - 1$  divides  $m$  and there are  $n - 2$  mutually orthogonal Latin squares of order  $q := m/(n - 1)$ . It is well known that  $n - 2$  mutually orthogonal Latin squares of order  $q$  exist if and only if there is an *orthogonal array*  $OA(q, n)$ , i.e., an  $n \times q^2$  matrix  $\mathbf{A}$  over  $S = \{1, 2, \dots, q\}$  such that  $\mathbf{A}^T$  is 2-surjective. Indeed, if  $L_1, L_2, \dots, L_{n-2}$  are pairwise orthogonal Latin squares, then we can take the vectors

$$(i, j, L_1(i, j), L_2(i, j), \dots, L_{n-2}(i, j))$$

as the columns of  $\mathbf{A}$ . By the discussion preceding Theorem 3.7.11, the existence of a 2-surjective  $q^2 \times n$  matrix over  $S$  is equivalent to the existence of an  $(n, q^2, n - 1)_q$  MDS code. For Theorem 3.7.11, see Carnielli [128]. For other constructions using MDS codes, see Carnielli [130] and Östergård [522].

Codes of length 4 and 5 are studied in Kalbfleisch and Stanton [358] and Stanton, Horton and Kalbfleisch [616]. Example 3.7.13 is from [616]. They describe the construction in the general case when an  $(n, K)_q$  code is used to construct an  $(n, \cdot)_1$  code over any larger alphabet, and present applications to the cases  $n = 4$  and  $n = 5$ . For further results in this direction, see also Kalbfleisch, Stanton and Horton [359]. A discussion on mixed codes of short lengths can be found in Östergård [516].

**§3.8** For an extensive treatment of local search methods, see Aarts and J. K. Lenstra [6], Aarts and Korst [4] and van Laarhoven and Aarts [401]. Simulated annealing is due to Kirkpatrick, Gelatt and Vecchi [375] and Černý [131]. The first results on using local search for producing error-correcting codes can be found in El Gamal, Hemachandra, Shperling and Wei [216]. Simulated annealing was first applied to covering codes in Wille [685] to show that  $K_3(6, 1) \leq 74$ . In van Laarhoven, Aarts, van Lint and Wille [402] it is proved that  $K_3(6, 1) \leq 73$ ,  $K_3(7, 1) \leq 186$  and using the matrix construction that  $K_3(8, 1) \leq 486$ . The bound  $K_3(6, 1) \leq 73$  was proved independently in Bernasconi [71]. For a combinatorial proof, see Östergård [519]. Wille [687] used simulated annealing to show that  $K(9, 1) \leq 62$  and  $K(10, 1) \leq 120$ . The bound  $K(10, 1) \leq 120$  was rediscovered by Östergård [511]. Other bounds for binary and nonbinary cases obtained using local search have been reported in Koschnick [386], Östergård [512], [516], [517], [522], [523], Östergård and Hämäläinen [525], Östergård and Kaikkonen [526] and Wille [688]. See also Charon, Hudry and Lobstein [132]. Local search has also been used to find suitable partitions of the code, cf. Chapter 4; see Östergård [514]. The mentioned alternative neighbourhood structure is from Östergård [523]. A discussion of local search in code constructions can also be found in Aarts and van Laarhoven [5], van der Ham [274], Honkala and Östergård [328] and van Lint [439].

This Page Intentionally Left Blank

# Chapter 4

## Normality

This chapter continues the study of constructions. We concentrate on two closely related constructions, the *amalgamated direct sum* (ADS) and the *blockwise direct sum* (BDS).

The ADS construction was presented by Graham and Sloane [265]. Compared to the direct sum, the ADS of two binary linear codes has length one less, dimension one less, and at least as small a covering radius, thus improving on the direct sum. However, this requires that the two codes have certain regularity properties. Such *normality* properties have been extensively studied, which is the reason why the ADS construction is treated separately, instead of being included in the previous chapter. Many binary linear codes are shown to be *normal* in Section 4.2. It is an open problem whether or not all binary linear codes are *normal*.

We can also form the ADS of two nonlinear codes. It is known that many nonlinear codes are *normal*, but not all. Namely, in Section 4.3 we construct a large number of *abnormal* binary nonlinear codes. In Section 4.4 we study normality of binary nonlinear codes and *subnormal* binary codes. It is an open problem whether or not all binary codes are *subnormal*.

The BDS construction simply means forming the union of  $t$  direct sums. This construction studied in Section 4.5 provides a natural generalization of the ADS and has been used to produce many good coverings. It gives rise to similar normality concepts.

### 4.1 Amalgamated direct sum

In this section we define the amalgamated direct sum (ADS) construction, *normal* and *subnormal* codes, and some other related concepts. We also discuss various basic results about ADS and normality. We begin with the definition

of a binary normal code.

**Definition 4.1.1** Let  $C$  be a binary  $(n, K)R$  code. For  $i = 1, 2, \dots, n$ , let  $C_0^{(i)}$  (respectively,  $C_1^{(i)}$ ) denote the set of codewords in which the  $i$ -th coordinate is 0 (respectively, 1). The integer

$$N^{(i)} = \max_{\mathbf{x} \in \mathbb{F}^n} \{d(\mathbf{x}, C_0^{(i)}) + d(\mathbf{x}, C_1^{(i)})\}$$

is called the norm of  $C$  with respect to the  $i$ -th coordinate and

$$N_{\min} = \min_i N^{(i)}$$

is called the minimum norm of  $C$ . (We use the convention that  $d(\mathbf{x}, \emptyset) = \infty$ .) The code  $C$  has norm  $N$  if  $N_{\min} \leq N$  and the coordinates  $i$  for which  $N^{(i)} \leq N$  are called acceptable with respect to  $N$ . If the code  $C$  is not clear from the context, we use the notations  $N^{(i)}(C)$  and  $N_{\min}(C)$ .

The code  $C$  is normal if it has norm  $2R+1$ . If  $N^{(i)} \leq 2R+1$ , then we say that the coordinate  $i$  is acceptable (short for acceptable with respect to  $2R+1$ ), or that  $C$  is normal with respect to the  $i$ -th coordinate. If  $C$  is not normal, it is called abnormal.

According to the previous definition a one-word code is not normal. In this chapter we assume that all codes have at least two codewords. One often defines  $d(\mathbf{x}, \emptyset) = n$  instead. Any code with at least two codewords is normal according to our definition if and only if it is normal according to this other definition. According to our definition, a coordinate that is identically 0 (or identically 1) is never acceptable, but would be acceptable using the other definition if  $n+R \leq 2R+1$ , i.e.,  $n \leq R+1$ .

In short, an  $(n, K)R$  code  $C$  is normal if there is a coordinate  $i$  such that

$$d(\mathbf{x}, C_0^{(i)}) + d(\mathbf{x}, C_1^{(i)}) \leq 2R+1 \text{ for all } \mathbf{x} \in \mathbb{F}^n. \quad (4.1.2)$$

If  $C$  is an  $(n, K)R$  code, we say that  $\mathbf{x} \in \mathbb{F}^n$  is bad for (coordinate)  $i$  if  $d(\mathbf{x}, C_0^{(i)}) + d(\mathbf{x}, C_1^{(i)}) > 2R+1$ , and  $\mathbf{x}$  is bad for  $C$  if it is bad for some  $i$ .

If an  $(n, K)R$  code  $C$  has norm  $N$ , then there is a coordinate  $i$  such that

$$d(\mathbf{x}, C_0^{(i)}) + d(\mathbf{x}, C_1^{(i)}) \leq N \text{ for all } \mathbf{x} \in \mathbb{F}^n,$$

and hence  $d(\mathbf{x}, C_0^{(i)}) \leq R$  or  $d(\mathbf{x}, C_1^{(i)}) \leq R$ . Therefore

$$R \leq \frac{1}{2}N. \quad (4.1.3)$$

Consequently, if  $C$  is normal, its minimum norm equals  $2R$  or  $2R+1$ .

The concept of normality is very suitable for binary linear codes. As we shall see in the next section, many binary linear codes are known to be normal, e.g., all linear codes with  $R \leq 3$ .

**Example 4.1.4** Consider the code

$$C = \{00000, 11000, 00111, 11111\}.$$

This code is the direct sum of the codes  $\{00, 11\}$  and  $\{000, 111\}$ , and hence its covering radius equals two. Now  $C_0^{(1)} = \{00000, 00111\}$  and  $C_1^{(1)} = \{11000, 11111\}$ , and we show that

$$d(\mathbf{x}, C_0^{(1)}) + d(\mathbf{x}, C_1^{(1)}) \leq 4, \quad (4.1.5)$$

for all  $\mathbf{x} \in \mathbb{F}^5$ , and that equality holds for instance when  $\mathbf{x} = 00001$ . In fact, we do not need to check that (4.1.5) holds for all  $\mathbf{x}$ . Of course, even checking all the 32 different choices for  $\mathbf{x}$  would be quite easy, but in many cases, e.g., in some proofs later on, it is very convenient to eliminate some of the cases using the following simple tricks.

First, we can use the fact that  $C$  is linear. Notice that if  $A \subseteq \mathbb{F}^n$ , then  $d(\mathbf{x}, A)$  is simply the smallest weight of the vectors in  $\mathbf{x} + A$ . Consequently,  $d(\mathbf{x} + \mathbf{y}, A) = d(\mathbf{x}, \mathbf{y} + A)$ . So, if  $\mathbf{x}$  and  $\mathbf{y}$  belong to the same coset, then  $\mathbf{y} = \mathbf{x} + \mathbf{c}$  for some codeword  $\mathbf{c} \in C$ , and

$$\begin{aligned} d(\mathbf{y}, C_0^{(i)}) + d(\mathbf{y}, C_1^{(i)}) &= d(\mathbf{x} + \mathbf{c}, C_0^{(i)}) + d(\mathbf{x} + \mathbf{c}, C_1^{(i)}) \\ &= d(\mathbf{x}, \mathbf{c} + C_0^{(i)}) + d(\mathbf{x}, \mathbf{c} + C_1^{(i)}) \\ &= d(\mathbf{x}, C_0^{(i)}) + d(\mathbf{x}, C_1^{(i)}), \end{aligned}$$

because  $\mathbf{c} + C_0^{(i)} = C_0^{(i)}$  and  $\mathbf{c} + C_1^{(i)} = C_1^{(i)}$  if  $\mathbf{c} \in C_0^{(i)}$ , and  $\mathbf{c} + C_0^{(i)} = C_1^{(i)}$  and  $\mathbf{c} + C_1^{(i)} = C_0^{(i)}$  if  $\mathbf{c} \in C_1^{(i)}$ . Hence, it is sufficient to consider one vector  $\mathbf{x}$  from each coset of  $C$ , for instance the vectors 00000, 00001, 00010, 00100, 10000, 10001, 10010, 10100.

Second, by symmetry — since any permutation that only changes the order of the last three coordinates belongs to the automorphism group of  $C$  — we can only consider the four cases  $\mathbf{x} = 00000, 00001, 10000, 10001$ .

Third, we observe that for the vector  $\mathbf{e}_1 = 10000$  we have

$$\begin{aligned} d(\mathbf{x} + \mathbf{e}_1, C_0^{(1)}) + d(\mathbf{x} + \mathbf{e}_1, C_1^{(1)}) &= d(\mathbf{x}, \mathbf{e}_1 + C_0^{(1)}) + d(\mathbf{x}, \mathbf{e}_1 + C_1^{(1)}) \\ &= d(\mathbf{x}, C_1^{(1)}) + d(\mathbf{x}, C_0^{(1)}) \end{aligned}$$

for all  $\mathbf{x} \in \mathbb{F}^5$ . Thus it is sufficient to check that (4.1.5) holds when  $\mathbf{x} = 00000$  and  $\mathbf{x} = 00001$ . In the latter case equality holds, in the former case the left hand side equals 2.

Therefore the norm of  $C$  with respect to the first coordinate is 4. Hence  $C$  is normal. By symmetry, also the second coordinate is acceptable. Similarly, we can check that the norm with respect to any of the last three coordinates is 5, so all the coordinates are acceptable.  $\square$

Recall that by Theorem 2.1.9, the covering radius of a binary linear  $[n, k]$  code  $C$  is the smallest number  $R$  such that every  $s \in \mathbb{F}^{n-k}$  can be written as a sum of at most  $R$  columns of its parity check matrix. In a similar way we can determine its norm with respect to any coordinate.

**Theorem 4.1.6** *Let  $C$  be a binary  $[n, k]R$  code with parity check matrix  $\mathbf{H}$  and consider a fixed coordinate  $i$ . For any  $s \in \mathbb{F}^{n-k}$ , let  $h_0(s)$  be the smallest number of columns of  $\mathbf{H}$  which add to  $s$ , not using the  $i$ -th column, and let  $h_1(s)$  be the minimum number, when the  $i$ -th coordinate must be used. We use the convention that  $h_0(s) = \infty$  (respectively,  $h_1(s) = \infty$ ) if  $s$  cannot be obtained in such a way. Then the norm of  $C$  with respect to the  $i$ -th coordinate is  $\max\{h_0(s) + h_1(s)\}$ , where the maximum is taken over all  $s \in \mathbb{F}^{n-k}$ .*

**Proof.** Let  $\mathbf{x} \in \mathbb{F}^n$  be arbitrary and  $s = \mathbf{Hx}^T$ . If the sum of columns  $i_1, \dots, i_t$  equals  $s$ , then the vector obtained by adding 1 to the coordinates  $i_1, \dots, i_t$  of  $\mathbf{x}$  belongs to  $C$ , and vice versa. Hence  $h_0(s)$  is the distance between  $\mathbf{x}$  and the nearest codeword of  $C$  that agrees with  $\mathbf{x}$  in the  $i$ -th coordinate, and  $h_1(s)$  is the distance between  $\mathbf{x}$  and the nearest codeword of  $C$  that disagrees with  $\mathbf{x}$  in the  $i$ -th coordinate.  $\square$

**Example 4.1.7** Consider the  $[10, 5, 3]$  code  $C$  with the generator matrix

$$\mathbf{G} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 \end{pmatrix}.$$

The code  $C$  has parity check matrix

$$\mathbf{H} = \begin{pmatrix} 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

Using Theorem 2.1.9 it is easy to see that the covering radius of  $C$  is 2.

It can be verified that this code is normal and the last nine coordinates are acceptable. (In fact, the last nine coordinates all occur in the support of a codeword of weight three, and the claim follows from Theorem 4.2.2 (ii).) However, the first coordinate is not acceptable. Indeed, if  $\mathbf{s}$  denotes the last column of  $\mathbf{H}$ , then using the previous theorem with  $i = 1$  we see that the norm with respect to the first coordinate is at least  $h_0(\mathbf{s}) + h_1(\mathbf{s}) = 1 + 5 = 6 > 5$ . In other words, the vector 0000000001 is bad for the first coordinate.  $\square$

We first discuss the amalgamated direct sum of two binary linear codes.

**Theorem 4.1.8** *Assume that  $A$  is a normal binary  $[n_A, k_A]R_A$  code with the last coordinate acceptable, and  $B$  is a normal binary  $[n_B, k_B]R_B$  code with the first coordinate acceptable. Then their amalgamated direct sum (ADS)*

$$\begin{aligned} A \dot{+} B &= \{(\mathbf{a}, 0, \mathbf{b}) : (\mathbf{a}, 0) \in A, (0, \mathbf{b}) \in B\} \\ &\cup \{(\mathbf{a}, 1, \mathbf{b}) : (\mathbf{a}, 1) \in A, (1, \mathbf{b}) \in B\} \end{aligned}$$

*is an  $[n_A + n_B - 1, k_A + k_B - 1]R$  code with  $R \leq R_A + R_B$ . More generally, if the norm of  $A$  with respect to the last coordinate is  $N_A$  and the norm of  $B$  with respect to the first coordinate is  $N_B$ , then the code  $A \dot{+} B$  has norm  $N_A + N_B - 1$  and hence covering radius at most  $\frac{1}{2}(N_A + N_B - 1)$ . In particular, if the covering radius of  $A \dot{+} B$  equals  $R_A + R_B$ , then  $A \dot{+} B$  is normal and the overlapping coordinate is acceptable.*

**Proof.** Clearly, the resulting code  $C = A \dot{+} B$  has length  $n_A + n_B - 1$ , is linear and has dimension  $k_A + k_B - 1$ .

Let  $\mathbf{z} = (\mathbf{x}, 0, \mathbf{y}) \in \mathbb{F}^{n_A + n_B - 1}$  be arbitrary, where  $\mathbf{x} \in \mathbb{F}^{n_A - 1}$  and  $\mathbf{y} \in \mathbb{F}^{n_B - 1}$ . Then

$$\begin{aligned} &d(\mathbf{z}, C_0^{(n_A)}) + d(\mathbf{z}, C_1^{(n_A)}) \\ &\leq \left( d((\mathbf{x}, 0), A_0^{(n_A)}) + d((0, \mathbf{y}), B_0^{(1)}) \right) \\ &\quad + \left( d((\mathbf{x}, 0), A_1^{(n_A)}) + d((0, \mathbf{y}), B_1^{(1)}) - 1 \right) \\ &= \left( d((\mathbf{x}, 0), A_0^{(n_A)}) + d((\mathbf{x}, 0), A_1^{(n_A)}) \right) \\ &\quad + \left( d((0, \mathbf{y}), B_0^{(1)}) + d((0, \mathbf{y}), B_1^{(1)}) \right) - 1 \\ &\leq N_A + N_B - 1. \end{aligned}$$

The same conclusion holds for the vector  $\mathbf{z} = (\mathbf{x}, 1, \mathbf{y})$ . Therefore  $C$  has norm  $N_A + N_B - 1$ . Because  $N_A \leq 2R_A + 1$  and  $N_B \leq 2R_B + 1$ , the code  $C$  has norm  $2R_A + 2R_B + 1$ , and by (4.1.3),

$$R \leq \frac{1}{2}(2R_A + 2R_B + 1),$$

i.e.,  $R \leq R_A + R_B$ . If equality holds, then  $C$  is normal and the coordinate  $n_A$  is acceptable.  $\square$

When we compare this code to the direct sum of  $A$  and  $B$  we see that we have obtained a code whose length and dimension are one smaller and whose covering radius is at least as small.

Of course, if  $A$  has length  $n_A$  and  $B$  has length  $n_B$  we can always form their ADS in  $n_A n_B$  different ways, so the ADS of two codes is not unique. If  $A$  and  $B$  are normal and the two chosen coordinates are acceptable, then we can use the previous theorem.

Assume that  $A$  and  $B$  are linear codes with generator matrices

$$\left( \begin{array}{ccccc} & 1 & 0 & 0 & 0 \\ & 0 & 1 & 0 & 0 \\ \mathbf{P} & & \ddots & & \\ & 0 & 0 & 0 & 1 \\ & 0 & 0 & 0 & 0 \end{array} \right)$$

and

$$\left( \begin{array}{ccc} 1 & 0 & 0 \\ \ddots & & \\ 0 & 0 & 1 \end{array} \mathbf{P}' \right).$$

When we form the ADS of  $A$  and  $B$  using the last coordinate of  $A$  and the first coordinate of  $B$ , the resulting code has generator matrix

$$\left( \begin{array}{ccccc} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ \mathbf{P} & & \ddots & & \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ & & & \ddots & \\ & & & 0 & 0 \end{array} \mathbf{P}' \right),$$

where all the blank entries are zeros.

For the illustration of ADS by means of parity check matrices, see Section 5.1.

**Example 4.1.9** The linear  $[3, 1]1$  code  $A = \{000, 111\}$  is normal. If  $B$  is a normal  $[n, k]R$  code and  $k \geq 1$ , then using the ADS construction we obtain an  $[n+2, k]R+1$  code  $C$ . The covering radius of  $C$  is indeed  $R+1$ : if  $d(\mathbf{x}, B) = R$  then  $d((1, 0, \mathbf{x}), C) = R+1$ .  $\square$

**Conjecture 4.1.10** Among the  $[n, k]R$  codes with  $k = k[n, R]$ , there exists at least one normal code. Consequently,

$$k[n+2, R+1] \leq k[n, R] \text{ for all } R < n. \quad (4.1.11)$$

In the same way we can form the ADS of two binary nonlinear codes. For nonlinear codes it is natural to define the following weaker concept.

**Definition 4.1.12** Let  $C$  be a binary  $(n, K)R$  code and  $C = C_1 \cup C_2$  be a partition of  $C$ , i.e.,  $C_1 \neq \emptyset$ ,  $C_2 \neq \emptyset$  and  $C_1 \cap C_2 = \emptyset$ . Then the subnorm of  $C$  with respect to this partition is

$$S(C_1, C_2) = \max_{\mathbf{x} \in \mathbb{F}^n} \{d(\mathbf{x}, C_1) + d(\mathbf{x}, C_2)\}$$

and

$$S_{\min} = \min S(C_1, C_2)$$

where the minimum is taken over all partitions of  $C$  is called the minimum subnorm of  $C$ . The code  $C$  has subnorm  $S$  if  $S_{\min} \leq S$  and any partition  $C_1 \cup C_2$  such that  $S(C_1, C_2) \leq S$  is called acceptable with respect to  $S$ .

The code  $C$  is subnormal if it has subnorm  $2R+1$ . If  $S(C_1, C_2) \leq 2R+1$ , then we say that the partition  $C_1 \cup C_2$  is acceptable (short for acceptable with respect to  $2R+1$ ), or that  $C$  is subnormal with respect to the partition  $C_1 \cup C_2$ .

In other words, an  $(n, K)R$  code  $C$  is subnormal if there is a partition  $C = C_1 \cup C_2$  such that

$$d(\mathbf{x}, C_1) + d(\mathbf{x}, C_2) \leq 2R+1 \text{ for all } \mathbf{x} \in \mathbb{F}^n.$$

If an  $(n, K)R$  code has subnorm  $S$ , then

$$R \leq \frac{1}{2}S, \tag{4.1.13}$$

and if  $C$  is subnormal, then its minimum subnorm is  $2R$  or  $2R+1$ . Clearly the minimum subnorm is at most the minimum norm.

We can now slightly modify the previous theorem.

**Theorem 4.1.14** Assume that  $A$  is a normal binary  $(n_A, K_A)R_A$  code with the last coordinate acceptable and  $B$  is a subnormal binary  $(n_B, K_B)R_B$  code with the partition  $B = B_1 \cup B_2$  acceptable. Then their amalgamated direct sum (ADS)

$$A \dot{+} B = \{(\mathbf{a}, \mathbf{b}) : (\mathbf{a}, 0) \in A, \mathbf{b} \in B_1\} \cup \{(\mathbf{a}, \mathbf{b}) : (\mathbf{a}, 1) \in A, \mathbf{b} \in B_2\}$$

is an  $(n_A + n_B - 1, K)R$  code with  $R \leq R_A + R_B$  and  $K = |A_0^{(n_A)}||B_1| + |A_1^{(n_A)}||B_2|$ . More generally, if the norm of  $A$  with respect to the last coordinate is  $N_A$  and the subnorm of  $B$  with respect to the partition  $B_1 \cup B_2$  is  $S_B$ , then the code  $A \dot{+} B$  has subnorm  $N_A + S_B - 1$  and covering radius at most  $\frac{1}{2}(N_A + S_B - 1)$ . In particular, if the covering radius of  $A \dot{+} B$  equals  $R_A + R_B$ , then  $A \dot{+} B$  is subnormal.

**Proof.** The proof is virtually identical to the proof of the previous theorem. Denote  $C = A \dot{+} B$ ,  $C_1 = \{(\mathbf{a}, \mathbf{b}) : (\mathbf{a}, 0) \in A, \mathbf{b} \in B_1\}$  and  $C_2 = \{(\mathbf{a}, \mathbf{b}) : (\mathbf{a}, 1) \in A, \mathbf{b} \in B_2\}$ . Let  $\mathbf{z} = (\mathbf{x}, \mathbf{y}) \in \mathbb{F}^{n_A+n_B-1}$  be arbitrary, where  $\mathbf{x} \in \mathbb{F}^{n_A-1}$  and  $\mathbf{y} \in \mathbb{F}^{n_B}$ . Then

$$\begin{aligned} & d(\mathbf{z}, C_1) + d(\mathbf{z}, C_2) \\ & \leq (d((\mathbf{x}, 0), A_0^{(n_A)}) + d(\mathbf{y}, B_1)) + (d((\mathbf{x}, 0), A_1^{(n_A)}) + d(\mathbf{y}, B_2) - 1) \\ & = (d((\mathbf{x}, 0), A_0^{(n_A)}) + d((\mathbf{x}, 0), A_1^{(n_A)})) + (d(\mathbf{y}, B_1) + d(\mathbf{y}, B_2)) - 1 \\ & \leq N_A + S_B - 1. \end{aligned}$$

Therefore  $C$  has subnorm  $N_A + S_B - 1$ . Because  $N_A \leq 2R_A + 1$  and  $S_B \leq 2R_B + 1$ , the code  $C$  has subnorm  $2R_A + 2R_B + 1$ , and  $R \leq R_A + R_B$  by (4.1.13). If equality holds, then  $C$  is subnormal.  $\square$

The code  $A \dot{+} B$  in the previous theorem is a subcode of the code  $A^* \oplus B$ . Here  $A^*$  denotes the code obtained by puncturing the last coordinate of  $A$ . Therefore its covering radius is always at least  $R_A + R_B - 1$  by Theorem 3.1.1.

One should notice that the definition of ADS as given in Theorem 4.1.8 is just a special case of the one given in the previous theorem. Indeed, if also  $B$  in the previous theorem is normal and the first coordinate is acceptable, and we choose  $B_1 = B_0^{(1)}$  and  $B_2 = B_1^{(1)}$ , then we obtain the same code  $A \dot{+} B$  as in Theorem 4.1.8.

In fact, we see that in Theorem 4.1.8 the code  $B$  does not have to be normal. Assume instead that  $B$  is subnormal and has an acceptable partition  $B_1 \cup B_2$  where  $B_1$  is a linear subcode of codimension 1, i.e., of dimension  $k_B - 1$ . We can then use the previous theorem, and still obtain a linear  $[n_A + n_B - 1, k_A + k_B - 1]R$  code with  $R \leq R_A + R_B$ .

**Example 4.1.15** The  $(3, 2)1$  code  $A = \{000, 111\}$  is normal. If  $B$  is a subnormal  $(n, K)R$  code with  $R < n$ , then using the ADS construction we obtain an  $(n + 2, K)R + 1$  code.  $\square$

**Conjecture 4.1.16** If  $R < n$ , there exists at least one subnormal code among the  $(n, K)R$  codes with  $K = K(n, R)$ . Consequently,

$$K(n + 2, R + 1) \leq K(n, R) \text{ for all } R < n. \quad (4.1.17)$$

**Theorem 4.1.18** If  $A$  or  $B$  is normal then so is their direct sum  $A \oplus B$ .

**Proof.** Denote  $A \oplus B$  by  $C$  and assume that  $A$  is normal with the first coordinate acceptable. For arbitrary  $\mathbf{x} \in \mathbb{F}^{n_A}$  and  $\mathbf{y} \in \mathbb{F}^{n_B}$  we have

$$d((\mathbf{x}, \mathbf{y}), C_0^{(1)}) + d((\mathbf{x}, \mathbf{y}), C_1^{(1)})$$

$$\begin{aligned}
&= d(\mathbf{x}, A_0^{(1)}) + d(\mathbf{y}, B) + d(\mathbf{x}, A_1^{(1)}) + d(\mathbf{y}, B) \\
&\leq 2R_A + 1 + 2R_B = 2R_C + 1,
\end{aligned}$$

and  $C$  is normal.  $\square$

**Theorem 4.1.19** *If  $1 \leq i \leq n$  and the norm of an  $(n, K)$  code  $C$  with respect to the  $i$ -th coordinate is  $N^{(i)}$ , then the norm of the extended code  $\widehat{C} = \{(\mathbf{c}, \pi(\mathbf{c})) : \mathbf{c} \in C\}$  with respect to the  $i$ -th coordinate equals  $2\lceil(N^{(i)} + 1)/2\rceil$ . In particular, if  $C$  is normal then so is  $\widehat{C}$ .*

**Proof.** Adding one more coordinate clearly increases the norm with respect to the  $i$ -th coordinate by at most two.

Let  $\mathbf{x} \in \mathbb{F}^n$  be arbitrary. Then all the codewords of  $C_0^{(i)}$  at distance  $d(\mathbf{x}, C_0^{(i)})$  from  $\mathbf{x}$  have the same (respectively, different) parity as  $\mathbf{x}$  if  $d(\mathbf{x}, C_0^{(i)})$  is even (respectively, odd). Hence  $d((\mathbf{x}, 0), \widehat{C}_0^{(i)}) + d((\mathbf{x}, 1), \widehat{C}_0^{(i)}) = 2d(\mathbf{x}, C_0^{(i)}) + 1$  and similarly  $d((\mathbf{x}, 0), \widehat{C}_1^{(i)}) + d((\mathbf{x}, 1), \widehat{C}_1^{(i)}) = 2d(\mathbf{x}, C_1^{(i)}) + 1$ . Therefore one of the integers  $d((\mathbf{x}, 0), \widehat{C}_0^{(i)}) + d((\mathbf{x}, 0), \widehat{C}_1^{(i)})$  and  $d((\mathbf{x}, 1), \widehat{C}_0^{(i)}) + d((\mathbf{x}, 1), \widehat{C}_1^{(i)})$  is at least  $d(\mathbf{x}, C_0^{(i)}) + d(\mathbf{x}, C_1^{(i)}) + 1$ . Hence the norm of  $\widehat{C}$  with respect to the  $i$ -th coordinate is at least  $N^{(i)} + 1$ .

Since all the codewords of  $\widehat{C}$  have even weight, the integers  $d(\mathbf{y}, \widehat{C}_0^{(i)})$  and  $d(\mathbf{y}, \widehat{C}_1^{(i)})$  have the same parity for all  $\mathbf{y} \in \mathbb{F}^{n+1}$  and  $i$ . Hence the norm of  $\widehat{C}$  with respect to the  $i$ -th coordinate is even.

If  $C$  is normal, so is  $\widehat{C}$ , because  $R(\widehat{C}) = R(C) + 1$  by Theorem 3.1.3.  $\square$

The following simple result gives a characterization of normality of a binary  $(n, K)R$  code in terms of the ADS construction: namely, if some ADS of  $C$  and the perfect repetition code of length  $2R + 3$  has covering radius  $2R + 1$ , then  $C$  is normal.

**Theorem 4.1.20** *If  $C$  is a binary  $(n, K)R$  code and adjoining  $2R + 2$  copies of the coordinate  $i$  to  $C$  increases its covering radius by exactly  $R + 1$ , then the code  $C$  is normal and the  $i$ -th coordinate is acceptable.*

**Proof.** Denote by  $D$  the resulting code. Let  $\mathbf{x} \in \mathbb{F}^n$  be arbitrary. Let  $\mathbf{u} \in \mathbb{F}^{2R+2}$  be any vector of weight  $\min\{2R+2, d(\mathbf{x}, C_1^{(i)})\}$ . Then  $d((\mathbf{x}, \mathbf{u}), D_1^{(i)}) \geq d(\mathbf{x}, C_1^{(i)}) + 2R + 2 - d(\mathbf{x}, C_1^{(i)}) = 2R + 2$ . Because  $D$  has covering radius  $2R + 1$ , we therefore have  $2R + 1 \geq d((\mathbf{x}, \mathbf{u}), D_0^{(i)}) = d(\mathbf{x}, C_0^{(i)}) + w(\mathbf{u}) = d(\mathbf{x}, C_0^{(i)}) + d(\mathbf{x}, C_1^{(i)})$  as claimed.  $\square$

## 4.2 Normality of binary linear codes

In this section we show how information about the code parameters can be used to deduce that many binary linear codes are normal. For normality results about certain well-known code families, like Reed-Muller and BCH codes, see Chapters 9 and 10.

We begin with a simple result giving an upper bound on the minimum norm of a binary linear code.

**Theorem 4.2.1** *If  $C$  is an  $[n, k]R$  code in which no coordinate is identically zero, then  $C$  has norm  $n$ .*

**Proof.** For arbitrary  $\mathbf{x} \in \mathbb{F}^n$ , and for  $j = 0, 1$ ,

$$d(\mathbf{x}, C_j^{(i)}) \leq \frac{1}{2^{k-1}} \sum_{\mathbf{c} \in C_j^{(i)}} d(\mathbf{x}, \mathbf{c}).$$

Therefore

$$d(\mathbf{x}, C_0^{(i)}) + d(\mathbf{x}, C_1^{(i)}) \leq \frac{1}{2^{k-1}} \sum_{\mathbf{c} \in C} d(\mathbf{x}, \mathbf{c}) = n,$$

since 0 and 1 both appear in each coordinate exactly  $2^{k-1}$  times.  $\square$

**Theorem 4.2.2 (i)** *If all binary linear codes with minimum distance  $2e + 1$  are normal and have at least two acceptable coordinates, then all binary linear codes with minimum distance  $2e + 2$  are normal.*

*(ii) For a binary linear code every coordinate in the support of a codeword of weight at most four is acceptable. In particular, all binary linear codes with minimum distance at most four are normal.*

**Proof.** (i) Let  $C$  be an  $[n, k, 2e+2]R$  code and  $\widehat{C} = \{(\mathbf{c}, \pi(\mathbf{c})) : \mathbf{c} \in C\}$  be the extended code. Assume that, e.g., the  $n$ -th coordinate is in the support of a minimum weight codeword of  $C$  (and hence  $\widehat{C}$ ), and denote by  $D$  the  $[n, k, 2e+1]$  code obtained by puncturing the  $n$ -th coordinate of  $\widehat{C}$ . By Theorem 3.1.3, the covering radius of  $\widehat{C}$  is  $R + 1$  and the covering radius of  $D$  is  $R$ . By the assumption,  $D$  is normal and  $N^{(i)}(D) \leq 2R + 1$  for some  $i \leq n - 1$ . By Theorem 4.1.19,  $N^{(i)}(\widehat{C}) = 2R + 2$ , and again by Theorem 4.1.19,  $N^{(i)}(C) < 2R + 2$ , completing the proof of (i).

(ii) Let  $C$  be an  $[n, k]R$  code. Assume that  $\mathbf{c} \in C$  has weight at most three and  $i \in \text{supp}(\mathbf{c})$ . We show that the  $i$ -th coordinate is acceptable.

Let  $\mathbf{x} \in \mathbb{F}^n$  be arbitrary and assume that the codeword  $\mathbf{c}' \in C$  satisfies the condition  $d(\mathbf{x}, \mathbf{c}') = d(\mathbf{x}, C)$ . We claim that

$$d(\mathbf{x}, C_0^{(i)}) + d(\mathbf{x}, C_1^{(i)}) \leq 2R + 1.$$

If  $d(\mathbf{x}, C) \leq R-1$ , then the claim is immediate, because  $d(\mathbf{x}, \mathbf{c}') + d(\mathbf{x}, \mathbf{c} + \mathbf{c}') \leq (R-1) + (R+2) = 2R+1$  and  $\mathbf{c}'$  and  $\mathbf{c} + \mathbf{c}'$  differ in the  $i$ -th coordinate. So assume that  $d(\mathbf{x}, C) = R$ . Because

$$\begin{aligned} d(\mathbf{x} + \mathbf{c}, C_0^{(i)}) + d(\mathbf{x} + \mathbf{c}, C_1^{(i)}) &= d(\mathbf{x}, \mathbf{c} + C_0^{(i)}) + d(\mathbf{x}, \mathbf{c} + C_1^{(i)}) \\ &= d(\mathbf{x}, C_1^{(i)}) + d(\mathbf{x}, C_0^{(i)}), \end{aligned}$$

it is sufficient to prove the claim when  $d(\mathbf{x}, C_0^{(i)}) = R$  and  $\mathbf{c}' \in C_0^{(i)}$ . If  $\mathbf{x}$  is bad for coordinate  $i$ , then  $d(\mathbf{x}, C_1^{(i)}) \geq R+2$ . Consequently,  $x_i = 1$ , otherwise  $d(\mathbf{x} + \mathbf{e}_i, C) = R+1$ . But then  $\mathbf{c} + \mathbf{c}'$  agrees with  $\mathbf{x}$  in the  $i$ -th coordinate and  $d(\mathbf{x}, \mathbf{c}') + d(\mathbf{x}, \mathbf{c} + \mathbf{c}') \leq R + (R+1) = 2R+1$ .

Assume now that  $\mathbf{c} \in C$  has weight four and  $i \in \text{supp}(\mathbf{c})$ . By permuting coordinates if necessary we may assume that  $n \in \text{supp}(\mathbf{c})$  and  $i \neq n$ . The same argument as in the proof of (i) shows that the  $i$ -th coordinate of  $C$  is acceptable.  $\square$

**Example 4.2.3** It is no longer true that every coordinate in the support of a codeword of weight five in a binary linear code is acceptable. Consider the code  $D$  generated by the matrix

$$\left( \begin{array}{cccccccccccccccc} 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \end{array} \right).$$

Notice that the first ten coordinates form the generator matrix of the  $[10, 5, 3]_2$  code  $C$  in Example 4.1.7. The minimum distance of  $D$  is equal to 5, and the first coordinate is in the support of a minimum weight codeword. However, we show that the first coordinate of  $D$  is not acceptable. The code  $D$  is obtained from  $C$  by taking four times the ADS with the code  $\{000, 111\}$ . By Theorem 4.1.8, the covering radius of  $D$  is 6. However, for the vector  $\mathbf{y} = 00000 00001 10101010$ ,  $d(\mathbf{y}, D_0^{(1)}) = d(00000 00001, C_0^{(1)}) + 4 = 5$  and  $d(\mathbf{y}, D_1^{(1)}) = d(00000 00001, C_1^{(1)}) + 4 = 9$ . Consequently,  $d(\mathbf{y}, D_0^{(1)}) + d(\mathbf{y}, D_1^{(1)}) = 14 > 2 \times 6 + 1$ .  $\square$

The following theorem also deals with nonlinear codes.

**Theorem 4.2.4** *Assume that  $C$  is an  $(n, K, d)R$  code.*

- (i) *If either  $d \geq 2R$ , or  $d = 2R-1$  and  $R$  does not divide  $n$ , then  $C$  is normal and all its coordinates are acceptable.*
- (ii) *If  $d = 2R-1$  and  $R$  divides  $n$ , but  $C$  is linear, then  $C$  is normal and at most one coordinate of  $C$  is not acceptable.*

**Proof.** If  $R = 0$  there is nothing to prove. Let  $R \geq 1$ .

(i) Assume that  $C$  is an  $(n, K, d)R$  code with  $d \geq 2R - 1$ . Assume on the contrary that the first coordinate is not acceptable, i.e., that

$$d(\mathbf{x}, C_0^{(1)}) + d(\mathbf{x}, C_1^{(1)}) > 2R + 1$$

holds for some  $\mathbf{x} \in \mathbb{F}^n$ . Let  $t = d(\mathbf{x}, C)$  and  $\mathbf{c} \in C$  be a codeword for which  $d(\mathbf{x}, \mathbf{c}) = t$ . By replacing  $C$  with the translate  $\mathbf{c} + C$  and  $\mathbf{x}$  with  $\mathbf{c} + \mathbf{x}$  if necessary we may assume that  $\mathbf{c} = 0$ . Because

$$d(\mathbf{x} + \mathbf{e}_1, C_0^{(1)}) + d(\mathbf{x} + \mathbf{e}_1, C_1^{(1)}) = d(\mathbf{x}, C_0^{(1)}) + d(\mathbf{x}, C_1^{(1)}),$$

we may further assume that  $x_1 = 0$ , and that  $\mathbf{x} = 01^t 0^{n-t-1}$ . Consider the vector  $\mathbf{y} = 1^{R+1} 0^{n-R-1}$ . There is a codeword  $\mathbf{b} \in C$  such that  $d(\mathbf{b}, \mathbf{y}) \leq R$ . Since  $w(\mathbf{y}) = R + 1$  and  $d \geq 2R - 1$ , we know that  $2R - 1 \leq w(\mathbf{b}) \leq 2R + 1$ . If  $\mathbf{b} \in C_1^{(1)}$ , then

$$\begin{aligned} d(\mathbf{x}, C_0^{(1)}) + d(\mathbf{x}, C_1^{(1)}) &\leq d(\mathbf{x}, \mathbf{0}) + d(\mathbf{x}, \mathbf{b}) \\ &\leq d(\mathbf{x}, \mathbf{0}) + d(\mathbf{x}, \mathbf{y}) + d(\mathbf{y}, \mathbf{b}) \\ &\leq t + (R + 1 - t) + R = 2R + 1. \end{aligned}$$

Therefore  $\mathbf{b} \in C_0^{(1)}$ . In particular,  $w(\mathbf{b}) = 2R - 1$ , because  $2R \leq w(\mathbf{b}) \leq 2R + 1$  implies that  $\text{supp}(\mathbf{y}) \subseteq \text{supp}(\mathbf{b})$ . If  $d \geq 2R$  we already have a contradiction. Now  $\text{supp}(\mathbf{x}) \subseteq \text{supp}(\mathbf{b})$  and  $t = d(\mathbf{x}, C) \leq d(\mathbf{x}, \mathbf{b}) = 2R - 1 - t$ , i.e.,  $t \leq R - 1$ . We can assume that  $\mathbf{b} = 01^{2R-1} 0^{n-2R}$ .

Consider now instead of  $\mathbf{y}$  the vector  $\mathbf{y}' = 1^R 0^{n-R} + \mathbf{e}_i$  where  $i > 2R$ . Applying the same argument we find a codeword  $\mathbf{b}'$  of weight  $2R - 1$  such that its first coordinate is 0 and  $\{2, 3, \dots, R, i\} \subseteq \text{supp}(\mathbf{b}')$ . Because  $d \geq 2R - 1$ , the codewords  $\mathbf{b}$  and  $\mathbf{b}'$  cannot have more than  $R - 1$  1's in common. When  $i$  goes through the values  $2R, 2R + 1, \dots, n$  we obtain  $(n - R)/R$  codewords of the form

$$\begin{array}{ccccccccc} & \overbrace{11\dots1}^{R-1} & \overbrace{11\dots1}^R & \overbrace{00\dots0}^R & \overbrace{00\dots0}^R & \dots & \overbrace{00\dots0}^R \\ 0 & 11\dots1 & 00\dots0 & 11\dots1 & 00\dots0 & \dots & 00\dots0 \\ 0 & 11\dots1 & 00\dots0 & 00\dots0 & 11\dots1 & \dots & 00\dots0 \\ & \vdots & & & & & & \\ 0 & 11\dots1 & 00\dots0 & 00\dots0 & 00\dots0 & \dots & 11\dots1. \end{array}$$

In particular,  $n$  must be divisible by  $R$ , proving (i).

(ii) Let  $\mathbf{c}_1$  be the sum of these  $(n - R)/R$  codewords. Because  $C$  is linear,  $\mathbf{c}_1 \in C$ . Suppose that the second coordinate is not acceptable either, and

that  $\mathbf{x}'$  is bad for it. We may assume that  $d(\mathbf{x}', C) = d(\mathbf{x}', \mathbf{0})$  by linearity, and further that  $x'_2 = 0$ .

Assume first that  $(n - R)/R$  is odd. Then  $\mathbf{c}_1 = 01^{n-1} \in C$ . Similarly we obtain a codeword  $\mathbf{c}_2 = 101^{n-2} \in C$ . But then  $110^{n-2} \in C$ , and the first two coordinates are acceptable by Theorem 4.2.2.

Assume therefore that  $(n - R)/R$  is even. Then  $\mathbf{c}_1 = 0^R 1^{n-R} \in C$ . By Theorem 4.2.2 we can assume that  $R \geq 2$ , because  $\mathbf{b} = 01^{2R-1} 0^{n-2R} \in C$ . It is not possible that  $\text{supp}(\mathbf{x}') \subseteq \{1, 2, \dots, R\}$ , because  $\mathbf{b} \in C$  would then imply that  $d(\mathbf{x}', \mathbf{b}) + d(\mathbf{x}', \mathbf{0}) \leq 2R + 1$ . Thus  $x'_i = 1$  for some  $i > R$ . In the same way as in the proof of (i) we find a codeword  $\mathbf{c}_2 \in C$  such that  $w(\mathbf{c}_2) = n - R$ ,  $c_{1,2} = 0 = c_{2,2}$  and  $c_{1,i} = 1 \neq c_{2,i} = 0$ . But then  $0 < d(\mathbf{c}_1, \mathbf{c}_2) \leq 2R - 2$ , a contradiction.  $\square$

The assumption of linearity in Theorem 4.2.4 (ii) cannot be dropped: it is shown in Corollary 4.3.9 that there are abnormal codes with  $R = 2$ ,  $d = 3$  for which  $n$  is even. A code satisfying the conditions of Theorem 4.2.4 (ii) can indeed have one unacceptable coordinate as shown by the simple example  $\{00^{2R-1}, 01^{2R-1}\}$  and the code in Example 4.1.7.

**Corollary 4.2.5** *All binary linear codes with  $R \leq 3$  are normal.*

**Proof.** Assume that  $C$  is a binary  $[n, k, d]R$  code. If  $d \leq 4$ , then the claim follows from Theorem 4.2.2. Otherwise,  $d \geq 2R - 1$  and the claim follows from the previous theorem.  $\square$

The following theorem summarizes other similar results known for binary linear codes.

**Theorem 4.2.6** *If  $C$  is an  $[n, k, d]$  code with  $n \leq 15$ ,  $k \leq 5$  or  $n - k \leq 9$ , then  $C$  is normal.*  $\square$

In the remainder of this section we only consider binary linear codes with no identically zero coordinates. Assume that  $k$  is fixed. Any binary linear code of dimension at most  $k$  can be obtained by assigning suitable multiplicities to the columns of the  $k$ -dimensional simplex code.

**Definition 4.2.7** *Let  $C$  be a binary code of length  $n$ , dimension at most  $k$  and covering radius  $R$  generated by the rows of a  $k \times n$  matrix  $\mathbf{G}$  with no zero columns. Let  $m_i$  denote the number of times the column that is the binary representation of  $i$  occurs in  $\mathbf{G}$ ,  $1 \leq i \leq 2^k - 1$ . The vector  $(m_1, m_2, \dots, m_{2^k-1})$  is called the signature of  $C$ . We then denote*

$$\mathcal{R}(C) = \mathcal{R}^{(k)}(m_1, \dots, m_{2^k-1}) = R - \sum_{i=1}^{2^k-1} \lfloor \frac{m_i}{2} \rfloor.$$

The contracted code  $\tilde{C}$  is generated by the rows of the matrix formed by taking one copy of each column of  $\mathbf{G}$  that has odd multiplicity. The length, dimension and covering radius of  $\tilde{C}$  are denoted by  $n_{\tilde{C}}$ ,  $k_{\tilde{C}}$  and  $R_{\tilde{C}}$ .

If all the components in the signature are even, the contracted code is not defined. Notice that the definition does not depend on the choice of  $\mathbf{G}$ . Clearly,

$$\mathcal{R}(C) = R - \frac{1}{2}n + \frac{1}{2}n_{\tilde{C}}. \quad (4.2.8)$$

Because  $R \leq n/2$  by Theorem 4.2.1, we know that

$$\mathcal{R}(C) \leq \lfloor \frac{1}{2}n_{\tilde{C}} \rfloor. \quad (4.2.9)$$

We now study how  $\mathcal{R}$  changes when the  $m_i$ 's increase but their parities remain unchanged. Two codes  $C$  and  $C'$  with signatures  $(m_1, m_2, \dots, m_{2^k-1})$  and  $(m'_1, m'_2, \dots, m'_{2^k-1})$  are called *congruent* if  $m_i \equiv m'_i \pmod{2}$  for all  $i$ . We then denote  $C \equiv D$ . If the multiplicities of the columns in  $C$  do not exceed the multiplicities of the same columns in  $D$ , we denote  $C \leq D$ .

**Theorem 4.2.10 (Monotonicity property)** *If  $C \equiv D$  and  $C \leq D$ , then  $\mathcal{R}(C) \leq \mathcal{R}(D)$ .*

**Proof.** It clearly suffices to prove the claim in the case when the last two coordinates of  $D$  are identical and  $C$  is obtained by puncturing these two coordinates. If  $C$  has covering radius  $R$ , then  $D$  has covering radius  $R+1$  or  $R+2$ , because  $d((\mathbf{x}, 0, 1), D) \geq d(\mathbf{x}, C) + 1$  for all  $\mathbf{x} \in \mathbb{F}^n$ . Consequently  $\mathcal{R}(D) \geq \mathcal{R}(C)$ .  $\square$

The previous proof shows that if all the components in the signature are even, then  $R = n/2$ . Therefore every code with dimension  $k \geq 2$  and covering radius  $t[n, k]$  has a contracted code.

Because  $C \equiv \tilde{C}$ , the monotonicity property implies that

$$\mathcal{R}(C) \geq \mathcal{R}(\tilde{C}) = R_{\tilde{C}} \geq 0. \quad (4.2.11)$$

We now show that  $t[n+2, k] = t[n, k] + 1$  for a fixed  $k$  when  $n$  is large enough.

Let  $k_B \leq k$  and  $B$  be an  $[n_B, k_B]$  projective code, i.e., a code with no zero or repeated columns, and

$$\mathcal{R}_n^*(B) = \min\{\mathcal{R}(C) : C \text{ is an } [n, k'] \text{ code with } k' \leq k, C \equiv B\}.$$

Equivalently, we go through all the  $k \times n$  matrices

$$\mathbf{G} = \left( \begin{array}{c|c} & \begin{matrix} 00\dots 0 \\ \vdots \\ 00\dots 0 \end{matrix} \\ \mathbf{G}_0 & \mathbf{G}(B) \end{array} \right) \quad (4.2.12)$$

where  $\mathbf{G}(B)$  is a  $k_B \times n_B$  generator matrix for  $B$  and every column in  $\mathbf{G}_0$  occurs an even number of times. Notice that the rank of  $\mathbf{G}$  may be smaller than  $k$ . For instance, if  $\mathbf{G}_0$  consists of  $n - n_B$  copies of a single column, then the code generated by the rows of  $\mathbf{G}$  has dimension  $k_B$  or  $k_B + 1$ .

By (4.2.8), the minimum covering radius of an  $[n, k']$  code  $C$  with  $k' \leq k$  and  $C \equiv B$  is

$$\frac{1}{2}n - \frac{1}{2}n_B + \mathcal{R}_n^*(B). \quad (4.2.13)$$

By the monotonicity property,  $\mathcal{R}_n^*(B)$  is nondecreasing with  $n$  and bounded above by  $\lfloor \frac{1}{2}n_B \rfloor$  by (4.2.9), and therefore for large  $n$ , it is a constant which we denote by  $\mathcal{R}_*(B)$ .

**Lemma 4.2.14** *Let  $B$  be a projective  $[n_B, k_B]$  code with  $k_B \leq k$ . For all sufficiently large  $n$  of the same parity as  $n_B$  there is a normal  $[n, k']$  code  $C$  with  $k' \leq k$ ,  $C \equiv B$  and  $\mathcal{R}(C) = \mathcal{R}_*(B)$ , which is generated by the rows of (4.2.12) where  $\mathbf{G}_0$  consists of  $n - n_B$  copies of a single column.*

**Proof.** For all  $n \equiv n_B \pmod{2}$ , let  $B_n^i$  denote the code generated by the rows of (4.2.12) when  $\mathbf{G}_0$  consists of  $n - n_B$  copies of the column that is the binary representation of  $i$ ,  $1 \leq i < 2^k$ . By the monotonicity property,  $\mathcal{R}(B_n^i)$  is nondecreasing with  $n$ . Furthermore,  $\mathcal{R}(B_n^i) \leq \lfloor \frac{1}{2}n_B \rfloor$  by (4.2.9), and hence, for a fixed  $i$ , the quantity  $\mathcal{R}(B_n^i)$  is a constant starting from some integer  $n(i)$ . Assume that  $\mathcal{R}(B_{n(r)}^r)$  is the smallest of the integers  $\mathcal{R}(B_{n(i)}^i)$ .

Assume that  $n > n(1) + \dots + n(2^k - 1)$  and that  $C$  is an  $[n, k']$  code such that  $k' \leq k$  and  $C \equiv B$ . Then for some  $i$  the column representing  $i$  appears in  $C$  at least  $n(i) + 1$  times. Hence  $C \geq B_{n(i)}^i$  and  $\mathcal{R}(C) \geq \mathcal{R}(B_{n(i)}^i)$ . This shows that  $\mathcal{R}_*(B) = \mathcal{R}(B_{n(r)}^r)$ .

By Theorem 4.1.20 the code  $B_n^r$  is normal for all  $n \geq n(r)$ , since adjoining any  $2s$  copies of the column representing  $r$  to  $B_n^r$  increases the covering radius by exactly  $s$ . Hence the code  $B_n^r$  is as required when  $n$  is large.  $\square$

**Theorem 4.2.15** *For a fixed  $k \geq 2$ , and all sufficiently large  $n$ ,*

$$t[n, k] = \frac{1}{2}n + \min_B \{\mathcal{R}_*(B) - \frac{1}{2}n_B\}, \quad (4.2.16)$$

where  $B$  ranges over all projective  $[n_B, k]$  codes with  $n \equiv n_B \pmod{2}$ ; in particular,

$$t[n+2, k] = t[n, k] + 1,$$

and furthermore, there is a normal  $[n, k]$  code attaining the bound  $t[n, k]$  in which all columns of the generator matrix have multiplicity one except for one column which has large multiplicity.

**Proof.** Trivially,  $t[n, k]$  equals the smallest possible covering radius of an  $[n, k']$  code with  $1 \leq k' \leq k$ .

For every projective code  $B$ , the minimum covering radius over all  $[n, k']$  codes  $C$  such that  $k' \leq k$  and  $C \equiv B$  is given by (4.2.13). Let  $n_0(B)$  be so large that the previous lemma holds and (4.2.13) equals  $\frac{1}{2}n + \mathcal{R}_*(B) - \frac{1}{2}n_B$  for all  $n \geq n_0(B)$ . There are only a finite number of projective codes  $B$  of dimension at most  $k$ ; let  $n_0 > k + \max_B n_0(B)$  where the maximum is taken over all such  $B$ . When  $n \geq n_0$ ,

$$t[n, k] = \frac{1}{2}n + \min_B \{\mathcal{R}_*(B) - \frac{1}{2}n_B\} \quad (4.2.17)$$

where  $B$  ranges over all projective  $[n_B, k_B]$  codes with  $n \equiv n_B \pmod{2}$  and  $k_B \leq k$ . Only the first term depends on  $n$ , and therefore  $t[n+2, k] = t[n, k] + 1$ .

Assume that the minimum of  $\mathcal{R}_*(B) - \frac{1}{2}n_B$  is attained by a projective  $[n_B, k_B]$  code  $B$ . We claim that the minimum is also attained by a projective code of dimension  $k$ . For any  $n \geq n_0$ , we can by the previous lemma adjoin  $n - n_B > k$  copies of a single column to  $B$  to obtain an  $[n, k']$  code  $C$  with  $k' \leq k$  such that  $\mathcal{R}(C) = \mathcal{R}_*(B)$ , i.e.,  $R(C) = t[n, k]$  by (4.2.17). Clearly  $k' = k_B$  or  $k' = k_B + 1$ . If  $k' = k_B + 1$  then  $C$  is generated by the matrix

$$\begin{pmatrix} 11\dots11 & 00\dots00 \\ 00\dots00 & \\ \vdots & \mathbf{G}(B) \\ 00\dots00 & \end{pmatrix},$$

and therefore  $C = A \oplus B$ , where  $A$  is the repetition code of length  $n - n_B$ , and  $t[n, k] = R(C) = R(A) + R(B)$ . Let  $C'$  be the code generated by

$$\begin{pmatrix} 11\dots11 & 00\dots00 \\ 00\dots00 & \\ \vdots & \mathbf{G}(B) \\ 00\dots01 & \end{pmatrix}.$$

By Theorem 3.4.2 this  $[n, k']$  code  $C'$  has covering radius at most  $R(A) + R(B) = t[n, k]$ , and hence  $R(C') = t[n, k]$ . If  $k' = k_B$ , then we simply define  $C' = C$ . In both cases  $C'$  is an  $[n, k']$  code with covering radius  $t[n, k]$  and has contracted code with dimension  $k'$ . Let  $C''$  be the code obtained by puncturing  $k - k'$  copies of the column with large multiplicity in  $C' \oplus \mathbb{F}^{k-k'}$ . Clearly  $C''$  is an  $[n, k]$  code with covering radius  $t[n, k]$ . The contracted code of  $C''$  has dimension  $k$  and must also attain the minimum in (4.2.17).

The last claim now immediately follows from the previous lemma.  $\square$

We discussed in the previous section that it is also useful to study binary linear codes  $C$  with an acceptable partition  $C_1 \cup C_2$  such that  $C_1$  is a linear

subcode of codimension 1. Of course, all normal codes have this property. The following theorem gives another family of codes with this property.

**Theorem 4.2.18** *Let  $C$  be a binary  $[n, k]R$  code. If*

$$2^{n-k}(2^{k-\lceil(n-R)/(R+1)\rceil}-1) < 2^k-1,$$

*then  $C$  is subnormal and has an acceptable partition  $H \cup (C \setminus H)$  where  $H$  is a linear subcode of  $C$  of dimension  $k-1$ . In particular, this is true if*

$$k/(n+1) > R/(R+1)$$

*or*

$$(n-k)/(n+1) > R/(R+1).$$

**Proof.** Given a coset  $C + \mathbf{y}$  with coset leader  $\mathbf{y}$  of weight  $w(\mathbf{y}) \leq R$ , let  $\mathbf{c}_1, \mathbf{c}_2, \dots, \mathbf{c}_m$  be a complete list of codewords such that  $d(\mathbf{y}, \mathbf{c}_i) \leq 2R+1-w(\mathbf{y})$ . Let  $H$  be a subspace of  $C$  of dimension  $k-1$ . If  $\mathbf{x} \in C + \mathbf{y}$ , then the fact that  $\mathbf{0} \in H$  implies that

$$d(\mathbf{x}, H) + d(\mathbf{x}, C \setminus H) = d(\mathbf{y}, H) + d(\mathbf{y}, C \setminus H) \leq 2R+1,$$

unless all the codewords  $\mathbf{c}_1, \dots, \mathbf{c}_m$  belong to  $H$ , or equivalently, the subspace  $V(\mathbf{y})$  generated by them is contained in  $H$ .

The number of  $(k-1)$ -dimensional subspaces  $H$  of  $C$  is  $2^k-1$ , and any subspace  $V(\mathbf{y})$  is contained in exactly  $2^{k-\dim V(\mathbf{y})}-1$  such subspaces  $H$ . Therefore it is sufficient to have

$$\sum(2^{k-\dim V(\mathbf{y})}-1) < 2^k-1,$$

where in the summation we take one  $\mathbf{y}$  from each coset. We claim that  $\dim V(\mathbf{y}) \geq (n-R)/(R+1)$ .

Assume that  $\mathbf{y}$  and  $\mathbf{z}$  are coset leaders and  $\text{supp}(\mathbf{y}) \subseteq \text{supp}(\mathbf{z})$ . Every codeword  $\mathbf{c}$  such that  $d(\mathbf{z}, \mathbf{c}) \leq 2R+1-w(\mathbf{z})$  also satisfies  $d(\mathbf{y}, \mathbf{c}) \leq d(\mathbf{y}, \mathbf{z}) + d(\mathbf{z}, \mathbf{c}) \leq (w(\mathbf{z})-w(\mathbf{y})) + (2R+1-w(\mathbf{z})) = 2R+1-w(\mathbf{y})$ . Thus  $\dim V(\mathbf{z}) \leq \dim V(\mathbf{y})$ . It is therefore sufficient to prove that  $\dim V(\mathbf{z}) \geq (n-R)/(R+1)$  when  $\text{supp}(\mathbf{z})$  is maximal.

Consider any  $j \notin \text{supp}(\mathbf{z})$ . By the maximality of  $\mathbf{z}$ , the vector  $\mathbf{z} + \mathbf{e}_j$  is not a coset leader, i.e., there is a codeword  $\mathbf{c} \neq \mathbf{0}$  such that  $d(\mathbf{z} + \mathbf{e}_j, \mathbf{c}) \leq w(\mathbf{z})$ . Because  $d(\mathbf{z}, \mathbf{c}) \geq w(\mathbf{z})$ , we have  $j \in \text{supp}(\mathbf{c})$ . On the other hand, because  $d(\mathbf{z}, \mathbf{c}) \leq d(\mathbf{z} + \mathbf{e}_j, \mathbf{c}) + 1 \leq w(\mathbf{z}) + 1$ , the set  $\text{supp}(\mathbf{c})$  can contain at most  $w(\mathbf{z}) + 1$  integers  $j \notin \text{supp}(\mathbf{z})$ . Any  $j' \notin \text{supp}(\mathbf{z}) \cup \text{supp}(\mathbf{c})$  is contained in the support of some codeword  $\mathbf{c}' \notin \{\mathbf{0}, \mathbf{c}\}$ , and clearly  $\mathbf{c}'$  and  $\mathbf{c}$  are linearly independent. All in all, there are  $n - w(\mathbf{z})$  elements  $j \notin \text{supp}(\mathbf{z})$ , and proceeding in the same way we obtain at least  $(n - w(\mathbf{z})) / (w(\mathbf{z}) + 1) \geq (n - R) / (R + 1)$  linearly independent codewords of  $V(\mathbf{z})$ .  $\square$

### 4.3 Abnormal binary nonlinear codes

Although no examples of abnormal binary linear codes are known, many abnormal binary nonlinear codes exist.

**Theorem 4.3.1** *Let  $B = \{\mathbf{b}_1, \mathbf{b}_2, \dots, \mathbf{b}_n\}$  be a binary code of length  $n$  and minimum distance  $d$ , and let*

$$T_i = \{\mathbf{y} \in \mathbb{F}^n : d(\mathbf{y}, \mathbf{b}_i) < \lfloor d/2 \rfloor, y_i = b_{i,i}\}.$$

*Then the code*

$$C = \mathbb{F}^n \setminus (T_1 \cup T_2 \cup \dots \cup T_n)$$

*has covering radius 1 and its minimum norm is greater than  $\lfloor d/2 \rfloor$ . In particular, if  $d \geq 6$ , then  $C$  is abnormal.*

**Proof.** We first prove that the covering radius of  $C$  is 1. By the triangle inequality, the sets  $T_i$  are disjoint. If  $\mathbf{z} \in \mathbb{F}^n$  and  $\mathbf{z} \notin C$ , then  $\mathbf{z} \in T_i$  for a unique  $i$ . Let  $\mathbf{c}$  be the vector obtained from  $\mathbf{z}$  by changing the  $i$ -th coordinate. Then  $d(\mathbf{z}, \mathbf{c}) = 1$ ,  $\mathbf{c} \notin T_i$  and  $d(\mathbf{c}, \mathbf{b}_i) \leq \lfloor d/2 \rfloor$ . Therefore  $d(\mathbf{c}, \mathbf{b}_j) \geq \lfloor d/2 \rfloor$  for all  $j \neq i$ , and  $\mathbf{c} \notin T_j$ . Hence  $\mathbf{c} \in C$  showing that the covering radius of  $C$  is 1.

By the construction, it is clear that  $d(\mathbf{b}_i, C_0^{(i)}) + d(\mathbf{b}_i, C_1^{(i)}) \geq \lfloor d/2 \rfloor + 1$  for all  $i$ . In particular, if  $d \geq 6$ , then the minimum norm of  $C$  is at least 4, and hence  $C$  is abnormal.  $\square$

For any fixed  $d$ , we can always find a code  $B$  of length  $n$  with  $n$  codewords and minimum distance  $d$ , when  $n$  is large enough. This follows from the Gilbert-Varshamov bound (Theorem 12.6.1), or, e.g., from the trivial lower bound

$$A(n, d) \geq 2^{\lfloor n/d \rfloor} \tag{4.3.2}$$

that we obtain by considering the codes  $D \oplus D \oplus \dots \oplus D$ , where  $D = \{0^d, 1^d\}$ .

The previous theorem therefore implies that for all sufficiently large  $n$  there exists an abnormal  $(n, \cdot)1$  code. The same is true for any fixed covering radius  $R$ . Indeed, if  $C$  is an abnormal  $(n, K)1$  code, then  $C \oplus \{0^{R-1}\}$  is an abnormal  $(n + R - 1, K)R$  code.

There are also several other ways of constructing abnormal codes with larger covering radius. Choose in the previous theorem  $d = 4R + 2$ . Assume that the code  $B = \{\mathbf{b}_1, \mathbf{b}_2, \dots, \mathbf{b}_n, \mathbf{b}_{n+1}\}$  has length  $n$  and minimum distance  $d$ , and let  $C$  be the code constructed in the previous theorem (using the first  $n$  vectors  $\mathbf{b}_1, \mathbf{b}_2, \dots, \mathbf{b}_n$ ). By the previous theorem, the minimum norm of the resulting code  $C$  is greater than  $2R + 1$ . The code  $C$  has covering radius 1, but we obtain a code  $C'$  with covering radius  $R$  simply by leaving out all the words in  $B_{R-1}(\mathbf{b}_{n+1})$ . The minimum norm of  $C'$  is at least  $2R + 2$ , and hence it is abnormal.

**Example 4.3.3** We now construct the smallest currently known abnormal binary code, which has length 9 and 118 codewords. We use the vectors

$$\begin{aligned}
 \mathbf{b}_1 &= 100110101 \\
 \mathbf{b}_2 &= 101010010 \\
 \mathbf{b}_3 &= 001000000 \\
 \mathbf{b}_4 &= 101001011 \\
 \mathbf{b}_5 &= 011000111 \\
 \mathbf{b}_6 &= 010101001 \\
 \mathbf{b}_7 &= 000111010 \\
 \mathbf{b}_8 &= 111111101 \\
 \mathbf{b}_9 &= 110001101.
 \end{aligned}$$

Although the conditions of Theorem 4.3.1 are not satisfied, we can check using a computer that the code

$$C = \mathbb{F}^9 \setminus (T_1 \cup T_2 \cup \dots \cup T_9),$$

where

$$T_i = \{\mathbf{y} \in \mathbb{F}^9 : d(\mathbf{y}, \mathbf{b}_i) \leq 2, y_i = b_{i,i}\},$$

has covering radius one, and is therefore abnormal. Any subcode of this code is also abnormal provided that it has covering radius one. Using a computer, an abnormal  $(9, 118)_1$  subcode of this  $(9, 258)_1$  code has been found. This  $(9, 118)_1$  code consists of the 81 words of the set  $F_1 \cup F_2 \cup \dots \cup F_9$ , where  $F_i = B_1(\mathbf{b}_i + \mathbf{e}_i) \setminus \{\mathbf{b}_i\}$  (cf. the proof of Theorem 4.4.6), and of the following 37 words:

$$\begin{array}{cccccccc}
 110110011 & 011011011 & 010000100 & 000000011 & 100100000 & 011011000 \\
 001110100 & 110110010 & 001110001 & 001001110 & 110001010 & 100101111 \\
 110010100 & 101000101 & 100000011 & 101101000 & 010011111 & 000101111 \\
 001100110 & 100011001 & 001001101 & 011101010 & 011011010 & 111010001 \\
 010011011 & 110010011 & 100011110 & 101011100 & 110111000 & 101111000 \\
 011101100 & 011011001 & 011110010 & 101100110 & 111100100 & 110100110 \\
 & 111000001.
 \end{array}$$

The vectors  $\mathbf{b}_i$  were constructed with the help of Corollary 4.4.5. The cardinality of  $C$  is much larger than that of the smallest known code of length 9 and covering radius 1 which has 62 codewords.  $\square$

In fact, for large  $n$  the smallest abnormal  $(n, \cdot)_1$  codes are not much bigger than the optimal codes.

**Theorem 4.3.4** For every  $\varepsilon > 0$  there is an integer  $n(\varepsilon)$  such that there is an abnormal  $(n, K)1$  code with

$$K \leq K(n, 1) + (\frac{1}{2} + \varepsilon)n^3$$

for all  $n \geq n(\varepsilon)$ .

**Proof.** If  $n$  is large enough, we can choose a code  $B = \{\mathbf{b}_1, \mathbf{b}_2, \dots, \mathbf{b}_n\}$  of length  $n$  and minimum distance 7. Denote

$$T_i = \{\mathbf{y} \in \mathbb{F}^n : d(\mathbf{y}, \mathbf{b}_i) \leq 2, y_i = b_{i,i}\},$$

and

$$T = T_1 \cup T_2 \cup \dots \cup T_n.$$

Let now  $C$  be a binary code attaining the bound  $K(n, 1)$ . Recall that its density is

$$\mu(n, 1) = K(n, 1)(n + 1)/2^n.$$

By replacing  $C$  with a suitable translate if necessary we can assume that

$$|C \cap T| \leq K(n, 1)nV(n - 1, 2)/2^n \leq \mu(n, 1)n^2/2 \leq (\frac{1}{2} + \varepsilon)n^2,$$

because  $\mu(n, 1) \leq 1 + 2\varepsilon$  for all sufficiently large  $n$  by Theorem 12.4.11. We now replace each word of  $C \cap T$  with  $n$  other vectors (some of which may already be codewords). If  $\mathbf{c} \in T_i$ , denote  $P(\mathbf{c}) = B_1(\mathbf{c} + \mathbf{e}_i) \setminus \{\mathbf{c}\}$ . Clearly  $P(\mathbf{c}) \cap T = \emptyset$  and  $B_1(P(\mathbf{c})) \supseteq B_1(\mathbf{c})$ . Hence

$$\left( C \cup \bigcup_{\mathbf{c} \in C \cap T} P(\mathbf{c}) \right) \setminus (C \cap T)$$

is an abnormal  $(n, K)1$  code with

$$K \leq K(n, 1) + (n - 1)|C \cap T| \leq K(n, 1) + (\frac{1}{2} + \varepsilon)n^3$$

as claimed.  $\square$

In view of possible generalizations of the nonlinear part of Theorem 4.2.4 we now try to construct abnormal codes whose minimum distance is large compared to  $R$ .

**Theorem 4.3.5** Assume that  $C \subseteq \mathbb{F}^n$  has covering radius  $R$  and minimum distance at least  $d$ , and  $B = \{\mathbf{b}_1, \mathbf{b}_2, \dots, \mathbf{b}_n\} \subseteq \mathbb{F}^n$  has minimum distance at least  $4R + d + 5$ . Denote

$$T_i = \{\mathbf{y} \in C : d(\mathbf{y}, \mathbf{b}_i) \leq 2R + 2, y_i = b_{i,i}\}.$$

Then

$$\left( C \setminus \bigcup_{i=1}^n T_i \right) \cup \left( \bigcup_{i=1}^n (\mathbf{e}_i + T_i) \right)$$

is an abnormal code with covering radius at most  $R+1$  and minimum distance at least  $d-1$ .

**Proof.** For each  $i$  we have replaced every codeword  $\mathbf{y} \in T_i$  with  $\mathbf{y} + \mathbf{e}_i$ . This decreases the minimum distance of the code by at most one since for  $\mathbf{y}_i \in T_i$ ,  $\mathbf{y}_j \in T_j$ ,  $i \neq j$  we have  $d(\mathbf{y}_i, \mathbf{y}_j) \geq 4R + d + 5 - (2R + 2) - (2R + 2) = d + 1$ . Since we are changing at most one coordinate in each codeword, the covering radius changes by at most one. Clearly for every  $i$ ,  $\mathbf{b}_i$  is bad for coordinate  $i$ , and  $C$  is abnormal.  $\square$

**Corollary 4.3.6** *For every  $R \geq 1$ , there is an  $n_0(R)$  such that for every  $n \geq n_0(R)$  there exists an abnormal binary code of length  $n$ , minimum distance at least  $R-1$  and covering radius at most  $R$ .*

**Proof.** Assume that  $R$  is arbitrary and  $C \subseteq \mathbb{F}^n$  has minimum distance  $R$  and is maximal, i.e., a code with the property that the minimum distance of  $C \cup \{\mathbf{x}\}$  is smaller than  $R$  for every  $\mathbf{x} \notin C$ . Then the covering radius of  $C$  is at most  $R-1$ . By the discussion following Theorem 4.3.1, for fixed  $R$ , there is an integer  $n_0$  such that for all  $n \geq n_0$  there exists a code  $B \subseteq \mathbb{F}^n$  with  $n$  codewords and minimum distance  $5R+1$ . The claim now follows from the previous theorem.  $\square$

**Corollary 4.3.7** *For every  $e \geq 1$  there is an  $m_0(e)$  such that for every  $m \geq m_0(e)$  there exists an abnormal binary code of length  $2^m-1$ , minimum distance at least  $2e$  and covering radius at most  $2e$ , and an abnormal binary code of length  $2^m$ , minimum distance at least  $2e+1$  and covering radius at most  $2e+1$ .*

**Proof.** By Theorem 10.3.12 the covering radius of the primitive BCH code of length  $2^m-1$  and designed distance  $2e+1$  is  $2e-1$  when  $m$  is large enough. The corresponding extended BCH code has length  $2^m$  and covering radius  $2e$ . The result now follows from Theorem 4.3.5.  $\square$

**Theorem 4.3.8** *Assume that  $C \subseteq \mathbb{F}^n$  has covering radius  $R$  and minimum distance at least  $d$  and has the property that  $d(\mathbf{x}, C_0^{(i)}) = d(\mathbf{x}, C_1^{(i)}) = R$*

for every  $i$  whenever  $d(\mathbf{x}, C) = R$ . Suppose that  $\{\mathbf{b}_1, \mathbf{b}_2, \dots, \mathbf{b}_n\} \subseteq \mathbb{F}^n$  has minimum distance at least  $6R + 1$ . Denote

$$T_i = \{\mathbf{y} \in C : d(\mathbf{y}, \mathbf{b}_i) \leq 2R, y_i = b_{i,i}\}.$$

If  $d \leq 2R$ , then

$$\left( C \setminus \bigcup_{i=1}^n T_i \right) \cup \left( \bigcup_{i=1}^n (\mathbf{e}_i + T_i) \right)$$

is an abnormal code with minimum distance at least  $d - 1$  and covering radius at most  $R$ .

**Proof.** We show that the covering radius of the resulting code  $C'$  is at most  $R$ . In exactly the same way as in the proof of Theorem 4.3.5 we then see that  $C'$  is abnormal and has minimum distance at least  $d - 1$ .

If  $d(\mathbf{x}, C) < R$ , then  $d(\mathbf{x}, C') \leq d(\mathbf{x}, C) + 1 \leq R$ . Assume that  $d(\mathbf{x}, C) = d(\mathbf{x}, \mathbf{c}_1) = R$ , where  $\mathbf{c}_1 \in C$ . If  $\mathbf{c}_1 \in C'$ , we are done, so assume that  $\mathbf{c}_1 \in T_i$  for some  $i$ . By the assumption on  $C$ , there is another codeword  $\mathbf{c}_2 \in C$  such that  $d(\mathbf{x}, \mathbf{c}_2) = R$  which disagrees with  $\mathbf{c}_1$  in the  $i$ -th coordinate. Consequently  $\mathbf{c}_2 \notin T_i$ . Moreover, for every  $j \neq i$ ,  $d(\mathbf{c}_2, \mathbf{b}_j) \geq d(\mathbf{b}_i, \mathbf{b}_j) - d(\mathbf{c}_2, \mathbf{b}_i) \geq d(\mathbf{b}_i, \mathbf{b}_j) - (d(\mathbf{c}_2, \mathbf{x}) + d(\mathbf{x}, \mathbf{c}_1) + d(\mathbf{c}_1, \mathbf{b}_i)) \geq 6R + 1 - R - R - 2R = 2R + 1$ , and hence  $\mathbf{c}_2 \notin T_j$ . Consequently,  $\mathbf{c}_2 \in C'$ , and  $d(\mathbf{x}, C') \leq R$ .  $\square$

Applying the previous theorem to the extended Hamming codes we obtain the following result. By Theorem 4.2.4, the minimum distance of the resulting code equals 3 and the covering radius equals 2.

**Corollary 4.3.9** *If  $m$  is large enough, there is an abnormal  $(2^m, \cdot, 3)2$  code.*

$\square$

## 4.4 Normality of binary nonlinear codes

We have seen in the previous section that abnormal binary nonlinear codes exist. However, we can prove a number of normality results for nonlinear codes. We show that all binary codes with covering radius one are subnormal, and that all binary  $(n, K)1$  codes with  $K < K(n, 1) + n$  are normal. In particular, all the optimal codes, for which  $K = K(n, 1)$ , are normal. In Theorem 4.2.4 we already proved that all binary codes with  $d \geq 2R$  are normal and all binary codes with  $d = 2R - 1$  are normal provided that  $R$  does not divide  $n$ .

Most of the results of this section are based on the following lemma.

**Lemma 4.4.1** *If  $C$  is an  $(n, K)1$  code and  $\mathbf{x}$  is bad for  $i$ , then either  $\mathbf{x} \in C$  or  $\mathbf{x} + \mathbf{e}_i \in C$ . If  $\mathbf{x} \in C$  is bad for  $i$ , then  $\mathbf{x} + \mathbf{e}_j \in C$  for all  $j \neq i$ .*

**Proof.** If  $C_0^{(i)} = \emptyset$  or  $C_1^{(i)} = \emptyset$  then the claim is obvious, so assume that  $C_0^{(i)} \neq \emptyset$  and  $C_1^{(i)} \neq \emptyset$ . Because  $\mathbf{x}$  is bad for  $i$ , we have  $d(\mathbf{x}, C_0^{(i)}) + d(\mathbf{x}, C_1^{(i)}) \geq 4$ . If  $\mathbf{x} \notin C$  and  $\mathbf{x} + \mathbf{e}_i \notin C$ , then  $d(\mathbf{x}, C_0^{(i)}) = 1$  and  $d(\mathbf{x}, C_1^{(i)}) \geq 3$ , or vice versa. Because  $d(\mathbf{x} + \mathbf{e}_i, C_a^{(i)})$  equals  $d(\mathbf{x}, C_a^{(i)}) - 1$  or  $d(\mathbf{x}, C_a^{(i)}) + 1$ , for  $a = 0, 1$ , we see that  $d(\mathbf{x} + \mathbf{e}_i, C_0^{(i)}) \geq 2$  and  $d(\mathbf{x} + \mathbf{e}_i, C_1^{(i)}) \geq 2$ , contradicting the fact that  $C$  has covering radius one. Thus  $\mathbf{x} \in C$  or  $\mathbf{x} + \mathbf{e}_i \in C$ . Suppose  $\mathbf{x} \in C$ . Without loss of generality,  $x_i = 0$ . Then  $d(\mathbf{x}, C_1^{(i)}) \geq 4$ , which implies that none of the vectors  $\mathbf{x} + \mathbf{e}_i + \mathbf{e}_j$ ,  $j \neq i$ , are covered by the words in  $C_1^{(i)}$ . But then they are all covered by the words of  $C_0^{(i)}$ , which means that all the vectors  $\mathbf{x} + \mathbf{e}_j$ ,  $j \neq i$ , belong to  $C$ .  $\square$

Notice that if  $C$  is an  $(n, K)1$  code and there is a vector which is bad for  $i$ , then Lemma 4.4.1 implies that there is a codeword which is bad for  $i$ .

If  $C$  is optimal, i.e.,  $K = K(n, 1)$ , and  $n \geq 3$ , there cannot be an index  $i$  such that  $\mathbf{x} \in C$  and  $\mathbf{x} + \mathbf{e}_j \in C$  for all  $j \neq i$ , because we could then replace  $\mathbf{x}$  and  $\mathbf{x} + \mathbf{e}_j$  (for one arbitrary  $j \neq i$ ) with the vector  $\mathbf{x} + \mathbf{e}_i + \mathbf{e}_j$  without increasing the covering radius. So, we have proved the following theorem.

**Theorem 4.4.2** *If  $C$  is an  $(n, K(n, 1))1$  code with  $n \geq 3$ , then  $C$  is normal and every coordinate is acceptable.*  $\square$

In fact, if  $C$  is an abnormal  $(n, K)1$  code we can find a normal  $(n, K)1$  code by changing some codewords in  $C$  in the following way. Let  $i$  be arbitrary,  $1 \leq i \leq n$ . If  $\mathbf{x} \in C$  is bad for  $i$  then by Lemma 4.4.1 we can replace  $\mathbf{x}$  with  $\mathbf{x} + \mathbf{e}_i$  without increasing the covering radius. After this change there are no vectors in  $B_1(\mathbf{x})$  that are bad for  $i$ . From now on, we shall never change any of the  $n$  codewords in  $B_1(\mathbf{x})$  again. We next search for a codeword  $\mathbf{y}$  that is bad for  $i$ . Clearly  $d(\mathbf{y}, \mathbf{x}) \geq 3$ . We change  $\mathbf{y}$  to  $\mathbf{y} + \mathbf{e}_i$  after which no vector in  $B_1(\mathbf{y})$  is bad for  $i$ . Proceeding in the same way we obtain a code whose  $i$ -th coordinate is acceptable.

**Theorem 4.4.3** *If  $C$  is an  $(n, K)1$  code and  $1 \leq i \leq n$ , we can find an  $(n, K)1$  code whose  $i$ -th coordinate is acceptable by changing the  $i$ -th coordinate in at most  $K/n$  codewords of  $C$ .*  $\square$

The following lemma provides a useful necessary condition for the existence of an abnormal  $(n, K)1$  code.

**Lemma 4.4.4** Suppose  $\mathbf{x} \in C$  is bad for  $i$ , and  $\mathbf{y} \in C$  is bad for  $j$ ,  $j \neq i$ . Then  $d(\mathbf{x}, \mathbf{y}) \geq 3$ . If  $d(\mathbf{x}, \mathbf{y}) \leq 4$  then  $x_i = y_i$  and  $x_j = y_j$ .

**Proof.** By Lemma 4.4.1,  $C$  contains the words  $\mathbf{x} + \mathbf{e}_h$ ,  $h \neq i$ . Assume that  $d(\mathbf{x}, \mathbf{y}) \leq 3$ . Then  $y_i = x_i$ , otherwise  $\mathbf{x}, \mathbf{y} \in C$  would imply that  $\mathbf{x}$  is not bad for  $i$ . Similarly  $y_j = x_j$ . If  $d(\mathbf{x}, \mathbf{y}) \leq 2$ , then  $\mathbf{x} + \mathbf{e}_j \in C$ ,  $\mathbf{y} \in C$ ,  $d(\mathbf{x} + \mathbf{e}_j, \mathbf{y}) \leq 3$  would imply that  $\mathbf{y}$  is not bad for  $j$ . Hence  $d(\mathbf{x}, \mathbf{y}) \geq 3$ . Suppose  $d(\mathbf{x}, \mathbf{y}) = 4$ . If  $x_i \neq y_i$  and  $x_h \neq y_h$ ,  $h \neq i, j$  then  $\mathbf{x} \in C$ ,  $\mathbf{y} + \mathbf{e}_h \in C$ ,  $d(\mathbf{x}, \mathbf{y} + \mathbf{e}_h) = 3$  would imply that  $\mathbf{x}$  is not bad for  $i$  because  $\mathbf{x}$  and  $\mathbf{y} + \mathbf{e}_h$  disagree in the  $i$ -th coordinate. Hence  $x_i = y_i$ . Similarly  $x_j = y_j$ .  $\square$

**Corollary 4.4.5** Suppose  $\mathbf{x} \notin C$  is bad for  $i$ , and  $\mathbf{y} \notin C$  is bad for  $j$ ,  $j \neq i$ . Then  $d(\mathbf{x}, \mathbf{y}) \geq 3$ . If  $d(\mathbf{x}, \mathbf{y}) \leq 4$  then  $x_i = y_i$  and  $x_j = y_j$ .

**Proof.** The vectors  $\mathbf{x} + \mathbf{e}_i$  and  $\mathbf{y} + \mathbf{e}_j$  satisfy the conditions of the previous lemma. Hence  $d(\mathbf{x} + \mathbf{e}_i, \mathbf{y} + \mathbf{e}_j) \geq 3$ ; and if  $d(\mathbf{x} + \mathbf{e}_i, \mathbf{y} + \mathbf{e}_j) \leq 4$  then  $x_i \neq y_i$ ,  $x_j \neq y_j$  and  $d(\mathbf{x}, \mathbf{y}) \geq 2 + d(\mathbf{x} + \mathbf{e}_i, \mathbf{y} + \mathbf{e}_j) \geq 5$ . If  $d(\mathbf{x} + \mathbf{e}_i, \mathbf{y} + \mathbf{e}_j) \geq 5$  then  $d(\mathbf{x}, \mathbf{y}) \geq 3$ , and  $d(\mathbf{x}, \mathbf{y}) \leq 4$  implies  $x_i = y_i$  and  $x_j = y_j$ .  $\square$

If  $\mathbf{x}$  and  $\mathbf{y}$  are both bad for  $i$  then it is obviously possible that  $d(\mathbf{x}, \mathbf{y}) < 3$ . E.g.,  $\mathbf{x} = 00111$ ,  $\mathbf{y} = 01111$ ,  $i = 1$ ,  $C = \{10000\} \cup (\{0\} \oplus \mathbb{F}^4)$ .

**Theorem 4.4.6** If  $n \geq 3$  and  $C$  is an  $(n, K)1$  code with  $s$  unacceptable coordinates, then

$$K \geq K(n, 1) + s.$$

In particular, if  $C$  is abnormal then

$$K \geq K(n, 1) + n.$$

**Proof.** For each unacceptable coordinate  $i$ , choose a codeword  $\mathbf{c}_i \in C$  bad for  $i$ . By Lemma 4.4.1,  $F_i = B_1(\mathbf{c}_i) \setminus \{\mathbf{c}_i + \mathbf{e}_i\} \subseteq C$ . Clearly  $\bigcup_{\mathbf{x} \in F_i} B_1(\mathbf{x}) = B_2(\mathbf{c}_i)$ , and as in the proof of Theorem 4.4.2, we can replace  $\mathbf{c}_i$  and  $\mathbf{c}_i + \mathbf{e}_j$  (for one arbitrary  $j \neq i$ ) with  $\mathbf{c}_i + \mathbf{e}_i + \mathbf{e}_j$  without increasing the covering radius. By Lemma 4.4.4, the distance between any two codewords  $\mathbf{c}_i$  is at least 3. We can do this replacement simultaneously for all  $F_i$ , and first delete  $2s$  codewords and then insert certain  $s$  vectors, without increasing the covering radius.  $\square$

**Theorem 4.4.7** If  $C$  is an abnormal  $(n, K)1$  code, then

$$K \geq \frac{2^n + (n-1)n(n+2)/2}{n+1}.$$

**Proof.** By Lemma 4.4.1, if  $\mathbf{c}_i \in C$  is bad for  $i$ , then  $F_i = B_1(\mathbf{c}_i) \setminus \{\mathbf{c}_i + \mathbf{e}_i\} \subseteq C$ . Each such set  $F_i$  contains  $n$  and covers  $V(n, 2)$  vectors. Therefore

$$K \geq \frac{2^n - nV(n, 2)}{V(n, 1)} + n^2$$

proving our claim.  $\square$

**Theorem 4.4.8** *If  $C$  is an  $(n, K)1$  code with  $n \geq 2$ , then  $C$  is subnormal.*

**Proof.** Consider a fixed coordinate  $i$ , and denote

$$A = \{\mathbf{x} \in C : \mathbf{x} \text{ is bad for coordinate } i\}.$$

By Lemma 4.4.1 the code  $C$  is normal if  $A = \emptyset$ , so we assume that  $A \neq \emptyset$ . Let  $T$  be a maximal subcode of  $A$  which has minimum distance two, i.e.,  $d(\mathbf{c}_1, \mathbf{c}_2) \geq 2$  for all  $\mathbf{c}_1, \mathbf{c}_2 \in T$  and  $d(\mathbf{c}, T) \leq 1$  for all  $\mathbf{c} \in A \setminus T$ . For every  $\mathbf{c} \in T$  we have, by Lemma 4.4.1,

$$F(\mathbf{c}) = \{\mathbf{c}\} \cup \{\mathbf{c} + \mathbf{e}_j : j \neq i\} \subseteq C,$$

and  $F(\mathbf{c}) \subseteq C_0^{(i)}$  or  $F(\mathbf{c}) \subseteq C_1^{(i)}$ .

We choose

$$C_0 = (C_0^{(i)} \cup T_1^{(i)}) \setminus T_0^{(i)}$$

$$C_1 = (C_1^{(i)} \cup T_0^{(i)}) \setminus T_1^{(i)}.$$

Then clearly  $C_0 \cup C_1 = C$ , and we claim that for this choice

$$d(\mathbf{x}, C_0) + d(\mathbf{x}, C_1) \leq 3 \text{ for all } \mathbf{x} \in \mathbb{F}^n.$$

Suppose first that  $d(\mathbf{x}, \mathbf{c}) \leq 2$  for some  $\mathbf{c} \in T$ . Assume further that  $\mathbf{c} \in C_0^{(i)}$  (the case  $\mathbf{c} \in C_1^{(i)}$  is similar). Then  $\mathbf{c} \in C_1$  and  $\mathbf{c} + \mathbf{e}_j \in C_0$  for all  $j \neq i$  by Lemma 4.4.1. If  $d(\mathbf{x}, \mathbf{c}) = 2$ , then  $d(\mathbf{x}, C_0) \leq 1$ ; if  $d(\mathbf{x}, \mathbf{c}) = 1$ , then  $d(\mathbf{x}, C_0) \leq 2$ ; if  $d(\mathbf{x}, \mathbf{c}) = 0$ , then  $d(\mathbf{x}, C_0) \leq 1$ . Anyway, we have  $d(\mathbf{x}, C_0) + d(\mathbf{x}, C_1) \leq 3$ .

We can therefore assume that  $d(\mathbf{x}, T) \geq 3$  (and  $n \geq 3$ ). If  $\mathbf{x}$  were bad for  $i$  then by Lemma 4.4.1,  $\mathbf{x} \in A$  or  $\mathbf{x} + \mathbf{e}_i \in A$ , but  $d(\mathbf{x}, T) \geq 3$  and  $d(\mathbf{x} + \mathbf{e}_i, T) \geq 2$  would contradict the maximality of  $T$ . Thus  $\mathbf{x}$  is not bad for  $i$ , i.e., there are codewords  $\mathbf{c}_0 \in C_0^{(i)}$  and  $\mathbf{c}_1 \in C_1^{(i)}$  such that  $d(\mathbf{x}, \mathbf{c}_0) + d(\mathbf{x}, \mathbf{c}_1) \leq 3$ . If  $\mathbf{c}_0 \notin T$  and  $\mathbf{c}_1 \notin T$  then we are already done. Clearly  $\mathbf{c}_0 \in T$ ,  $\mathbf{c}_1 \in T$  is not possible because  $d(\mathbf{x}, T) \geq 3$ . Assume therefore that  $\mathbf{c}_0 \in T$ ,  $\mathbf{c}_1 \notin T$  (the case  $\mathbf{c}_0 \notin T$ ,  $\mathbf{c}_1 \in T$  is similar). Because  $d(\mathbf{x}, \mathbf{c}_0) + d(\mathbf{x}, \mathbf{c}_1) \leq 3$  and  $d(\mathbf{x}, T) \geq 3$  we have  $d(\mathbf{x}, \mathbf{c}_0) = 3$ ,  $\mathbf{x} = \mathbf{c}_1$ . Now  $\mathbf{c}_0 \in C_1$ ,  $\mathbf{c}_1 \in C_1$ , and it is sufficient to find a

codeword  $\mathbf{c}_2 \in C_0$  such that  $d(\mathbf{x}, \mathbf{c}_2) \leq 3$ . By Lemma 4.4.1,  $\mathbf{c}_0 + \mathbf{e}_j \in C$  for all  $j \neq i$ . Choose now  $j$  in such a way that  $d(\mathbf{x}, \mathbf{c}_0 + \mathbf{e}_j) = 2$ . Then  $\mathbf{c}_0 + \mathbf{e}_j \in C_0^{(i)}$  and  $\mathbf{c}_0 + \mathbf{e}_j \notin T$  since  $T$  has minimum distance two, and consequently  $\mathbf{c}_0 + \mathbf{e}_j \in C_0$ .  $\square$

## 4.5 Blockwise direct sum

The ADS is obtained by taking the union of two direct sums (after puncturing). A natural generalization — both to binary and nonbinary codes — is to consider the union of a larger number of direct sums. In the following discussion we assume that  $V$ ,  $V_1$  and  $V_2$  are  $\mathbb{F}_q^n$ ,  $\mathbb{Z}_q^n$  or  $\mathbb{Z}_{q_1}\mathbb{Z}_{q_2}\dots\mathbb{Z}_{q_n}$ , but possibly for different values of  $n, q, q_1, \dots, q_n$ .

Assume that  $A_1, A_2, \dots, A_t \subseteq V_1$  and  $B_1, B_2, \dots, B_t \subseteq V_2$ . Consider the union

$$C = \bigcup_{i=1}^t (A_i \oplus B_i).$$

If

$$D_A = \{(d(\mathbf{x}, A_1), d(\mathbf{x}, A_2), \dots, d(\mathbf{x}, A_t)) : \mathbf{x} \in V_1\}$$

and

$$D_B = \{(d(\mathbf{y}, B_1), d(\mathbf{y}, B_2), \dots, d(\mathbf{y}, B_t)) : \mathbf{y} \in V_2\},$$

then the covering radius of  $C$  is the smallest  $R$  such that the sum of a vector from  $D_A$  and a vector from  $D_B$  has always at least one component less than or equal to  $R$ .

**Definition 4.5.1** *A family  $C_1, C_2, \dots, C_t \subseteq V$  has  $t$ -subnorm  $S$  if*

$$\min_{1 \leq i \leq t} d(\mathbf{x}, C_i) + \max_{1 \leq i \leq t} d(\mathbf{x}, C_i) \leq S \quad (4.5.2)$$

*holds for all  $\mathbf{x} \in V$ .*

Notice that in the previous definition we do not require that the sets  $C_i$  are disjoint. As before, we use the convention that  $d(\mathbf{x}, \emptyset) = \infty$ .

**Theorem 4.5.3** *Assume that the family  $A_1, A_2, \dots, A_t \subseteq V_1$  has  $t$ -subnorm  $S_A$  and the family  $B_1, B_2, \dots, B_t \subseteq V_2$  has  $t$ -subnorm  $S_B$ . Then the covering radius  $R$  of their blockwise direct sum (BDS)*

$$C = \bigcup_{i=1}^t (A_i \oplus B_i)$$

*satisfies the inequality*

$$R \leq \frac{1}{2}(S_A + S_B).$$

**Proof.** Let  $(\mathbf{x}, \mathbf{y}) \in V_1 \oplus V_2$  be arbitrary. Assume  $d(\mathbf{x}, A_u) = \min_i d(\mathbf{x}, A_i)$  and  $d(\mathbf{y}, B_v) = \min_i d(\mathbf{y}, B_i)$ . Then  $d(\mathbf{x}, A_i) \leq S_A - d(\mathbf{x}, A_u)$  for all  $i$  because the family  $A_1, A_2, \dots, A_t$  has  $t$ -subnorm  $S_A$ , and  $d(\mathbf{y}, B_i) \leq S_B - d(\mathbf{y}, B_v)$  for all  $i$ , because the family  $B_1, B_2, \dots, B_t$  has  $t$ -subnorm  $S_B$ . Consequently

$$\begin{aligned} 2d((\mathbf{x}, \mathbf{y}), C) &\leq d((\mathbf{x}, \mathbf{y}), A_u \oplus B_u) + d((\mathbf{x}, \mathbf{y}), A_v \oplus B_v) \\ &= d(\mathbf{x}, A_u) + d(\mathbf{y}, B_u) + d(\mathbf{x}, A_v) + d(\mathbf{y}, B_v) \\ &\leq d(\mathbf{x}, A_u) + (S_B - d(\mathbf{y}, B_v)) + (S_A - d(\mathbf{x}, A_u)) + d(\mathbf{y}, B_v) \\ &= S_A + S_B \end{aligned}$$

proving our claim.  $\square$

If  $C' \subseteq C$  and  $C$  is a union of  $t$  disjoint translates of  $C'$ , we denote by  $C/C'$  such a family of translates. Notice that if  $C = \mathbb{F}^n$  then  $C/C'$  has  $t$ -subnorm  $R'$ , where  $R'$  is the covering radius of  $C'$ .

By Theorem 2.6.5 the Hamming code  $\mathcal{H}_m$  of length  $2^m - 1$  is the union of  $2^{m-1}$  disjoint translates of the  $(2^m - 1, 2^{2^m-2^m}, 5)3$  punctured Preparata code  $\mathcal{P}_m^*$  for every even  $m \geq 4$ .

If  $\mathbf{x} \notin \mathcal{H}_m$ , then the fact that  $\mathcal{H}_m$  is perfect implies that there are  $2^{m-1}$  codewords  $\mathbf{c} \in \mathcal{H}_m$  such that  $d(\mathbf{c}, \mathbf{x}) \leq 2$ . Because the minimum distance of  $\mathcal{P}_m^*$  is 5, any two of these codewords have to be in different translates of  $\mathcal{P}_m^*$ , and hence there is exactly one in each translate. This shows that the family  $\mathcal{H}_m/\mathcal{P}_m^*$  has  $2^{m-1}$ -subnorm 3.

The extended Hamming code  $\widehat{\mathcal{H}}_m$  of length  $2^m$  is the union of  $2^{m-1}$  disjoint translates of the  $(2^m, 2^{2^m-2^m}, 6)4$  Preparata code  $\mathcal{P}_m$  for every even  $m \geq 4$ . The family  $\widehat{\mathcal{H}}_m/\mathcal{P}_m$  has  $2^{m-1}$ -subnorm 4. Indeed, because  $\mathcal{H}_m/\mathcal{P}_m^*$  has  $2^{m-1}$ -subnorm 3, the family  $\widehat{\mathcal{H}}_m/\mathcal{P}_m$  has trivially  $2^{m-1}$ -subnorm 5; furthermore, there are only even weight codewords in the family  $\widehat{\mathcal{H}}_m/\mathcal{P}_m$ , and therefore it has  $2^{m-1}$ -subnorm 4.

**Theorem 4.5.4** *There exists a  $(2^m + 2^{m-1} - 1, 2^{2^m+2^{m-1}-2^{m-1}}, 3)2$  code if  $m \geq 4$  is even.*

**Proof.** The family  $\mathbb{F}^{2^{m-1}-1}/\mathcal{H}_{m-1}$  has  $2^{m-1}$ -subnorm 1 and the family  $\widehat{\mathcal{H}}_m/\mathcal{P}_m$  has  $2^{m-1}$ -subnorm 4. Their BDS clearly has the required length, cardinality and minimum distance. By Theorem 4.5.3 the covering radius of the resulting  $(n, 2^{n-2^m}, 3)$  code is at most 2. However, it cannot be less than 2, because otherwise the code would be perfect and therefore  $n = 2^{2^m} - 1$ , a contradiction.  $\square$

**Example 4.5.5** Choosing  $m = 4$  in Theorem 4.5.4 we obtain a  $(23, 2^{15})2$  code. It is known that there is no linear  $[23, 15]2$  code, see Table 7.1.  $\square$

**Theorem 4.5.6** *There exists a  $(2^{m+1} - 1, 2^{2^{m+1} - 3m - 1}, 5)3$  code if  $m \geq 4$  is even.*

**Proof.** The family  $\mathcal{H}_m/\mathcal{P}_m^*$  has  $2^{m-1}$ -subnorm 3 and  $\widehat{\mathcal{H}}_m/\mathcal{P}_m$  has  $2^{m-1}$ -subnorm 4, and by Theorem 4.5.3 their BDS is as required. Because the resulting code is not perfect, its covering radius cannot be less than 3.  $\square$

Recall that the density of an  $(n, K)R$  code  $C$  is  $\mu(C) = KV(n, R)/2^n$ , the quotient of the cardinality of  $C$  and the sphere-covering lower bound. Denote

$$\mu_d(n, R) = \min\{\mu(C) : \text{an } (n, \cdot, d)R \text{ code } C \text{ exists}\}$$

and

$$\mu_d(R) = \liminf_{n \rightarrow \infty} \mu_d(n, R).$$

An easy calculation leads to the following corollary to Theorem 4.5.6.

**Corollary 4.5.7**  $\mu_5(3) \leq 4/3$ .  $\square$

In the same way Theorem 4.5.4 implies that  $\mu_3(2) \leq 9/8$ . This is improved in the following theorem.

**Theorem 4.5.8**  $\mu_3(2) = \mu_4(2) = 1$ .

**Proof.** Assume that  $C$  is an  $(n, 2^{n-m+1}, d)2$  code with  $d = 3$  or  $d = 4$ , and that there is a family  $\mathbb{F}^n/C$  consisting of  $2^{m-1}$  disjoint translates of  $C$ . This family has  $2^{m-1}$ -subnorm 2, and therefore by Theorem 4.5.3 the BDS of the families  $\mathcal{H}_m/\mathcal{P}_m^*$  and  $\mathbb{F}^n/C$  is a  $(2^m - 1 + n, 2^{2^m - 2m + n}, d)R$  code with  $R \leq 2$ . By the Notes about Section 5.4 we can choose  $C$  to be an  $[n, n - m + 1, 3]2$  code, where  $n = 5 \cdot 2^{m/2-2} - 1$  and  $m \geq 4$  is even. It is easy to verify that the density of the resulting code tends to 1, when  $n$  tends to infinity. Again it is easy to verify that the resulting code is not perfect and therefore has covering radius 2. This proves the first claim. By the Notes about Section 5.4 we can choose  $C$  to be an  $[n, n - m + 1, 4]2$  code, where  $n = 23 \cdot 2^{m/2-4} - 3$  and  $m \geq 10$  is even, and the second claim similarly follows.  $\square$

The following two definitions are useful in recording a few known results about nonbinary codes and BDS.

**Definition 4.5.9** A code  $C \subseteq V$  with covering radius  $R$  is  $t$ -subnormal if there is a partition  $C = C_1 \cup C_2 \cup \dots \cup C_t$ ,  $C_i \cap C_j = \emptyset$  whenever  $i \neq j$ , such that the family  $C_1, C_2, \dots, C_t$  has  $t$ -subnorm  $2R + 1$ .

**Definition 4.5.10** A code  $C \subseteq V$  with covering radius  $R$  is  $q$ -normal with respect to the  $i$ -th coordinate, if the  $i$ -th coordinate is  $q$ -ary, say over the alphabet  $Q = \{0, 1, \dots, q-1\}$  and the family  $C_0, C_1, \dots, C_{q-1}$  has  $q$ -subnorm  $2R$ , where  $C_a = \{(c_1, \dots, c_{i-1}, c_i + a, c_{i+1}, \dots, c_n) : \mathbf{c} \in C\}$  for all  $a \in Q$ . The code  $C$  is  $q$ -normal if it is  $q$ -normal with respect to some  $q$ -ary coordinate.

When  $C$  is a binary code and  $t = 2$ , the definitions of  $t$ -subnormal and  $t$ -normal codes reduce to the usual definitions of subnormality and normality.

Notice that in Theorem 4.5.3 there are  $t!$  different ways of pairing the sets  $B_j$  with the sets  $A_i$ , i.e., changing the indexing of the sets  $B_j$ . If  $A \subseteq V_1$  is a  $t$ -subnormal code with  $K_A$  codewords, and  $B \subseteq V_2$  a  $t$ -normal code with  $K_B$  codewords, then the average cardinality of the resulting code is  $K_A K_B / t$ . Therefore we can always find an indexing which results in a code with cardinality at most  $K_A K_B / t$ .

**Theorem 4.5.11** A nontrivial perfect code of length at least 2 is  $q$ -normal with respect to every  $q$ -ary coordinate.

**Proof.** Assume that  $C \subseteq \mathbb{Z}_q \oplus V$  is a nontrivial perfect code. Because  $C$  is nontrivial, its covering radius  $R$  satisfies the inequality  $n \geq 2R + 1$ . Consider the code  $C^*$  obtained by puncturing the first coordinate and denote

$$C_a = \{\mathbf{c} \in V : (a, \mathbf{c}) \in C\}.$$

Let  $\mathbf{x} \in V$  be arbitrary, and assume that  $d(\mathbf{x}, C^*) = d(\mathbf{x}, C_a) = s$ . We now show that

$$d(\mathbf{x}, C_i) = 2R - s$$

for all  $i \in \mathbb{Z}_q$ ,  $i \neq a$ , from which the claim follows.

Assume that the codeword  $\mathbf{c} \in C_a$  satisfies  $d(\mathbf{x}, \mathbf{c}) = s$ . Choose a vector  $\mathbf{y} \in V$  such that  $d(\mathbf{x}, \mathbf{y}) = R - s$  and  $d(\mathbf{c}, \mathbf{y}) = R$ . Then  $d((a, \mathbf{c}), (i, \mathbf{y})) = R + 1$  for every  $i \in \mathbb{Z}_q$ ,  $i \neq a$ . Because  $C$  is perfect there is a word  $(b, \mathbf{z}) \in C$  such that  $d((i, \mathbf{y}), (b, \mathbf{z})) \leq R$ . Then  $d((a, \mathbf{c}), (b, \mathbf{z})) \geq 2R + 1$  implies that  $b = i$ . Hence  $\mathbf{z} \in C_i$  and  $d(\mathbf{x}, C_i) \leq d(\mathbf{x}, \mathbf{z}) \leq d(\mathbf{x}, \mathbf{y}) + d(\mathbf{y}, \mathbf{z}) \leq R - s + R = 2R - s$ . On the other hand, the minimum distance of  $C^*$  is  $2R$ , and therefore if  $\mathbf{c}' \in C^*$  and  $\mathbf{c}' \neq \mathbf{c}$ , then  $d(\mathbf{x}, \mathbf{c}') \geq d(\mathbf{c}, \mathbf{c}') - d(\mathbf{c}, \mathbf{x}) \geq 2R - s$ . Consequently  $d(\mathbf{x}, C_i) \geq 2R - s$ .  $\square$

An immediate modification of the proof of Theorem 4.4.2 gives the following generalization.

**Theorem 4.5.12** *If  $n \geq 3$  and a code  $C \subseteq \mathbb{Z}_{q_1} \mathbb{Z}_{q_2} \dots \mathbb{Z}_{q_n}$  has covering radius 1 and is optimal, i.e., has the smallest cardinality among such codes, then  $C$  is 2-normal with respect to every binary coordinate.*  $\square$

When  $R = 1$  it is possible to generalize some of the results presented earlier in the binary case.

**Theorem 4.5.13** *For every  $n$  there exists an  $(n, K_3(n, 1))_{31}$  code which is 3-normal.*  $\square$

**Theorem 4.5.14** *All nontrivial linear  $q$ -ary codes with covering radius 1 are  $q$ -subnormal with the exception of the  $[4, 2]_{31}$  Hamming code; all of them are  $q$ -normal.*  $\square$

## 4.6 Notes

**§4.1** The concept of a normal code and ADS were defined by Graham and Sloane in [265] and the definition was extended to binary nonlinear codes in Cohen, Lobstein and Sloane [165]. In Graham and Sloane [265] the norm was defined to be what we have called the minimum norm. In the subsequent papers Cohen, Lobstein and Sloane [165], Sloane [591], Kilby and Sloane [374] and in fact also in the original manuscript of Graham and Sloane [265] the current definition of norm is used. (The term minimum norm is not used.) The definition of [265] is also commented in Bhandari and Garg [79]. In fact, our definition slightly differs from the one in [165], [591], [374] in one minor respect. Originally the term acceptable was used to mean what we call acceptable with respect to  $N$  (and  $N$  was assumed to be clear from the context). However, in normality proofs one almost exclusively chooses  $N = 2R + 1$ , and therefore in several papers the term acceptable is used in this more restricted sense. We have adopted the same practice, and as in Cohen, Litsyn, Lobstein and Mattson [158] use the term acceptable with respect to  $N$  in the more general case. Like, e.g., in Hou [335], we use the convention  $d(\mathbf{x}, \emptyset) = \infty$  instead of the more usual  $d(\mathbf{x}, \emptyset) = n$ . In this way we guarantee that the subsets of the codes  $A$  and  $B$  occurring in the definition of the ADS are always nonempty. As mentioned, this small change does not alter the meaning of normality for any code with at least two codewords.

Conjectures 4.1.10 and (4.1.17) are from Cohen, Lobstein and Sloane [165]. It has been shown in Lobstein [449] that the conjecture (4.1.11) is equivalent to the conjecture that  $t[n+2, k] \leq t[n, k] + 1$  for all  $k \geq 1$ ; see also Cohen, Litsyn, Lobstein and Mattson [158]. This conjecture is from Cohen, Karpovsky,

Mattson and Schatz [156]. It is shown in [156] that  $t[n+2, k] \leq t[n, k] + 1$  when  $n$  is large enough compared to  $n - k$ .

Examples 4.1.4, 4.1.7 and 4.1.9 and Theorems 4.1.6 and 4.1.8 are from Graham and Sloane [265]. Theorem 4.1.18 is from Kilby and Sloane [374]. The definition of a subnormal code is due to Honkala [309]. For another partitioning property, see Lobstein [449] and Cohen, Lobstein and Sloane [165]. Theorem 4.1.14 is from Honkala [312]. In the linear case this construction is called the *subspace direct sum* construction; see Calderbank [111]. Subnormal linear codes  $C$  with an acceptable partition  $C_1 \cup C_2$  where  $C_1$  is a linear subcode of codimension 1 have been considered in Honkala [312], and Calderbank [111] where they are called *codes with 1-norm  $2R + 1$* .

In [630] Struik defines an  $(n, K)R$  code  $C$  to be normal if it has subnorm  $S \leq 2R + 1$  and an acceptable partition  $C = C_1 \cup C_2$  such that the family  $C_1^*, C_2^*$  obtained by puncturing a suitable coordinate has 2-subnorm  $S' < S$ . Then the family  $C_1^*, C_2^*$  has 2-subnorm  $2R$ , and the code  $C' = (\{0\} \oplus C_1^*) \cup (\{1\} \oplus C_2^*)$  is an  $(n, K)$  code that has norm  $2R + 1$ . Conversely, if  $C'$  is any  $(n, K)$  code that has norm  $2R + 1$  with respect to the  $i$ -th coordinate, and  $C_0$  and  $C_1$  are obtained by puncturing the  $i$ -th coordinate of the codes  $C_0^{(i)}$  and  $C_1^{(i)}$  respectively, then the family  $C_0, C_1$  has 2-subnorm  $2R$ ; cf. Calderbank [111]. For the remark that the covering radius of  $A \dot{\oplus} B$  is at least  $R_A + R_B - 1$  and a discussion of the ADS construction and suitable conditions guaranteeing the normality of the resulting code, see Janwa and Mattson [351].

To obtain (4.1.17) it is sufficient to prove for all  $R < n$  that among the  $(n, K)R$  codes with  $K = K(n, R)$  there is a code  $C$  with a partition  $C = C_1 \cup C_2$  such that  $d(\mathbf{x}, C_1) + d(\mathbf{x}, C_2) \leq 2R + 1$  whenever  $d(\mathbf{x}, C) = R$ ; see Honkala [314] and Östergård [512]. In [512] such codes are called *semi-normal*. Conjecture (4.1.17) holds for  $R = 1$ , e.g., by Theorem 4.4.2. It was originally proved by verifying the conjecture for all  $n$ ; see Lobstein [449], Cohen, Lobstein and Sloane [165], [166] and Cohen [144].

Theorem 4.1.19 is from Graham and Sloane [265]. Our proof follows Struik [630, Lemma 4.15]. Theorem 4.1.20 is from Kilby and Sloane [374].

**§4.2** Theorem 4.2.1 is from Graham and Sloane [265]. It was shown in Cohen, Lobstein and Sloane [165] that a binary linear code with minimum distance  $d \leq 3$  is normal and every coordinate in the support of a minimum weight codeword is acceptable. The same result was stated for  $d = 4$  and  $d = 5$  in Kilby and Sloane [374]. However, as shown by Hou [332], see Example 4.2.3, the result no longer holds for  $d = 5$ . The case  $d = 4$  was proved in Hou [332]. The normality of binary linear codes with  $d = 5$  is an open problem. Theorem 4.2.2 (i) is due to Struik [630, Section 4.5] who used it to obtain the case  $d = 4$  from the case  $d = 3$ . In Struik [630] it is shown that if  $C$  is a binary code that is invariant under the translation  $\mathbf{x} \rightarrow \mathbf{x} + \mathbf{a}$  for some nonzero vector  $\mathbf{a}$  of weight at most 4, then  $C$  is normal with respect to every coordinate in the

support of  $\mathbf{a}$ ; our formulation of Theorem 4.2.2 (ii) is the special case when  $C$  is linear.

Theorem 4.2.4 is proved in Graham and Sloane [265] when  $d = 2R + 1$ , in van Wee [676] when  $d = 2R$ , in Hou [335] when  $d = 2R - 1$  and  $C$  is linear, and Etzion, Greenberg and Honkala [223] in the remaining case.

The normality of binary linear codes with  $R \leq 2$  was proved in Cohen, Lobstein and Sloane [165]. Corollary 4.2.5 is from Hou [332].

Normality of binary linear codes with  $k \leq 2$  was proved in Graham and Sloane [265], the case  $k = 3, 4$  in Sloane [591] and the case  $k = 5$  in Kilby and Sloane [374]. It is also shown in [374] that a binary linear code is normal if the contracted code  $\tilde{C}$  has dimension at most five. The normality of binary linear codes with  $n \leq 8$  was proved in Graham and Sloane [265] and with  $n \leq 12$  in Cohen, Lobstein and Sloane [165]. From the tables of Brouwer and Verhoeff [96] we see that every binary linear code of length at most 14 is normal, cf. Kilby and Sloane [374]. Indeed, all such codes satisfy  $k \leq 5$  or  $d \leq 4$ , except possibly a  $[14, 6, 5]_4$  code. However, a  $[14, 6, 5]_4$  code has a  $[9, 5, 3]$  residual code (cf. the proof of Lemma 8.1.11), which is maximal and therefore has covering radius at most 2. This implies that a  $[14, 6, 5]_4$  code has norm  $5 + 2 \cdot 2 = 9$  and is normal. Janwa and Mattson [350], [351] show that all binary linear codes with  $n = 15$  are normal. They also show that all binary linear codes with  $n - k \leq 9$  are normal, and establish the normality of some classes of codes of length 16 and codimension 10.

For Definition 4.2.7, see Cohen, Karpovsky, Mattson and Schatz [156] and Sloane [591]. The following discussion and Theorem 4.2.10 are from Sloane [591] and Lemma 4.2.14 and Theorem 4.2.15 are from Kilby and Sloane [374]. Theorem 4.2.18 is from Calderbank [111]; the second sufficient condition is from Struik [630].

It is shown in Graham and Sloane [265] that every binary linear  $[n, k, d]_R$  code has norm  $4R + 2$ . This was improved to  $4R - 1$  for  $R > 0$  in Janwa [345] and to  $3R + 1$  in Adams [8]. Hou [332] obtained the upper bounds  $2R + \lceil d/2 \rceil - 1$  for  $d \geq 3$ , and  $3R - 2$  for  $R \geq 3$ . For upper bounds depending on the contracted code  $\tilde{C}$  or  $k$ , see Sloane [591] and Janwa [345].

Other results about normality of binary linear codes can be found in Bhandari and Garg [80], Cohen, Lobstein and Sloane [165], Janwa [345], Kilby and Sloane [374], Mattson [472] and Sloane [591].

**§4.3** Theorem 4.3.1 is due to P. Frankl and is from Kilby and Sloane [374]. Abnormal codes with larger covering radius were first constructed in van Wee [676] using a construction different from the one presented here. Example 4.3.3 is from Honkala and Hämäläinen [323]. Theorem 4.3.4 is from Honkala [311] (where instead of Theorem 12.4.11 the result  $\mu(n, 1) \leq 3/2$  for all  $n$  from Beveraggi and Cohen [77] was used). Theorems 4.3.5 and 4.3.8 and Corollaries 4.3.6, 4.3.7 and 4.3.9 are from Etzion, Greenberg and Honkala

[223]. Applying Theorem 4.3.8 to long punctured Preparata codes of length  $2^{2m} - 1$  yields abnormal codes with minimum distance at least 4 and covering radius at most 3, and applying it to long Preparata codes of length  $2^{2m}$  yields abnormal codes with minimum distance at least 5 and covering radius at most 4; see [223].

§4.4 Theorem 4.4.2 has been proved independently by Hämäläinen in [323] and van Wee [676]. Our proof follows Honkala and Hämäläinen [323]. Lemma 4.4.4, Corollary 4.4.5 and Theorems 4.4.3, 4.4.6 and 4.4.7 are from [323].

If  $C$  is an abnormal  $(n, K)1$  code we can choose  $n$  codewords  $\mathbf{c}_1, \mathbf{c}_2, \dots, \mathbf{c}_n$  of  $C$  such that for every  $i$ ,  $\mathbf{c}_i$  is bad for coordinate  $i$ . Denote  $\mathbf{b}_i = \mathbf{c}_i + \mathbf{e}_i$ , and  $T_i = \{\mathbf{x} \in \mathbb{F}^n : d(\mathbf{x}, \mathbf{b}_i) \leq 2, x_i = b_{i,i}\}$ . Then it is clear that  $C \subseteq \mathbb{F}^n \setminus (T_1 \cup T_2 \cup \dots \cup T_n)$ . By Corollary 4.4.5,  $d(\mathbf{b}_i, \mathbf{b}_j) \geq 3$  for all  $i \neq j$ , and  $b_{i,i} = b_{j,i}$  and  $b_{i,j} = b_{j,j}$  whenever  $d(\mathbf{b}_i, \mathbf{b}_j) \leq 4$ . It is not difficult to show that such a code  $\{\mathbf{b}_1, \mathbf{b}_2, \dots, \mathbf{b}_n\}$  does not exist when  $n \leq 7$ . When  $n = 8$  it can be shown that such a code  $\{\mathbf{b}_1, \mathbf{b}_2, \dots, \mathbf{b}_n\}$  is essentially unique but any code  $C$  satisfying  $C \subseteq \mathbb{F}^n \setminus (T_1 \cup T_2 \cup \dots \cup T_n)$  has covering radius greater than one. For details, see Honkala and Hämäläinen [323]. Therefore an abnormal  $(n, K)1$  code must satisfy  $n \geq 9$ . By Theorem 4.4.7, the cardinality of any abnormal  $(n, K)1$  code with  $n \geq 9$  satisfies  $K \geq 91$ . By considering the case  $n = 9$  in more detail it has been shown in [323] that this estimate can be improved to  $K \geq 96$ .

Theorem 4.4.8 is from Honkala [314].

§4.5 The first generalization of the normality and subnormality and the ADS to the nonbinary case is due to Lobstein and van Wee [455]: an  $(n, K)R$  code  $C$  over  $\mathbb{Z}_q$  is called subnormal if there is a partition of  $C$  into  $q$  subsets  $C_1, C_2, \dots, C_q$  such that  $d(\mathbf{x}, C_1) + d(\mathbf{x}, C_2) + \dots + d(\mathbf{x}, C_q) \leq qR + q - 1$  for all  $\mathbf{x} \in \mathbb{Z}_q^n$ . This definition turned out to be quite restrictive, and they showed, for example, that the nontrivial perfect nonbinary codes are not subnormal. A similar definition for mixed codes is discussed in van Lint, Jr. [440]. In Östergård [512] a  $q$ -ary code  $C$  is defined to be  $p$ -seminormal if it can be partitioned into  $p$  subcodes  $C_1, C_2, \dots, C_p$  such that  $\max_i d(\mathbf{x}, C_i) \leq R + 1$  whenever  $d(\mathbf{x}, C) = R$ ; and seminormal if it is  $q$ -seminormal. It was shown in [512] that the Hamming codes can be combined efficiently with  $q$ -ary seminormal codes using the ADS construction. The definitions 4.5.1 and 4.5.9 are essentially from Honkala [313], cf. also Struik [630, Definition 4.11]. More generally, in Honkala [313] a family  $C_1, C_2, \dots, C_t \subseteq V$  whose union  $C$  has covering radius  $R$  is defined to have  $(t, u)$ -subnorm  $S$  if  $\min_{1 \leq i \leq t} d(\mathbf{x}, C_i) + \max_{1 \leq i \leq t} d(\mathbf{x}, C_i) \leq S$  whenever  $R - u \leq d(\mathbf{x}, C) \leq R$ . Definition 4.5.10 is from Östergård [514]; see also Honkala [313]. The BDS construction is a well-known construction of error-correcting codes: see Sloane, Reddy and Chen [596], MacWilliams and Sloane [464, Chapter 18, Construction X4], van Pul and Etzion [547] and Brouwer, Shearer, Sloane and W. D. Smith [95]. The

ADS can be viewed as a combination of puncturing and BDS. Theorem 4.5.3 is from Honkala [313]. For numerical applications and some related results, see Östergård [512], [514] and Honkala [319].

Theorems 4.5.4 and 4.5.6, Example 4.5.5 and Corollary 4.5.7 are from Etzion and Greenberg [222]. Theorem 4.5.8 is from Struik [630]. For other similar code families, see both Etzion and Greenberg [222] and Struik [630].

Theorem 4.5.11 is from Honkala [313]. Theorem 4.5.12 is from Hämäläinen (personal communication) and Honkala [311]. For the proofs of Theorems 4.5.13 and 4.5.14, see Honkala [313] and [319], respectively.

# Chapter 5

## Linear constructions

In this chapter, we discuss various constructions of linear — mostly binary — codes with best possible covering properties. We may want to find  $t[n, k]$ , that is, given the length  $n$  and the dimension  $k$ , the smallest possible covering radius of a linear code having these parameters. Or, given the length  $n$  and the covering radius  $R$ , we may wish to find  $k[n, R]$ , that is, the smallest possible dimension. A third alternative is, given the codimension (or redundancy)  $m$  and the covering radius  $R$ , to find the *length function*,  $\ell(m, R)$ , that is, the smallest possible length. Constructing linear codes with good covering properties can provide upper bounds on  $t[n, k]$ ,  $k[n, R]$ , or  $\ell(m, R)$ . Lower bounds are discussed in Chapter 7, where tables of the best known bounds on  $t[n, k]$  and  $\ell(m, R)$  are given in Section 7.3.

Some constructions mentioned in Chapters 3 and 4 can be extended to (or were first used for) linear codes; for instance, the direct sum construction (cf. Section 3.2), the amalgamated direct sum construction (cf. Section 4.1) and the blockwise direct sum (cf. Section 4.5). Local search (see Section 3.8) could also be used for finding good linear codes.

Here we concentrate on constructions specific to the linear case. Section 5.1 gives some useful properties of the functions  $t[n, k]$  and  $\ell(m, R)$ , as well as a matrix representation for the amalgamated direct sum of two linear codes. Section 5.2 deals with the case  $R = 1$  and the case of small dimensions ( $k \leq 8$ ), with an extensive use of the properties of Hamming, simplex and first order Reed-Muller codes. In Section 5.3 we show how to improve on the amalgamated direct sum of two Hamming codes. Section 5.4 is the core of this chapter and describes in detail one of the most efficient constructions for linear codes: Davydov's, which gives infinite families of covering codes, binary or nonbinary; however, here we only discuss the binary case. Notes at the end of the chapter contain supplementary remarks and references, mainly about the covering problem under conditions on the minimum distance, the

nonbinary case and the possible extension of Davydov's construction to the nonlinear case.

## 5.1 Basic facts about linear covering codes

The function  $t[n, k]$  gives the smallest possible covering radius among all  $[n, k]$  codes. The function  $\ell(m, R)$  is the smallest possible length of a code with codimension (or redundancy)  $m$  and covering radius  $R$ .

These two functions provide two different ways of giving the same information on covering codes; the values of one of them can be deduced from those of the other: for  $k < n$ ,  $t[n, k]$  is the smallest  $R$  such that  $\ell(n - k, R) \leq n$ ; and for  $m > 0$ ,  $\ell(m, R)$  is the smallest  $n$  such that  $t[n, n - m] \leq R$ . See also Section 7.3 for the respective advantages of functions  $t$  and  $\ell$ .

The function  $k[n, R]$ , the smallest possible dimension of a code with length  $n$  and covering radius  $R$ , is less often used (but its analogue in the nonlinear case,  $K(n, R)$ , is very much in use).

The following two theorems are direct consequences of the direct sum of two codes.

**Theorem 5.1.1** *For all integers  $n, n_1, n_2, k, k_1, k_2$  such that  $n \geq k \geq 0$ ,  $n_1 \geq k_1 \geq 0$ ,  $n_2 \geq k_2 \geq 0$ ,*

$$t[n_1 + n_2, k_1 + k_2] \leq t[n_1, k_1] + t[n_2, k_2], \quad (5.1.2)$$

$$t[n + 1, k] \leq t[n, k] + 1, \quad (5.1.3)$$

$$t[n + 1, k + 1] \leq t[n, k]. \quad (5.1.4)$$

□

**Theorem 5.1.5** *For all integers  $m_1, m_2, R_1, R_2$  such that  $m_1 \geq R_1 \geq 0$ ,  $m_2 \geq R_2 \geq 0$ ,*

$$\ell(m_1 + m_2, R_1 + R_2) \leq \ell(m_1, R_1) + \ell(m_2, R_2). \quad (5.1.6)$$

□

**Theorem 5.1.7** *For  $n \geq k \geq 1$ ,*

$$t[n, k] \leq \left\lceil \frac{n - k}{2} \right\rceil. \quad (5.1.8)$$

**Proof.** For any  $n$  and  $k$  with  $n \geq k \geq 1$ , we can choose a code with parity check matrix of the form  $\mathbf{H} = (\mathbf{I}_{n-k} | (1^{n-k})^T | \mathbf{H}')$ . Inequality (5.1.8) follows, by Theorem 2.1.9.  $\square$

The following three lemmas are less elementary, but are useful in the case of codes of small dimensions (see Theorems 5.2.3 and 5.2.7).

**Lemma 5.1.9** *For  $k \geq 4$  and  $n \geq 2^{k-2}$ ,*

$$t[n, k] \leq \left\lfloor \frac{n}{2} \right\rfloor - 2^{(k-4)/2}. \quad (5.1.10)$$

**Proof.** Set  $k' = k - 2$  and split  $n$  as  $n = 2^{k'} + (n - 2^{k'})$ ,  $k$  as  $k = (k' + 1) + 1$ . Then  $t[n, k] \leq t[2^{k'}, k' + 1] + t[n - 2^{k'}, 1]$ . Using an upper bound on the covering radius of the first order Reed-Muller code of length  $2^{k'}$  (see Corollary 9.2.5), we obtain:  $t[n, k] \leq (2^{k'-1} - 2^{(k'-2)/2}) + (\left\lfloor \frac{n}{2} \right\rfloor - 2^{k'-1})$ .  $\square$

**Lemma 5.1.11** *If  $k \geq 2$ , then*

$$t[n, k] \geq \lceil n/2 \rceil - 2^{k-2}. \quad (5.1.12)$$

**Proof.** Let  $C$  be an  $[n, k]R$  code, with generator matrix  $\mathbf{G}$ , assumed without all-zero column. Let  $\tilde{C}$  be the contracted  $[n_{\tilde{C}}, k_{\tilde{C}}]$  code of  $C$ :  $\tilde{C}$  has a generator matrix consisting of one copy of each column that appears an odd number of times in  $\mathbf{G}$  (see Definition 4.2.7). Obviously  $n$  and  $n_{\tilde{C}}$  have same parity and  $R \geq (n - n_{\tilde{C}})/2 + R(\tilde{C})$ .

On the other hand,  $\tilde{C}$  has no repeated column and is obtained from the simplex code (of length  $2^k - 1$ ) by puncturing  $2^k - 1 - n_{\tilde{C}}$  coordinates (see the definition of the simplex code in Section 2.6). Since the simplex code of length  $2^k - 1$  has covering radius  $2^{k-1} - 1$  (see Theorem 9.2.1) and since puncturing a code  $p$  times reduces its covering radius by at most  $p$  (see Theorem 3.1.1), we get  $R(\tilde{C}) \geq n_{\tilde{C}} - 2^{k-1} \geq \lceil n_{\tilde{C}}/2 \rceil - 2^{k-2}$ . So  $R \geq (n - n_{\tilde{C}})/2 + \lceil n_{\tilde{C}}/2 \rceil - 2^{k-2} = \lceil n/2 \rceil - 2^{k-2}$ .

We conclude by noting that no  $[n, k]$  code with covering radius  $t[n, k]$  need have the all-zero column in its generator matrix.  $\square$

**Lemma 5.1.13** *If  $k \geq 2$ , if  $n > 2^k + 1 - \max\{k, 2^{(k-2)/2}\}$  and if  $C$  is an  $[n, k]$  code that has covering radius  $R = t[n, k]$  and a generator matrix  $\mathbf{G}$  with no all-zero column, then  $\mathbf{G}$  has repeated columns and*

$$t[n, k] \geq t[n - 2, k] + 1. \quad (5.1.14)$$

**Proof.** Suppose that  $\mathbf{G}$  has no repeated columns. Then  $C$  is a punctured simplex code and  $R \geq 2^{k-1} - 1 - (2^k - 1 - n) = n - 2^{k-1}$ . On the other hand, Theorem 5.1.7 and Lemma 5.1.9 show that  $R \leq \lceil \frac{n-k}{2} \rceil$  for  $k \geq 2$  and  $R \leq \min\{\lceil \frac{n-k}{2} \rceil, \lfloor \frac{n}{2} \rfloor - 2^{(k-4)/2}\}$  for  $k \geq 4$ . But if these upper and lower bounds on  $R$  hold, then it is impossible to have  $n > 2^k + 1 - \max\{k, 2^{(k-2)/2}\}$ . So there is a column appearing at least twice in  $\mathbf{G}$ , which shows that  $R \geq 1 + t[n-2, k]$ . We conclude in the same way as for Lemma 5.1.11.  $\square$

Note that the condition  $n > 2^k + 1 - \max\{k, 2^{(k-2)/2}\}$  has been used only to force the generator matrix to have repeated columns. Any other way of proving that necessarily the generator matrix has repeated columns leads to inequality (5.1.14) (cf. proof of Theorem 5.2.7).

We end this section with the amalgamated and blockwise direct sums for linear codes. Actually ADS was introduced first for linear codes then extended without difficulty to the nonlinear case. Its main properties have been given in Section 4.1 and here we content ourselves with illustrating this construction by means of parity check matrices. Let  $C_1$  and  $C_2$  be two codes of length  $n_1$  and  $n_2$ , respectively, and with parity check matrices  $\mathbf{H}(C_1) = (\mathbf{x}_1 \mathbf{x}_2 \dots \mathbf{x}_{n_1})$  and  $\mathbf{H}(C_2) = (\mathbf{y}_1 \mathbf{y}_2 \dots \mathbf{y}_{n_2})$ ; assume that  $C_1$  is normal with the last coordinate acceptable and  $C_2$  is normal with the first coordinate acceptable (actually, one of the codes may be only subnormal). Then a parity check matrix,  $\mathbf{H}(C_1 \oplus C_2)$ , of the amalgamated direct sum of  $C_1$  and  $C_2$  is

$$\left( \begin{array}{ccc|c|cc} \mathbf{x}_1 & \dots & \mathbf{x}_{n_1-1} & \mathbf{x}_{n_1} & \mathbf{0} & \dots & \mathbf{0} \\ \mathbf{0} & \dots & \mathbf{0} & \mathbf{y}_1 & \mathbf{y}_2 & \dots & \mathbf{y}_{n_2} \end{array} \right)$$

where  $\mathbf{0}$ 's represent all-zero columns of appropriate lengths.

A particular case is when  $C_1$  is a normal  $[n, k]R$  code and  $C_2$  the repetition code of length  $2i+1$ . Then  $C_1 \oplus C_2$  is an  $[n+2i, k]R+i$  code, for  $i = 0, 1, \dots$

Linear codes can be obtained via BDS (cf. Section 4.5). We give an example proving that  $t[47, 28] \leq 5$ .

**Example 5.1.15** Let  $C_{23}$  be the binary  $[23, 12]3$  Golay code. There exists a  $[23, 16]2$  code  $D$  such that the families  $D/C_{23}$  and  $\widehat{D}/\widehat{C}_{23}$  have 16-subnorms 5 and 6, respectively. Their BDS yields a  $[47, 28]5$  code.  $\square$

## 5.2 The case $R = 1$ ; examples of small codes

The following theorem, which settles the case  $R = 1$ , stems from the existence of perfect Hamming codes, with parameters  $n = 2^m - 1$ ,  $k = n - m$ ,  $d = 3$

and  $R = 1$ , for  $m \geq 1$  (cf. Sections 2.6 and 11.1; see also Theorem 2.1.9: if  $R = 1$  all nonzero columns must occur).

**Theorem 5.2.1** *For all  $m \geq 1$ ,*

$$\ell(m, 1) = 2^m - 1. \quad (5.2.2)$$

□

The case of codes of small dimensions, namely up to  $k = 5$ , is completely solved.

**Theorem 5.2.3** *For all  $n \geq 1$ ,*

$$t[n, 1] = \left\lfloor \frac{n}{2} \right\rfloor. \quad (5.2.4)$$

*For all  $n \geq 2$ ,*

$$t[n, 2] = \left\lfloor \frac{n-1}{2} \right\rfloor. \quad (5.2.5)$$

*For all  $n \geq 3$ ,*

$$t[n, 3] = \left\lfloor \frac{n-2}{2} \right\rfloor. \quad (5.2.6)$$

**Proof.** Examples of  $[n, 1]$ ,  $[n, 2]$  and  $[n, 3]$  codes achieving, respectively,  $t[n, 1]$ ,  $t[n, 2]$  and  $t[n, 3]$  are the repetition code  $\{0^n, 1^n\}$ , the direct sum of the two codes  $\{0^{n-1}, 1^{n-1}\}$  and  $\{0, 1\}$ , and the direct sum of the three codes  $\{0^{n-2}, 1^{n-2}\}$ ,  $\{0, 1\}$  and  $\{0, 1\}$ , respectively. This proves the upper bounds.

For lower bounds, simply use Lemma 5.1.11 for dimension 2, and for dimension 3 when  $n$  is odd. For the case  $n$  even, we know (by the sphere-covering bound) that  $t[6, 3] = 2$ . Iteration of Lemma 5.1.13 gives the desired result.

□

**Theorem 5.2.7**  $t[5, 4] = 1$ ; for  $n \geq 4$  and  $n \neq 5$ ,

$$t[n, 4] = \left\lfloor \frac{n-4}{2} \right\rfloor. \quad (5.2.8)$$

$t[6, 5] = 1$ ; for  $n \geq 5$  and  $n \neq 6$ ,

$$t[n, 5] = \left\lfloor \frac{n-5}{2} \right\rfloor. \quad (5.2.9)$$

**Proof.** Examples of  $[n, 4]$  codes reaching  $t[n, 4]$  are given, for  $n$  even,  $n \geq 6$ , by the amalgamated direct sum of the  $[6, 4]1$  normal code  $\{000, 111\} \oplus \{0, 1\} \oplus \{0, 1\} \oplus \{0, 1\}$  on the one hand, and the normal code  $\{0^{n-5}, 1^{n-5}\}$  on the other hand. For  $n$  odd,  $n \geq 7$ , we take the amalgamated direct sum of the  $[7, 4]1$  normal Hamming code and  $\{0^{n-6}, 1^{n-6}\}$ .

Taking the direct sum of  $\{0, 1\}$  and an  $[n, 4]$  code achieving  $t[n, 4]$  yields an  $[n+1, 5]$  code with covering radius  $t[n+1, 5]$ .

For lower bounds, the sphere-covering bound shows that  $t[11, 4] = 3$  and  $t[13, 4] = 4$ ; using Lemma 5.1.13 repeatedly gives the result for dimension 4 and odd  $n$ .

We now show that  $t[12, 4] = 4$ , which, again by Lemma 5.1.13, ends the case of dimension 4 (for smaller values of  $n$ , the sphere-covering bound will do). Suppose on the contrary that  $t[12, 4] = 3$ . Then there must be repeated columns in the generator matrix of any  $[12, 4]3$  code  $C$  (for otherwise  $C$  can be obtained from the  $[15, 4]7$  simplex code by puncturing three times and therefore  $R(C) \geq 7 - 3$ , a contradiction). So  $R(C) \geq 1 + t[10, 4]$ . By the sphere-covering bound,  $t[10, 4] \geq 3$  and  $R(C) \geq 4$ .

The case of dimension 5 is harder. The sphere-covering bound shows that for  $n \leq 10$ ,  $t[n, 5] \geq \lfloor \frac{n-5}{2} \rfloor$ . A computer was used to show that any  $[11, 5]2$ ,  $[13, 5]3$ ,  $\dots$ ,  $[25, 5]9$  code necessarily has repeated columns in its generator matrix. Now consider an  $[11, 5]R$  code  $C$ . If  $C$  has a repeated column, then  $R \geq 1 + t[9, 5] = 3$ ; if not, the computer search shows that  $R \geq 3$ , i.e.,  $t[11, 5] = 3$  (and  $t[12, 5] = 3$ ). The same reasoning can be used for  $n$  up to 26. Let  $C$  be a  $[27, 5]R$  code. If  $C$  has a repeated column, then  $R \geq 1 + t[25, 5] = 11$ ; if not,  $C$  is a punctured  $[31, 5]15$  simplex code whose covering radius is at least  $15 - 4 = 11$ . The same reasoning leads to  $n = 31$ , and for  $n \geq 32$ , we are immediately done since only 31 nonzero columns of length 5 are available for a generator matrix (we need not use the all-zero column).  $\square$

For  $k = 6$  and  $k = 7$ , we have the following upper bounds.

**Theorem 5.2.10** For  $n \geq 14$ ,

$$t[n, 6] \leq \left\lfloor \frac{n-8}{2} \right\rfloor. \quad (5.2.11)$$

For  $n \geq 19$ ,

$$t[n, 7] \leq \left\lfloor \frac{n-9}{2} \right\rfloor. \quad (5.2.12)$$

**Proof.** The rows of the matrix

$$\left( \begin{array}{cccccccccccccc} 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 \end{array} \right)$$

span a  $[14, 6]3$  normal code  $C$ . Taking the amalgamated direct sum of  $C$  and the repetition code of length  $2i+1$  gives a  $[14+2i, 6]3+i$  code, which in turn gives a  $[15+2i, 7]3+i$  code.

The matrix

$$\left( \begin{array}{cccccccccccccc} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 \end{array} \right)$$

is the generator matrix of a  $[19, 6]5$  normal code and, in the same way, we get  $[19+2i, 6]5+i$  and  $[20+2i, 7]5+i$  codes.  $\square$

The above results suggest the following conjecture (compare with Theorem 4.2.15).

**Conjecture 5.2.13** For all  $p \geq 2$  and for  $n$  sufficiently large,

$$t[n, 2p] = \left\lfloor \frac{n - 2^p}{2} \right\rfloor, \quad (5.2.14)$$

$$t[n, 2p+1] = \left\lfloor \frac{n - 2^p - 1}{2} \right\rfloor. \quad (5.2.15)$$

For sufficiently large  $n$ , the following upper bounds can be established.

**Theorem 5.2.16** For all  $p \geq 2$  and for  $n \geq 2^{2p} - 1$ ,

$$t[n, 2p+1] \leq \left\lfloor \frac{n - 2^p}{2} \right\rfloor. \quad (5.2.17)$$

For all  $p \geq 2$  and for  $n$  even,  $n \geq 2^{2p-1}$ ,

$$t[n, 2p] \leq \left\lfloor \frac{n - 2^{(2p-1)/2}}{2} \right\rfloor. \quad (5.2.18)$$

For all  $p \geq 2$  and for  $n$  odd,  $n \geq 2^{2p-1} - 1$ ,

$$t[n, 2p] \leq \left\lfloor \frac{n - 2^{(2p-1)/2} - 1}{2} \right\rfloor. \quad (5.2.19)$$

**Proof.** It is known (see Section 9.2 on Reed-Muller codes) that first order Reed-Muller  $[2^{2p}, 2p+1]$  codes have covering radius  $R = 2^{2p-1} - 2^{p-1}$  and are normal, and that punctured first order Reed-Muller  $[2^{2p}-1, 2p+1]$  codes have covering radius  $R-1$  and are normal. Using the amalgamated direct sum of these codes and a repetition code of odd length yields the first part of the theorem.

For even dimension, first order Reed-Muller codes are only conjectured to be normal and their covering radius is not known. However, it is possible to use some properties of norms (cf. Section 9.2): first order Reed-Muller  $[2^{2p-1}, 2p]$  codes have norm

$$N = \lfloor n - \sqrt{n} \rfloor = \lfloor 2^{2p-1} - 2^{(2p-1)/2} \rfloor. \quad (5.2.20)$$

Thus, for all  $i \geq 0$ , one can construct  $[2^{2p-1} + 2i, 2p]$  codes with norm  $N + 2i$  and covering radius at most  $R$ , where  $R = \lfloor (N + 2i)/2 \rfloor$ ; because they are even weight, these codes in turn produce, when punctured,  $[2^{2p-1} + 2i - 1, 2p]$  codes with covering radius at most  $R-1$  (see Theorem 3.1.3).  $\square$

The first part of Theorem 5.2.16 can be slightly improved: inequality (5.2.17) holds for all  $n \geq 2^{2p} - 2^{p+1} + 3$ . Indeed, the first order Reed-Muller  $[2^{2p}, 2p+1]$  code is self-complementary and has strength 2 (its dual being an extended Hamming code — see the last paragraph of Section 2.2) and the same is true for any code obtained by puncturing any number of coordinates. If we puncture at most  $2^{p+1} - 3$  coordinates, we obtain a code with length  $n$  between  $2^{2p}$  and  $2^{2p} - 2^{p+1} + 3 = (2^p - 1)^2 + 2$ . From Section 9.2, we know that this new code has norm  $\lfloor n - \sqrt{n-1} \rfloor = n - 2^p$  and its covering radius is at most half of that.

Finally, a recent result, proving that the  $[128, 8]56$  first order Reed-Muller code is normal (see Theorem 9.2.24), yields an upper bound on  $t[n, 8]$  which coincides with its conjectured exact value in (5.2.14).

**Theorem 5.2.21** For  $n \geq 127$ ,

$$t[n, 8] \leq \left\lfloor \frac{n - 16}{2} \right\rfloor. \quad (5.2.22)$$

$\square$

### 5.3 Saving more than one coordinate

Let  $C_1$  and  $C_2$  be  $[n_1, k_1]R_1$  and  $[n_2, k_2]R_2$  codes, respectively. Taking their direct sum yields an  $[n_1 + n_2, k_1 + k_2]R_1 + R_2$  code. Their amalgamated direct sum possibly yields an  $[n_1 + n_2 - 1, k_1 + k_2 - 1]R_1 + R_2$  code. This proves that inequality (5.1.2) holds:

$$t[n_1 + n_2, k_1 + k_2] \leq t[n_1, k_1] + t[n_2, k_2],$$

and, if the amalgamated direct sum works best:

$$t[n_1 + n_2 - 1, k_1 + k_2 - 1] \leq t[n_1, k_1] + t[n_2, k_2]. \quad (5.3.1)$$

This is why the amalgamated direct sum of two codes is said to *save one coordinate* over their direct sum. This can be expressed even better in terms of the function  $\ell$ ; inequality (5.1.2) is equivalent to inequality (5.1.6):

$$\ell(m_1 + m_2, R_1 + R_2) \leq \ell(m_1, R_1) + \ell(m_2, R_2)$$

and inequality (5.3.1) reads:

$$\ell(m_1 + m_2, R_1 + R_2) \leq \ell(m_1, R_1) + \ell(m_2, R_2) - 1. \quad (5.3.2)$$

One can do better with Hamming codes. Let  $A$  and  $B$  be two Hamming codes of lengths  $n_A = 2^m - 1$  and  $n_B = 2^{m+i} - 1$  ( $i = 0, 1, \dots$ ), dimensions  $k_A = 2^m - m - 1$  and  $k_B = 2^{m+i} - (m + i) - 1$ , and covering radius 1. Let  $n_i = n_A + n_B - 1 = 2^{m+i} + 2^m - 3$ . Codes  $A$  and  $B$  are normal, so:

$$\ell(2m + i, 2) \leq n_i. \quad (5.3.3)$$

Let  $\Psi_A$  (respectively,  $\Psi_B$ ) be the set of all binary columns of length  $m$  (respectively,  $m + i$ ), except the all-one and all-zero columns. Let  $\Omega_A \subseteq \Psi_A$  and  $\Omega_B \subseteq \Psi_B$  be two sets to be specified and  $\Omega_A^c = \Psi_A \setminus \Omega_A$ ,  $\Omega_B^c = \Psi_B \setminus \Omega_B$ . Consider the  $(2m + i) \times (n_i - 1)$  matrix

$$\mathbf{H} = \left( \begin{array}{c|c|c|c} \Omega_A & \Omega_A^c & \mathbf{0} & \mathbf{1} \\ \hline \mathbf{0} & 1 & \Omega_B & \Omega_B^c \end{array} \right)$$

where  $\mathbf{0}$  and  $\mathbf{1}$  represent all-zero and all-one matrices of appropriate sizes. For  $m = 3$  and  $i \geq 1$ , or for  $m \geq 4$ , it is then possible to choose  $\Omega_A$  and  $\Omega_B$  in such a way that the code with parity check matrix  $\mathbf{H}$  has covering radius 2, which improves on (5.3.3):

$$\ell(2m + i, 2) \leq n_i - 1.$$

Since the most favourable cases are  $i = 0$  or  $i = 1$ , we have:

**Theorem 5.3.4** For all  $m \geq 3$ ,

$$\ell(2m+1, 2) \leq 2^{m+1} + 2^m - 4.$$

For all  $m \geq 4$ ,

$$\ell(2m, 2) \leq 2^{m+1} - 4. \quad (5.3.5)$$

□

One can save more coordinates: through simple matrix constructions, one obtains:

$$\ell(2m, 2) \leq 2^{m+1} - 2^a - 1, \quad (5.3.6)$$

but the value of  $a$  and how large  $m$  must be are not specified in general. The smallest example is a  $[59, 49]_2$  code, i.e.,  $\ell(10, 2) \leq 59$ , whereas inequality (5.3.5) only gives  $\ell(10, 2) \leq 60$ .

The following theorem shows the possibility, for  $\ell(2m, 2)$  and  $\ell(2m+1, 2)$ , to save around  $2^{m/2}$  coordinates, compared to the direct sum or the amalgamated direct sum.

**Theorem 5.3.7** For all  $m \geq 1$ ,

$$\ell(4m, 2) \leq 2^{2m+1} - 2^m - 1.$$

For all  $m \geq 2$ ,

$$\ell(4m+1, 2) \leq 2^{2m+1} + 2^{2m} - 2^m - 2,$$

$$\ell(4m+2, 2) \leq 2^{2m+2} - 2^m - 2,$$

$$\ell(4m+3, 2) \leq 2^{2m+2} + 2^{2m+1} - 2^m - 2.$$

□

We give no proof of these results, because the next section provides linear constructions yielding in particular, for covering radius two (see Theorem 5.4.27):

- for  $m \geq 4$ ,  $\ell(2m, 2) \leq 27 \cdot 2^{m-4} - 1 = 2^{m+1} - 2^{m-2} - 2^{m-4} - 1$ ,
  - for  $m \geq 1$ ,  $\ell(2m+1, 2) \leq 5 \cdot 2^{m-1} - 1 = 2^{m+1} + 2^m - 2^{m-1} - 1$ ,
- which improve on Theorem 5.3.7.

## 5.4 Davydov's basic construction

In this section, we follow Davydov [179] and describe his basic construction, considering only binary linear codes. Notes at the end of the chapter discuss, among other problems, the nonbinary and the nonlinear cases.

We give infinite families of normal  $[n, n - r]R$  codes, our goal being to minimize  $n$ , in order to get upper bounds on the length function. Taking a parity check matrix of an  $[n_0, n_0 - r_0]R_0 \leq R$  “starting” code  $C_0$  (actually, often  $R = R_0$ ), we construct a parity check matrix for an  $[n, n - r]R$  code  $C$  having the following parameters:  $n = 2^m n_0 + n_1(m)$ ,  $r = r_0 + mR$ , where  $m$  is an integer ranging from a lower bound  $m_0$  to infinity and  $n_1$  a function of  $m$  to be specified later.

Let us begin with two examples. In the second example, as well as in the whole section, binary  $m$ -tuples have a dual identity: they are binary vectors but at the same time can be viewed as elements of the field with  $2^m$  elements. In particular, whenever we consider the product of two binary vectors  $\mathbf{a}$  and  $\mathbf{b}$ , denoted by  $\mathbf{ab}$ , they are considered as field elements.

**Example 5.4.1** Let  $\mathbf{A}_1 = (\mathbf{x}_1 \mathbf{x}_2 \dots \mathbf{x}_{2^m-1})$  be a parity check matrix of the binary Hamming  $[2^m - 1, 2^m - 1 - m]1$  code. Let  $M = 2^m$  and  $\mathbb{F}_M = \{\mathbf{f}_1, \dots, \mathbf{f}_M\}$ , where the elements  $\mathbf{f}_i$  are considered as columns of length  $m$ . Let  $C$  be the code with parity check matrix

$$\mathbf{H}(C) = \left( \begin{array}{c|cccc} 0^{m \times (2^m-1)} & \mathbf{P}(\mathbf{x}_1) & \mathbf{P}(\mathbf{x}_2) & \dots & \mathbf{P}(\mathbf{x}_{2^m-1}) \\ \hline \mathbf{A}_1 & \mathbf{B} & \mathbf{B} & \dots & \mathbf{B} \end{array} \right),$$

where  $\mathbf{B} = (\mathbf{f}_1 \dots \mathbf{f}_M)$  and  $\mathbf{P}(\mathbf{x}_i)$  consists of column  $\mathbf{x}_i$  repeated  $M$  times. Then the code  $C$  is a  $[2^{2m} - 1, 2^{2m} - 1 - 2m]1$  code. Obviously, the matrix  $\mathbf{H}(C)$  contains all nonzero columns of length  $2m$  and  $C$  is a Hamming code.  $\square$

**Example 5.4.2** Let  $C_0$  be the binary  $[7, 2]3$  starting code with parity check matrix

$$\mathbf{H}(C_0) = (\mathbf{x}_1 \mathbf{x}_2 \dots \mathbf{x}_7) = \begin{pmatrix} 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}. \quad (5.4.3)$$

Let  $\mathbf{A}_1$  be a parity check matrix of the binary Hamming  $[2^m - 1, 2^m - 1 - m]1$  code. For  $M = 2^m$ , let  $\mathbf{b}, \mathbf{f}_i$  be columns of length  $m$ , also representing elements in  $\mathbb{F}_M$ , with  $\mathbf{f}_i \neq \mathbf{f}_j$  for  $i \neq j$ . Let

$$\mathbf{B}(\mathbf{b}) = \begin{pmatrix} \mathbf{f}_1 & \mathbf{f}_2 & \dots & \mathbf{f}_M \\ \mathbf{b}\mathbf{f}_1 & \mathbf{b}\mathbf{f}_2 & \dots & \mathbf{b}\mathbf{f}_M \\ \mathbf{b}^2\mathbf{f}_1 & \mathbf{b}^2\mathbf{f}_2 & \dots & \mathbf{b}^2\mathbf{f}_M \end{pmatrix} \quad (5.4.4)$$

and finally

$$\mathbf{H}(C) = \left( \begin{array}{c|ccc} 0^{5 \times (2^m-1)} & \mathbf{P}(\mathbf{x}_1) & \dots & \mathbf{P}(\mathbf{x}_7) \\ \hline \mathbf{D} & \mathbf{B}(\mathbf{b}_1) & \dots & \mathbf{B}(\mathbf{b}_7) \end{array} \right), \quad (5.4.5)$$

where  $\mathbf{P}(\mathbf{x}_i)$  consists of column  $\mathbf{x}_i$  repeated  $M$  times,  $\mathbf{b}_1, \dots, \mathbf{b}_7$  are columns of length  $m$  and

$$\mathbf{D} = \begin{pmatrix} 0^{2m \times (2^m-1)} \\ \mathbf{A}_1 \end{pmatrix}. \quad (5.4.6)$$

Then  $\mathbf{H}(C)$  is a  $(5 + 3m) \times (2^{m+3} - 1)$  parity check matrix of a code  $C$  with parameters  $n = 7 \cdot 2^m + (2^m - 1)$ ,  $k = n - (5 + 3m)$ . If  $7 \leq 2^m$  (i.e.,  $m \geq 3$ ) and if  $\mathbf{b}_i \neq \mathbf{b}_j$  for  $i \neq j$ , then  $C$  has covering radius at most 3 and is normal.

The normality of  $C$  is a consequence of Theorem 4.2.2, since obviously the code  $C$  has minimum distance at most 3. It can also be viewed as a consequence of Corollary 4.2.5, as soon as we have proved that  $C$  has covering radius 3, i.e., any nonzero vector  $\mathbf{y} \in \mathbb{F}^{5+3m}$  is a sum of at most three columns of  $\mathbf{H}(C)$ .

Observe that  $C_0$ , with covering radius 3, actually has an additional property: any vector in  $\mathbb{F}^5$  is a sum of 2 or 3 columns of  $\mathbf{H}(C_0)$ . Second, we see that, if  $z$  is 2 or 3, and if  $\{j_1, \dots, j_z\} \subset \{1, \dots, 7\}$ , then any column  $\mathbf{u} \in \mathbb{F}^{3m}$  is a sum of at least  $z$  and at most 3 columns, with one column taken from each of the  $z$  matrices  $\mathbf{B}(\mathbf{b}_{j_1}), \dots, \mathbf{B}(\mathbf{b}_{j_z})$  and (if  $z = 2$ ) one possible additional column taken from  $\mathbf{D}$ . Indeed, if  $z = 3$ , consider the following system of three equations in  $\mathbb{F}_M$ , where the elements  $\mathbf{f}, \mathbf{f}', \mathbf{f}''$  are the three unknowns and  $\mathbf{u} = (\mathbf{u}_0 | \mathbf{u}_1 | \mathbf{u}_2)^T$ , with  $\mathbf{u}_i \in \mathbb{F}^m$ :

$$(S_1) : \begin{cases} \mathbf{f} + \mathbf{f}' + \mathbf{f}'' = \mathbf{u}_0 \\ \mathbf{b}_{j_1}\mathbf{f} + \mathbf{b}_{j_2}\mathbf{f}' + \mathbf{b}_{j_3}\mathbf{f}'' = \mathbf{u}_1 \\ \mathbf{b}_{j_1}^2\mathbf{f} + \mathbf{b}_{j_2}^2\mathbf{f}' + \mathbf{b}_{j_3}^2\mathbf{f}'' = \mathbf{u}_2 \end{cases}.$$

This system has determinant

$$\begin{vmatrix} 1 & 1 & 1 \\ \mathbf{b}_{j_1} & \mathbf{b}_{j_2} & \mathbf{b}_{j_3} \\ \mathbf{b}_{j_1}^2 & \mathbf{b}_{j_2}^2 & \mathbf{b}_{j_3}^2 \end{vmatrix},$$

which is nonzero for distinct vectors  $\mathbf{b}_j$ . If  $z = 2$ , then solve the system

$$(S_2) : \begin{cases} \mathbf{f} + \mathbf{f}' = \mathbf{u}_0 \\ \mathbf{b}_{j_1}\mathbf{f} + \mathbf{b}_{j_2}\mathbf{f}' = \mathbf{u}_1 \end{cases}.$$

If  $\mathbf{u}_2 \neq \mathbf{b}_{j_1}^2 \mathbf{f} + \mathbf{b}_{j_2}^2 \mathbf{f}'$ , then choose in  $\mathbf{D}$  the column whose lower part is equal to  $\mathbf{u}_2 + \mathbf{b}_{j_1}^2 \mathbf{f} + \mathbf{b}_{j_2}^2 \mathbf{f}'$ , which can be done since  $\mathbf{A}_1$  is a parity check matrix of a Hamming code.

Now for any nonzero vector  $\mathbf{y} \in \mathbb{F}^{5+3m}$  it is easy to prove the existence of at most three columns of  $\mathbf{H}(C)$  summing to  $\mathbf{y}$ . Let  $\mathbf{y} = (\mathbf{y}_0 | \mathbf{y}_1)^T$ , with  $\mathbf{y}_0 \in \mathbb{F}^5$  and  $\mathbf{y}_1 \in \mathbb{F}^{3m}$ . We observed that  $\mathbf{y}_0^T$  can be represented as a sum of  $z = 2$  or  $3$  columns of  $\mathbf{H}(C_0)$ :  $\mathbf{y}_0^T = \mathbf{x}_{j_1} + \dots + \mathbf{x}_{j_z}$ . This means that there is a vector  $\mathbf{u} = (0^{2^m-1} | \mathbf{u}_1 | \dots | \mathbf{u}_7) \in \mathbb{F}^{2^{m+3}-1}$  (with  $\mathbf{u}_i \in \mathbb{F}^{2^m}$  for  $1 \leq i \leq 7$ ), such that

$$\mathbf{H}(C)\mathbf{u}^T = (\mathbf{y}_0 | \mathbf{y}_2)^T,$$

$2 \leq z = w(\mathbf{u}) \leq 3$ ,  $w(\mathbf{u}_{j_1}) = \dots = w(\mathbf{u}_{j_z}) = 1$  and  $w(\mathbf{u}_i) = 0$  for the remaining  $7 - z$  indices  $i$ . Therefore, vector  $\mathbf{y}_2^T$  is a sum of  $z$  columns, with one column taken from each of the matrices  $\mathbf{B}(\mathbf{b}_{j_1}), \dots, \mathbf{B}(\mathbf{b}_{j_z})$ . If  $z = 3$ , we know that we can choose these columns so that  $\mathbf{y}_2 = \mathbf{y}_1$ . This specific choice does not affect  $\mathbf{y}_0^T$ . So  $\mathbf{y}$  is a sum of three columns of  $\mathbf{H}(C)$ . If  $z = 2$ , we can choose one column in each of the matrices  $\mathbf{B}(\mathbf{b}_{j_1}), \mathbf{B}(\mathbf{b}_{j_2})$ , then, possibly, one column in  $\mathbf{D}$ , in order to get  $\mathbf{y}_1^T$ . This proves that  $\mathbf{y}$  can be written as a sum of at most three columns of  $\mathbf{H}(C)$ .  $\square$

In order to minimize  $n_1(m)$ , we consider codes  $C_0$  having an additional property (as in Example 5.4.2): they are  $(R_0^*, R_1^*)$ -subsets of  $\mathbb{F}^{n_0}$ :

**Definition 5.4.7** Let  $\mathbf{H}$  be an  $r \times n$  matrix,  $b$  and  $c$  be two integers,  $b \geq c \geq 1$ . Let  $[\mathbf{H}]b, c = \{\mathbf{y} \in \mathbb{F}^r : \text{there is } \mathbf{x} \in \mathbb{F}^n \text{ such that } \mathbf{y} = \mathbf{H}\mathbf{x}^T \text{ and } c \leq w(\mathbf{x}) \leq b\}$ .

Let  $C_0$  be an  $[n_0, n_0 - r_0]R_0$  code with parity check matrix  $\mathbf{H}(C_0)$ . For  $R_0^* \geq R_1^* \geq 0$ ,  $C_0$  is an  $(R_0^*, R_1^*)$ -subset of  $\mathbb{F}^{n_0}$  and is denoted by  $[n_0, n_0 - r_0]R_0^*, R_1^*$  if the following holds:

If  $R_1^* \geq 1$ ,  $[\mathbf{H}(C_0)]R_0^*, R_1^* = \mathbb{F}^{r_0}$

and for  $A < R_0^*, [\mathbf{H}(C_0)]A, R_1^* \subset [\mathbf{H}(C_0)]R_0^*, R_1^*$ .

If  $R_1^* = 0$ ,  $[\mathbf{H}(C_0)]R_0^*, 1 \supseteq \mathbb{F}^{r_0} \setminus \{0^{r_0}\}$

and for  $A < R_0^*, [\mathbf{H}(C_0)]A, 1 \subset [\mathbf{H}(C_0)]R_0^*, 1$ .

In other words, if  $R_1^* \geq 1$ , then any column in  $\mathbb{F}^{r_0}$  can be represented as a sum of at least  $R_1^*$  and at most  $R_0^*$  different columns of  $\mathbf{H}(C_0)$ , and, if  $R_1^* = 0$ , then any nonzero column in  $\mathbb{F}^{r_0}$  can be represented as a sum of at

most  $R_0^*$  columns of  $\mathbf{H}(C_0)$ ; furthermore, for a given  $R_1^*$ ,  $R_0^* = R_0^*(R_1^*)$  is the smallest integer with this property. We have:  $R_0^*(0) = R_0$  (this is the classical definition of a covering code) and  $R_0^*(R_1^*) \geq R_0$ .

Or: for any vector in  $\mathbb{F}^{n_0}$ , there is a codeword at distance at least  $R_1^*$  and at most  $R_0^*$  (this characterization is used for the nonlinear case); for  $R_1^* \geq 1$ , the codewords can be seen as the centres of “spherical capsules” covering the space, having internal radius  $R_1^*$ , external radius  $R_0^*$  and “thickness”  $R_0^* - R_1^* + 1$  (cf.  $L$ -spheres, when  $L$  is the interval  $[R_1^*, R_0^*]$ , in Section 19.1, and weighted  $m$ -coverings with  $m_{R_1^*} = m_{R_1^*+1} = \dots = m_{R_0^*} = 1$  and  $m_i = 0$  for  $i \in [0, n] \setminus [R_1^*, R_0^*]$ , in Section 13.1).

Let  $\{\mathbf{H}_i : 1 \leq i \leq v\}$  be a set of  $v$  matrices all having  $w$  rows. Let

$$\{\mathbf{H}_1 + \dots + \mathbf{H}_v\} = \{\mathbf{x} \in \mathbb{F}^w : \mathbf{x} = \mathbf{h}_1 + \dots + \mathbf{h}_v\},$$

where  $\mathbf{h}_i$  is a column of matrix  $\mathbf{H}_i$ , for  $1 \leq i \leq v$ . We can now define an  $R$ -closed family of matrices and an  $(R, R_1^*)$ -complementary matrix of an  $R$ -closed family of matrices.

**Definition 5.4.8** If  $0 \leq R < n_0$ , a set of matrices  $\{\mathbf{H}_i : 1 \leq i \leq n_0\}$ , all having  $w$  rows, is said to be  $R$ -closed if for any set of  $R$  distinct indices  $J_R = \{j_1, \dots, j_R\} \subset \{1, \dots, n_0\}$ , any column in  $\mathbb{F}^w$  can be represented as a sum of  $R$  columns, one column taken from each of the  $R$  matrices  $\mathbf{H}_{j_1}, \dots, \mathbf{H}_{j_R}$ , i.e.,

$$\{\mathbf{H}_{j_1} + \dots + \mathbf{H}_{j_R}\} = \mathbb{F}^w. \quad (5.4.9)$$

If  $0 \leq R_1^* \leq R < n_0$ , a matrix  $\mathbf{L}$ , having  $w$  rows, is said to be  $(R, R_1^*)$ -complementary to the  $R$ -closed family of matrices  $\{\mathbf{H}_i : 1 \leq i \leq n_0\}$  if the following two conditions hold:

**Condition 1.** For any set of  $z$  distinct indices  $J_z = \{j_1, \dots, j_z\} \subset \{1, \dots, n_0\}$  ( $R_1^* \leq z \leq R$  and  $1 \leq z$ ), any column in  $\mathbb{F}^w$  can be represented as a sum of at least  $z$  and at most  $R$  columns, with one column taken from each of the  $z$  matrices  $\mathbf{H}_{j_1}, \dots, \mathbf{H}_{j_z}$  and possible additional columns (at most  $R - z$ ) taken from  $\mathbf{L}, \mathbf{H}_1, \dots, \mathbf{H}_{n_0}$ , where a matrix  $\mathbf{H}_i$  ( $1 \leq i \leq n_0$ ) provides either zero or an even number of additional columns.

**Condition 2.** If  $R_1^* = 0$ , any nonzero column in  $\mathbb{F}^w$  can be represented as a sum of at most  $R$  columns taken from  $\mathbf{L}, \mathbf{H}_1, \dots, \mathbf{H}_{n_0}$ , where a matrix  $\mathbf{H}_i$  ( $1 \leq i \leq n_0$ ) provides either zero or an even number of columns.

Condition 1 is satisfied if for any set of indices  $\{j_1, \dots, j_z\}$ ,

$$\{\mathbf{H}_{j_1} + \dots + \mathbf{H}_{j_z}\} + (\{0^w\} \cup [\mathbf{L}]R - z, 1) = \mathbb{F}^w \quad (5.4.10)$$

(the possible additional columns all come from  $\mathbf{L}$ ). Condition 2 is satisfied if  $\mathbf{L}$  is a parity check matrix of a code with covering radius  $R$ , i.e.,

$$[\mathbf{L}]R, 1 = \mathbb{F}^w \setminus \{0^w\}, \quad (5.4.11)$$

which means that all columns come from  $\mathbf{L}$ .

For any column  $\mathbf{x}$ , let  $\mathbf{P}(\mathbf{x})$  be a matrix consisting of column  $\mathbf{x}$  repeated a certain number of times, determined by context:

$$\mathbf{P}(\mathbf{x}) = (\mathbf{x} \mathbf{x} \dots \mathbf{x}).$$

We can now state the first theorem.

**Theorem 5.4.12** *Let  $\mathbf{H}(C_0) = (\mathbf{x}_1 \mathbf{x}_2 \dots \mathbf{x}_{n_0})$  be a parity check matrix of an  $[n_0, n_0 - r_0] R_0^*, R_1^*$  code  $C_0$  (the  $\mathbf{x}_i$ 's represent columns of length  $r_0$ ). Let  $\{\mathbf{H}_i : 1 \leq i \leq n_0\}$  be an  $R$ -closed family of  $w \times n_2$  matrices. Let  $\mathbf{L}$  be a  $w \times n_1$  matrix which is  $(R, R_1^*)$ -complementary to  $\{\mathbf{H}_i\}$  ( $R \geq R_0^* \geq R_1^* \geq 0$ ). Then the  $(r_0 + w) \times (n_1 + n_0 n_2)$  matrix*

$$\mathbf{H}(C) = \left( \begin{array}{c|cccc} \mathbf{0} & \mathbf{P}(\mathbf{x}_1) & \mathbf{P}(\mathbf{x}_2) & \dots & \mathbf{P}(\mathbf{x}_{n_0}) \\ \mathbf{L} & \mathbf{H}_1 & \mathbf{H}_2 & \dots & \mathbf{H}_{n_0} \end{array} \right) \quad (5.4.13)$$

(if  $R = R_1^*$ , then the matrices  $\mathbf{L}$  and  $\mathbf{0}$  do not appear) is a parity check matrix of a code  $C$  with length  $n = n_1 + n_0 n_2$ , codimension  $r = r_0 + w$  and covering radius at most  $R$ .

**Proof.** We have to prove that any nonzero column  $\mathbf{y} \in \mathbb{F}^{r_0+w}$  is a sum of at most  $R$  columns of  $\mathbf{H}(C)$ . Let  $\mathbf{y} = (\mathbf{y}_0 | \mathbf{y}_1)^T$ , with  $\mathbf{y}_0 \in \mathbb{F}^{r_0}$  and  $\mathbf{y}_1 \in \mathbb{F}^w$ .

— Case  $R_1^* \geq 1$ . By hypothesis, the starting code  $C_0$  is an  $(R_0^*, R_1^*)$ -subset of  $\mathbb{F}^{n_0}$ , so there are columns  $\mathbf{x}_{j_1}, \mathbf{x}_{j_2}, \dots, \mathbf{x}_{j_z}$  in  $\mathbf{H}(C_0)$  (with  $R_1^* \leq z \leq R_0^*$ ) such that

$$\mathbf{y}_0^T = \mathbf{x}_{j_1} + \mathbf{x}_{j_2} + \dots + \mathbf{x}_{j_z}.$$

This means that there is a vector  $\mathbf{u} = (0^{n_1} | \mathbf{u}_1 | \dots | \mathbf{u}_{n_0}) \in \mathbb{F}^{n_1 + n_0 n_2}$  (with  $\mathbf{u}_i \in \mathbb{F}^{n_2}$  for  $1 \leq i \leq n_0$ ), such that

$$\mathbf{H}(C)\mathbf{u}^T = (\mathbf{y}_0 | \mathbf{y}_1)^T,$$

when  $R_1^* \leq z = w(\mathbf{u}) \leq R_0^*$ ,  $w(\mathbf{u}_{j_1}) = w(\mathbf{u}_{j_2}) = \dots = w(\mathbf{u}_{j_z}) = 1$  and  $w(\mathbf{u}_i) = 0$  for the remaining  $n_0 - z$  indices  $i$ . Therefore, vector  $\mathbf{y}_1^T$  is a sum of  $z$  columns, with one column taken from each of the matrices  $\mathbf{H}_{j_1}, \mathbf{H}_{j_2}, \dots, \mathbf{H}_{j_z}$ .

If  $z = R$ , we can choose these columns in such a way that  $\mathbf{y}_2 = \mathbf{y}_1$ , because  $\{\mathbf{H}_i : 1 \leq i \leq n_0\}$  is an  $R$ -closed family. The specific choice of these columns does not affect  $\mathbf{y}_0^T$ , because of the structure of the upper part of matrix  $\mathbf{H}(C)$ . Hence  $\mathbf{y}$  is a sum of  $R$  columns of  $\mathbf{H}(C)$ .

If  $z < R$ , we choose one column in each of the matrices  $\mathbf{H}_{j_1}, \mathbf{H}_{j_2}, \dots, \mathbf{H}_{j_z}$  together with some (at most)  $R - z$  columns in  $\mathbf{L}, \mathbf{H}_1, \mathbf{H}_2, \dots, \mathbf{H}_{n_0}$  (with an even — possibly zero — number of these additional columns in each  $\mathbf{H}_i$ ), in order to get  $\mathbf{y}_1^T$  (Condition 1 in Definition 5.4.8). The structure of the upper part of matrix  $\mathbf{H}(C)$  guarantees that we still get  $\mathbf{y}_0^T$ .

– Case  $R_1^* = 0$ . If  $\mathbf{y}_0 \neq 0^{r_0}$ ,  $\mathbf{y}_0^T$  is a sum of at most  $R_0^* \leq R$  columns of  $\mathbf{H}(C_0)$  and the end of this case is similar to the previous one (again, using Condition 1). If  $\mathbf{y}_0 = 0^{r_0}$ , then  $\mathbf{y}_1 \neq 0^w$  and, by Condition 2 of Definition 5.4.8,  $\mathbf{y}_1^T$  is a sum of at most  $R$  columns taken from  $\mathbf{L}, \mathbf{H}_1, \mathbf{H}_2, \dots, \mathbf{H}_{n_0}$  (with zero or an even number of columns in each  $\mathbf{H}_i$ ). We conclude in the same way as above.  $\square$

Now, which matrices could be used as  $\mathbf{L}$  and  $\mathbf{H}_i$ ? The following implementation is suggested, with various possible relationships between its parameters. Let  $\mathbf{B}(\xi, \mathbf{b})$  be the following  $mR \times 2^m$  matrix (for such matrices, we also say that they have  $R$  block-rows, each block-row being a group of  $m$  rows):

$$\mathbf{B}(\xi, \mathbf{b}) = \begin{pmatrix} \mathbf{f}_1 & \mathbf{f}_2 & \dots & \mathbf{f}_M \\ \mathbf{b}\mathbf{f}_1 & \mathbf{b}\mathbf{f}_2 & \dots & \mathbf{b}\mathbf{f}_M \\ \mathbf{b}^2\mathbf{f}_1 & \mathbf{b}^2\mathbf{f}_2 & \dots & \mathbf{b}^2\mathbf{f}_M \\ \dots & \dots & \dots & \dots \\ \mathbf{b}^{R-\xi-1}\mathbf{f}_1 & \mathbf{b}^{R-\xi-1}\mathbf{f}_2 & \dots & \mathbf{b}^{R-\xi-1}\mathbf{f}_M \\ \hline (\mathbf{a}_1 + \mathbf{b})^{-1}\mathbf{f}_1 & (\mathbf{a}_1 + \mathbf{b})^{-1}\mathbf{f}_2 & \dots & (\mathbf{a}_1 + \mathbf{b})^{-1}\mathbf{f}_M \\ (\mathbf{a}_2 + \mathbf{b})^{-1}\mathbf{f}_1 & (\mathbf{a}_2 + \mathbf{b})^{-1}\mathbf{f}_2 & \dots & (\mathbf{a}_2 + \mathbf{b})^{-1}\mathbf{f}_M \\ \dots & \dots & \dots & \dots \\ (\mathbf{a}_\xi + \mathbf{b})^{-1}\mathbf{f}_1 & (\mathbf{a}_\xi + \mathbf{b})^{-1}\mathbf{f}_2 & \dots & (\mathbf{a}_\xi + \mathbf{b})^{-1}\mathbf{f}_M \end{pmatrix}, \quad (5.4.14)$$

where  $M = 2^m$ ,  $\xi \in \{0, 1, \dots, R-1\}$ , the columns  $\mathbf{b}, \mathbf{f}_i, \mathbf{a}_j$ , of length  $m$  also represent elements in  $\mathbb{F}_{2^m}$ , with  $\mathbf{f}_i \neq \mathbf{f}_j$  for  $i \neq j$ ,  $\mathbf{a}_i \neq \mathbf{a}_j$  for  $i \neq j$ , and  $\mathbf{b} \neq \mathbf{a}_i$  for all  $i = 1, 2, \dots, \xi$ . If  $\xi = 0$ , the lower part of matrix  $\mathbf{B}(\xi, \mathbf{b})$  does not appear.

Let  $\mathcal{F}$  be the family of  $n_0$  matrices defined by:

$$\mathcal{F} = \{\mathbf{B}(\xi, \mathbf{b}_i) : \mathbf{b}_i \in \mathbb{F}_{2^m}, 1 \leq i \leq n_0, \mathbf{b}_i \neq \mathbf{b}_j \text{ if } i \neq j\}, \quad (5.4.15)$$

if  $n_0 \leq 2^m$ ; or

$$\mathcal{F} = \{\mathbf{B}(\xi, \mathbf{b}_i) : \mathbf{b}_i \in \mathbb{F}_{2^m}, 1 \leq i \leq 2^m, \mathbf{b}_i \neq \mathbf{b}_j \text{ if } i \neq j\} \cup \{\mathbf{W}\}, \quad (5.4.16)$$

if  $n_0 = 2^m + 1$ . Here  $\mathbf{W}$  is the  $mR \times 2^m$  matrix

$$\mathbf{W} = \begin{pmatrix} \mathbf{0} & \mathbf{0} & \dots & \mathbf{0} \\ \mathbf{f}_1 & \mathbf{f}_2 & \dots & \mathbf{f}_M \end{pmatrix}$$

whose upper part consists of  $2^m$  zero columns of length  $m(R-1)$  and whose lower part consists of the  $2^m$  different columns of length  $m$ .

The family of matrices  $\mathcal{F}$  will be shown to be  $R$ -closed under certain conditions (see Lemma 5.4.21) and used in Theorem 5.4.12 as  $\{\mathbf{H}_i : 1 \leq i \leq n_0\}$  (so  $w = mR$ ,  $n_2 = 2^m$  and  $n_0 \leq 2^m + 1$ ; see Theorem 5.4.24).

In order to define the matrix  $\mathbf{D}(\chi, \mathbf{g}, \rho)$  which will be used as the matrix  $\mathbf{L}$ , we need some notations.

Let  $\rho$  be an integer and let  $G(\rho)$  be the set of vectors with positive integer components such that  $\mathbf{g} \in G(\rho)$  if and only if the following three conditions hold:

- (i)  $\mathbf{g} = (R_1, R_2, \dots, R_\gamma)$ , with  $1 \leq R_i \leq \rho$  for all  $i = 1, 2, \dots, \gamma$  and  $\gamma \geq \lceil \log_2(\rho + 1) \rceil$ .
- (ii)  $\sum_{i=1}^{\gamma} R_i = \rho$ .
- (iii) For every integer  $t$  between 1 and  $\rho$ , there is a (not necessarily unique) set  $\theta(\mathbf{g}, t) \subseteq \{R_1, R_2, \dots, R_\gamma\}$  such that  $\sum_{R_i \in \theta(\mathbf{g}, t)} R_i = t$ ; by convention,  $\theta(\mathbf{g}, 0) = \emptyset$ .

We now introduce three subsets of  $G(\rho)$ .

- For  $\alpha = 0$  or 1 and  $\nu \in \{1, 2, \dots, \rho\}$ , denote

$$G_1(\rho, \nu, \alpha) = \{\mathbf{g} \in G(\rho) : R_i = 1 \text{ for } i = 1, 2, \dots, \nu \text{ and} \\ R_i \leq \nu + \alpha \text{ for } i = \nu + 1, \dots, \gamma\}.$$

For given  $\rho, \nu, \alpha$ ,  $G_1(\rho, \nu, \alpha)$  generally has several elements.

- $G_2(\rho)$  is a singleton:

$$G_2(\rho) = \{\mathbf{g} \in G(\rho) : \gamma = \lceil \log_2(\rho + 1) \rceil, R_1 = \lceil \rho/2 \rceil \text{ and} \\ R_i = \left\lceil 1/2(\rho - \sum_{j=1}^{i-1} R_j) \right\rceil \text{ for } i = 2, \dots, \gamma\}.$$

- $G_3(\rho)$  is a singleton:

$$G_3(\rho) = \{\mathbf{g} \in G(\rho) : \gamma = \lceil \log_2(\rho + 1) \rceil, R_1 = \rho - 2^{\gamma-1} + 1, \text{ and} \\ R_i = 2^{\gamma-i} \text{ for } i = 2, \dots, \gamma\}.$$

If  $\mathbf{g} \in G_1(\rho, \nu, \alpha)$ , it is possible to choose  $\theta(\mathbf{g}, t)$  in such a way that its elements  $R_i$  have consecutive indices and it contains at least one of the two elements  $R_\nu$  and  $R_{\nu+1}$ . This specific set  $\theta(\mathbf{g}, t)$  is denoted by  $K(\mathbf{g}, t)$  ( $K(\mathbf{g}, 0) = \emptyset$ ) and can be obtained in the following way: let  $y(\mathbf{g}, t)$  be defined by  $\sum_{i=1}^{y(\mathbf{g}, t)} R_{\nu+i} \leq t < \sum_{i=1}^{y(\mathbf{g}, t)+1} R_{\nu+i}$  and let  $Y(\mathbf{g}, t) = \sum_{i=1}^{y(\mathbf{g}, t)} R_{\nu+i}$  (if  $t < R_{\nu+1}$  or  $\nu = \rho$ , then  $y(\mathbf{g}, t) = Y(\mathbf{g}, t) = 0$ ). Let  $X(\mathbf{g}, t) = \nu + 1 - (t - Y(\mathbf{g}, t))$ . Then we can set

$$K(\mathbf{g}, t) = \{R_{X(\mathbf{g}, t)}, R_{X(\mathbf{g}, t)+1}, \dots, R_{\nu+y(\mathbf{g}, t)}\}. \quad (5.4.17)$$

**Example 5.4.18**  $\mathbf{g} = (1, 1, 1, 1, 4, 5, 5) \in G_1(18, 4, 1)$ ;  $y(\mathbf{g}, 10) = 2, Y(\mathbf{g}, 10) = 9, X(\mathbf{g}, 10) = 4$  and  $K(\mathbf{g}, 10) = \{R_4, R_5, R_6\}$ ;  $y(\mathbf{g}, 3) = Y(\mathbf{g}, 3) = 0, X(\mathbf{g}, 3) = 2$  and  $K(\mathbf{g}, 3) = \{R_2, R_3, R_4\}$ .  $\square$

For  $\mathbf{g} \in G(\rho)$ , let  $f(\mathbf{g}) = i$  if for every  $t$  there is a set  $\theta(\mathbf{g}, t)$  such that  $R_j \in \theta(\mathbf{g}, t), j \leq i$ , implies that  $R_k \in \theta(\mathbf{g}, t)$  for all  $k$  between 1 and  $j-1$ , but this property does not hold for  $i+1$ .

**Example 5.4.19** –  $\mathbf{g} = (12, 6, 3, 2, 1) \in G_2(24), f(\mathbf{g}) = 1$ .

–  $\mathbf{g} = (7, 8, 4, 2, 1) \in G_3(22), f(\mathbf{g}) = 2$ .  $\square$

Now let  $\mathbf{g} = (R_1, R_2, \dots, R_\gamma) \in G(\rho)$ ,  $\lambda = R - \rho \geq 0$  and

$$\mathbf{D}(\chi, \mathbf{g}, \rho) = \left( \begin{array}{cccc|ccc} \mathbf{A}_1 & 0 & \dots & 0 & 0 & 0 & \dots & 0 \\ 0 & \mathbf{A}_2 & \dots & 0 & 0 & 0 & \dots & 0 \\ \dots & \dots \\ 0 & 0 & \dots & \mathbf{A}_\chi & 0 & 0 & \dots & 0 \\ \hline 0 & 0 & \dots & 0 & 0 & 0 & \dots & 0 \\ \dots & \dots \\ 0 & 0 & \dots & 0 & 0 & 0 & \dots & 0 \\ \hline 0 & 0 & \dots & 0 & \mathbf{A}_{\chi+1} & 0 & \dots & 0 \\ 0 & 0 & \dots & 0 & 0 & \mathbf{A}_{\chi+2} & \dots & 0 \\ \dots & \dots \\ 0 & 0 & \dots & 0 & 0 & 0 & \dots & \mathbf{A}_\gamma \end{array} \right), \quad (5.4.20)$$

where in the middle part there are  $m\lambda$  rows of zeros and  $\mathbf{A}_i$  is an  $mR_i \times N_i$  parity check matrix of an  $[N_i, N_i - mR_i]R_i$  code  $C_i$ . If  $R_i = 1$ , then we take a Hamming code:  $N_i = 2^m - 1$ . The matrix  $\mathbf{D}(\chi, \mathbf{g}, \rho)$  has  $mR$  rows and  $n_1(m) = \sum_{i=1}^\gamma N_i$  columns. Notice that if  $\chi = 0$  (respectively,  $\gamma$ ), then the uppermost (respectively, lowest) part disappears; if  $R = \rho$ , the middle part of  $\mathbf{D}(\chi, \mathbf{g}, \rho)$  vanishes and the matrix is reduced to the direct sum of matrices  $\mathbf{A}_i$  and is a parity check matrix of an  $[n_1(m), n_1(m) - m\rho]\rho = \sum_{i=1}^\gamma R_i$  code.

Matrix  $\mathbf{D}(\chi, \mathbf{g}, \rho)$  will be shown to be  $(R, R_1^*)$ -complementary to the  $R$ -closed family  $\mathcal{F}$ , under certain conditions (see Lemma 5.4.21), and will replace matrix  $\mathbf{L}$  in Theorem 5.4.12 (see Theorem 5.4.24).

**Lemma 5.4.21** The family of matrices  $\mathcal{F}$ , defined by (5.4.14), and (5.4.15) or (5.4.16), is  $R$ -closed and matrix  $\mathbf{D}(\chi, \mathbf{g}, \rho)$ , defined by (5.4.20), is  $(R, R_1^*)$ -complementary to  $\mathcal{F}$ , if one of the following six sets of conditions holds:

- (i)  $n_0 = 2^m + 1, \xi = 0, \lambda = \max\{0, R_1^* - 2\}, \mathbf{g} \in G_1(\rho, \nu, 0), \nu \geq 1, R_\gamma = 1, \chi = \nu$ .
- (ii)  $n_0 = 2^m + 1, \xi = 0, \lambda = \max\{0, R_1^* - 1\}, \mathbf{g} = (1, 1, \dots, 1), \chi = 0$ .

- (iii)  $n_0 \leq 2^m, \xi = 0, \lambda = \max\{0, R_1^* - 1\}, \mathbf{g} \in G_1(\rho, \nu, 0), \nu \geq 1, \chi = \nu.$
- (iv)  $n_0 \leq 2^m, \xi = 0, \lambda = R_1^*, \mathbf{g} = (1, 1, \dots, 1), \chi = 0.$
- (v)  $n_0 \leq 2^m - 1, \xi = 0, \mathbf{b}_i \neq 0^m \text{ for all } i, \lambda = R_1^*, \mathbf{g} \in G_1(\rho, \nu, 1), \nu \geq 1, \chi = \nu.$
- (vi)  $n_0 \leq 2^m - \xi, \xi = \rho - \sum_{i=1}^j R_i, 1 \leq j \leq f(\mathbf{g}), \lambda = R_1^*, \chi = 0, \text{ for all } \mathbf{g} \in G(\rho).$

**Proof.** We prove that equalities (5.4.10) and (5.4.11) hold. They now read: for any set of  $z$  distinct indices  $J_z = \{j_1, \dots, j_z\} \subset \{1, \dots, n_0\}$  ( $R_1^* \leq z \leq R$  and  $1 \leq z$ ):

$$\{\mathbf{B}(\xi, \mathbf{b}_{j_1}) + \dots + \mathbf{B}(\xi, \mathbf{b}_{j_z})\} + \{0^{mR}\} \cup [\mathbf{D}(\chi, \mathbf{g}, \rho)]R - z, 1 = \mathbb{F}^{mR}, \quad (5.4.22)$$

with  $\mathbf{B}(\xi, \mathbf{b}_{j_k}) = \mathbf{W}$  if  $j_k = 2^m + 1$ . And:

$$[\mathbf{D}(\chi, \mathbf{g}, \rho)]R, 1 = \mathbb{F}^{mR} \setminus \{0^{mR}\}. \quad (5.4.23)$$

By the assumptions,  $R_1^* \leq z \leq R$ ,  $\lambda = R - \rho$  and  $\lambda \leq R_1^*$ , and therefore  $0 \leq z - \lambda \leq \rho$  and we can form the set  $\theta(\mathbf{g}, z - \lambda)$ .

Let  $\mathbf{D}'(\chi, \mathbf{g}, \rho)$  be the matrix consisting of all the columns of  $\mathbf{D}(\chi, \mathbf{g}, \rho)$  containing submatrices  $\mathbf{A}_i$  for which  $R_i \notin \theta(\mathbf{g}, z - \lambda)$ . Now consider, in  $\mathbf{D}'(\chi, \mathbf{g}, \rho)$ , only those block-rows which contain submatrices  $\mathbf{A}_i$  for which  $R_i \notin \theta(\mathbf{g}, z - \lambda)$ ; there are

$$\sum_{R_i \notin \theta(\mathbf{g}, z - \lambda)} R_i = \sum_{1 \leq i \leq \gamma} R_i - \sum_{R_i \in \theta(\mathbf{g}, z - \lambda)} R_i = \rho - (z - \lambda) = R - z$$

such block-rows and they form a parity check matrix of a code with covering radius

$$\sum_{R_i \notin \theta(\mathbf{g}, z - \lambda)} R_i = R - z.$$

The remaining  $z$  block-rows of  $\mathbf{D}'(\chi, \mathbf{g}, \rho)$  are zero; we number them from  $\tau_1$  to  $\tau_z$ .

Let  $\mathbf{u} = (\mathbf{u}_1 | \mathbf{u}_2 | \dots | \mathbf{u}_R)^T$  be an arbitrary column in  $\mathbb{F}^{mR}$ , with  $\mathbf{u}_i \in \mathbb{F}^m$ . In a first step, we prove that there exists a suitable choice for the set  $\theta(\mathbf{g}, z - \lambda)$  such that we can take  $z$  columns, one from each of the matrices  $\mathbf{B}(\xi, \mathbf{b}_{j_k})$  ( $k = 1, \dots, z$ ), in such a way that their sum is equal to a column  $\mathbf{u}^* \in \mathbb{F}^{mR}$  which matches  $\mathbf{u}$  in all positions of block-rows  $\tau_1, \tau_2, \dots, \tau_z$ . By the previous discussion, we can find (at most)  $R - z$  columns in  $\mathbf{D}'(\chi, \mathbf{g}, \rho)$  such that, added to  $\mathbf{u}^*$ , they give  $\mathbf{u}$ . This means that equality (5.4.22) holds. So it remains to prove that such a choice for  $\theta(\mathbf{g}, z - \lambda)$  exists.

Let  $\mathbf{f}_i \mathbf{w}_v(\mathbf{b}_{j_k}) \in \mathbb{F}_{2^m}$  be the element of  $\mathbf{B}(\xi, \mathbf{b}_{j_k})$  (or  $\mathbf{W}$  if  $j_k = 2^m + 1$ ) located at the intersection of block-row  $v$  and column  $i$  (the definitions of

matrices  $\mathbf{B}(\xi, \mathbf{b})$  and  $\mathbf{W}$  show that  $\mathbf{w}_v(\mathbf{b}_{j_k})$  can be equal to 0, 1, a power of  $\mathbf{b}_{j_k}$ , or  $(\mathbf{b}_{j_k} + \mathbf{a})^{-1}$  with  $\mathbf{a} \in \mathbb{F}_{2^m}$ ,  $\mathbf{a} \neq \mathbf{b}_{j_k}$ .

Let  $(S)$  be the following system of  $z$  equations in  $\mathbb{F}_{2^m}$ , where the elements  $\mathbf{f}_{i_k}$  are the  $z$  unknowns:

$$(S) : \sum_{k=1}^z \mathbf{f}_{i_k} \mathbf{w}_{\tau_c}(\mathbf{b}_{j_k}) = \mathbf{u}_{\tau_c}^T, \quad 1 \leq c \leq z.$$

If the determinant,  $\Delta(S)$ , of  $(S)$  is nonzero, then we are done. The case  $z = 1$  is easy, so from now on we assume that  $z \geq 2$ .

Case (i) Assume first that  $j_z = 2^m + 1$  and  $\mathbf{b}_{j_{z-1}} = 0^m$ .

Let  $\Omega = z - \lambda - 2$ ;  $\Omega \geq 0$ , because  $z \geq 2$  and  $\lambda = \max\{0, R_1^* - 2\}$ . Consider  $\theta(\mathbf{g}, z - \lambda) = \{R_1 = 1, R_\gamma = 1\} \cup K(\mathbf{g}, \Omega)$ , where  $K(\mathbf{g}, \Omega) = \emptyset$  if  $\Omega = 0$  and  $K(\mathbf{g}, \Omega) = \{R_{X(\mathbf{g}, \Omega)}, R_{X(\mathbf{g}, \Omega)+1}, \dots, R_{\nu+y(\mathbf{g}, \Omega)}\}$  — cf. (5.4.17) — if  $\Omega > 0$ .

For  $\Omega = 0$ , we have  $\theta(\mathbf{g}, z - \lambda) = \{R_1 = 1, R_\gamma = 1\}$  and  $\tau_1 = 1, \tau_2 = T + 1, \dots, \tau_{z-1} = T + \lambda, \tau_z = R$ .

For  $\Omega > 0$ ,  $K(\mathbf{g}, \Omega)$  contains  $R_\chi$  or  $R_{\chi+1}$ , because  $\chi = \nu$ . So if we take  $\tau_1 = 1, \tau_i = X(\mathbf{g}, \Omega) + i - 2$  for  $i = 2, \dots, z - 1$ , and  $\tau_z = R$ , we include  $T + 1, T + 2, \dots, T + \lambda$ .

Thus, if we let  $s + 1 = X(\mathbf{g}, \Omega)$ , the determinant  $\Delta(S)$  now reads:

$$\Delta(S) = \begin{vmatrix} 1 & \dots & 1 & 1 & 0 \\ \mathbf{b}_{j_1}^s & \dots & \mathbf{b}_{j_{z-2}}^s & 0 & 0 \\ \mathbf{b}_{j_1}^{s+1} & \dots & \mathbf{b}_{j_{z-2}}^{s+1} & 0 & 0 \\ \dots & \dots & \dots & \dots & \dots \\ \mathbf{b}_{j_1}^{s+z-3} & \dots & \mathbf{b}_{j_{z-2}}^{s+z-3} & 0 & 0 \\ \mathbf{b}_{j_1}^{R-1} & \dots & \mathbf{b}_{j_{z-2}}^{R-1} & 0 & 1 \end{vmatrix}$$

and is nonzero (see [464, Ch. 11, Sec. 5]).

Next, assume that  $j_k \neq 2^m + 1$  for all  $k = 1, \dots, z$  and  $\mathbf{b}_{j_z} = 0^m$ . Consider  $\Omega = z - \lambda - 1$  and  $\theta(\mathbf{g}, z - \lambda) = \{R_1 = 1\} \cup K(\mathbf{g}, \Omega)$ .

Finally, assume that  $j_k \neq 2^m + 1$  and  $\mathbf{b}_{j_k} \neq 0^m$  for all  $k = 1, \dots, z$ . Consider  $\Omega = z - \lambda$  and  $\theta(\mathbf{g}, z - \lambda) = K(\mathbf{g}, \Omega)$ .

This ends Case (i). Cases (ii)–(v) are similar.

Case (vi) Inequality  $n_0 \leq 2^m - \xi$  is necessary, because we want  $\{\mathbf{a}_1, \dots, \mathbf{a}_\xi\} \cap \{\mathbf{b}_1, \dots, \mathbf{b}_{n_0}\} = \emptyset$ .

Choose  $\theta(\mathbf{g}, z - \lambda)$  in such a way that if  $R_i \in \theta(\mathbf{g}, z - \lambda), i \leq j$ , then  $R_1, \dots, R_{i-1}$  all belong to  $\theta(\mathbf{g}, z - \lambda)$ :

$$z - \lambda = (R_1 + R_2 + \dots + R_i) + \sum_{k > j, R_k \in \theta(\mathbf{g}, z - \lambda)} R_k,$$

where  $0 \leq i \leq j$ ; if  $i = 0$ , the terms between parentheses do not appear. Now consider:

$$\tau_1 = 1, \dots, \tau_\lambda = \lambda;$$

if  $i \neq 0$ ,  $\tau_{\lambda+1} = \lambda + 1, \dots, \tau_{\lambda+R_1+R_2+\dots+R_i} = \lambda + R_1 + R_2 + \dots + R_i$  and possibly  $\tau_{\lambda+R_1+R_2+\dots+R_i+1}, \dots$ , defined by the remaining elements in  $\theta(\mathbf{g}, z - \lambda)$ ;

if  $i = 0$ ,  $\tau_{\lambda+1}, \dots$ , defined by the remaining elements in  $\theta(\mathbf{g}, z - \lambda)$ .

Equalities  $\lambda + \sum_{1 \leq i \leq j} R_i = \lambda + \rho - \xi = R - \xi$  imply that the determinant  $\Delta(S)$  has the form:

$$\Delta(S) = \begin{vmatrix} 1 & \dots & 1 \\ \mathbf{b}_{j_1} & \dots & \mathbf{b}_{j_z} \\ \mathbf{b}_{j_1}^2 & \dots & \mathbf{b}_{j_z}^2 \\ \dots & \dots & \dots \\ \mathbf{b}_{j_1}^{\delta-1} & \dots & \mathbf{b}_{j_z}^{\delta-1} \\ (\mathbf{a}_{c_1} + \mathbf{b}_{j_1})^{-1} & \dots & (\mathbf{a}_{c_1} + \mathbf{b}_{j_z})^{-1} \\ \dots & \dots & \dots \\ (\mathbf{a}_{c_{z-\delta}} + \mathbf{b}_{j_1})^{-1} & \dots & (\mathbf{a}_{c_{z-\delta}} + \mathbf{b}_{j_z})^{-1} \end{vmatrix},$$

where  $\delta \leq R - \xi$  denotes the number of elements in the upper part of the determinant. Now (see [464, Ch. 11, Sec. 4]), this determinant is nonzero.

The case  $z = R$  shows that  $\mathcal{F}$  is an  $R$ -closed family.

If  $R_1^* = 0$ , then, for all cases (i)–(vi),  $\lambda = 0$ , so  $R = \rho$  and  $\mathbf{D}(\chi, \mathbf{g}, \rho)$  is a parity check matrix of a code with covering radius  $R$ . Therefore equality (5.4.23) holds.  $\square$

Lemma 5.4.21 provides sufficient conditions for the family of matrices  $\mathcal{F}$  to be  $R$ -closed and the matrix  $\mathbf{D}(\chi, \mathbf{g}, \rho)$  to be  $(R, R_1^*)$ -complementary. As an almost immediate consequence, we have the following theorem:

**Theorem 5.4.24** *Let  $\mathbf{H}(C_0) = (\mathbf{x}_1 \mathbf{x}_2 \dots \mathbf{x}_{n_0})$  be a parity check matrix of an  $[n_0, n_0 - r_0] R_0^*, R_1^*$  code  $C_0$  (the  $\mathbf{x}_i$ 's represent columns of length  $r_0$ ). Let  $\mathcal{F}$  and  $\mathbf{D}(\chi, \mathbf{g}, \rho)$  be as in Lemma 5.4.21 and*

$$\mathbf{H}(C) = \left( \begin{array}{c|cccc} \mathbf{0} & \mathbf{P}(\mathbf{x}_1) & \mathbf{P}(\mathbf{x}_2) & \dots & \mathbf{P}(\mathbf{x}_{n_0}) \\ \hline \mathbf{D}(\chi, \mathbf{g}, \rho) & \mathbf{B}(\xi, \mathbf{b}_1) & \mathbf{B}(\xi, \mathbf{b}_2) & \dots & \mathbf{B}(\xi, \mathbf{b}_{n_0}) \end{array} \right). \quad (5.4.25)$$

*If  $\rho = 0$ , the left part of matrix  $\mathbf{H}(C)$ , containing  $\mathbf{D}(\chi, \mathbf{g}, \rho)$ , does not appear; if  $n_0 = 2^m + 1$ , then  $\mathbf{B}(\xi, \mathbf{b}_{n_0})$  is replaced by  $\mathbf{W}$ .*

*Then  $\mathbf{H}(C)$  is a parity check matrix of an  $[n, n-r]$  code  $C$ , with  $n = 2^m n_0 + n_1(m)$ ,  $r = r_0 + mR$ . If one of the six sets of conditions of Lemma 5.4.21 holds, then  $C$  has covering radius at most  $R$ . If moreover  $m \geq 2$ , then  $C$  is normal.*

Note that if  $\rho = 0$ , then  $R = \lambda > 0$ . But (depending on which of the six sets of conditions holds)  $\lambda = R_1^* - 2$  or  $\lambda = R_1^* - 1$  or  $\lambda = R_1^*$ . So in this case, as in Theorem 5.4.12, matrix  $\mathbf{D}(\chi, \mathbf{g}, \rho)$  is not considered.

**Proof.** All we have to show is that the resulting code  $C$  is normal when  $m \geq 2$ . If  $\rho \neq 0$ , there is always at least one component  $R_i$  of vector  $\mathbf{g}$  which is equal to one, because  $t = 1$  must be represented as a sum of elements of  $\mathbf{g}$ . This implies that  $\mathbf{A}_i$  is a parity check matrix of a Hamming code and  $C$  has minimum distance at most three. If  $\rho = 0$ , choosing four elements  $\mathbf{f}_i$  which are linearly dependent shows that  $C$  has minimum distance at most four. In both cases, by Theorem 4.2.2,  $C$  is normal.  $\square$

**Example 5.4.26** Consider again Example 5.4.2, where  $C_0$  is the  $[7, 2]3, 2$  code with parity check matrix  $\mathbf{H}(C_0)$  given by (5.4.3). Let  $\mathbf{g} = (1), \lambda = 2, \chi = 0$ , so that

$$\mathbf{D}(\chi, \mathbf{g}, \rho) = \begin{pmatrix} 0^{2m \times (2^m - 1)} \\ \mathbf{A}_1 \end{pmatrix},$$

where  $\mathbf{A}_1$  is a parity check matrix of the binary Hamming  $[2^m - 1, 2^m - 1 - m]1$  code: the matrix  $\mathbf{D}(\chi, \mathbf{g}, \rho)$  coincides with the matrix  $\mathbf{D}$  defined by (5.4.6). Let  $\xi = 0$ . Then the matrix  $\mathbf{B}(\xi, \mathbf{b})$  coincides with the matrix  $\mathbf{B}(\mathbf{b})$  defined in (5.4.4), and the matrix  $\mathbf{H}(C)$ , given by (5.4.5), is a parity check matrix of a code  $C$  with parameters  $q = 2, n = 2^{m+3} - 1, k = n - (5 + 3m)$ . If  $7 \leq 2^m$  (i.e.,  $m \geq 3$ ), we are in Case (iv) of Lemma 5.4.21 and conclude, if  $\mathbf{b}_i \neq \mathbf{b}_j$  for  $i \neq j$ , that  $C$  has covering radius at most 3 and is normal. The case  $m = 3$  gives  $t[63, 49] \leq 3$  or  $\ell(14, 3) \leq 63$ .  $\square$

Cases (i)–(vi) of Lemma 5.4.21 do not exhaust the possible constructions in Theorem 5.4.24. Choosing the vectors  $\mathbf{g}$  in  $G_2(\rho)$  and  $G_3(\rho)$ , only possible in Case (vi), often reduces  $n_1(m)$  but worsens the lower bound on  $m$ .

The proof of Theorem 5.4.12 shows that we can weaken the conditions on matrices  $\mathbf{L}$  and  $\{\mathbf{H}_i\}$ : in Definition 5.4.8, equality (5.4.9) and Condition 1 need not hold for *all* sets of distinct indices  $J_R = \{j_1, \dots, j_R\} \subset \{1, \dots, n_0\}$  or  $J_z = \{j_1, \dots, j_z\} \subset \{1, \dots, n_0\}$  ( $R_1^* \leq z \leq R$  and  $1 \leq z$ ); it is sufficient that they hold for a set of sets of indices  $J(\mathbf{H}(C_0))$  which depends on  $\mathbf{H}(C_0)$  and can be defined (possibly not uniquely) as follows:  $J(\mathbf{H}(C_0))$  contains, for all columns  $\mathbf{u} \in \mathbb{F}^w$ , one set of indices  $J(\mathbf{u})$  such that  $R_1^* \leq |J(\mathbf{u})| \leq R$ ,  $1 \leq |J(\mathbf{u})|$  and  $\sum_{i \in J(\mathbf{u})} \mathbf{x}_i = \mathbf{u}$ , where  $\mathbf{x}_i$  is the  $i$ -th column of the matrix  $\mathbf{H}(C_0)$ .

Theorem 5.4.24 shows the necessity of finding good starting codes  $C_0$ .

In the binary case, the main results due to Davydov's construction as well as variations on it are put together in the following three theorems. For smaller  $m$ , other upper bounds, also derived from these constructions, are given in Tables 7.1–7.4 in Section 7.3.

**Theorem 5.4.27**

- (i) For all  $m \geq 4$ ,  $\ell(2m, 2) \leq 27 \cdot 2^{m-4} - 1$ .
- (ii) For all  $m \geq 1$ ,  $\ell(2m + 1, 2) \leq 5 \cdot 2^{m-1} - 1$ .

□

**Theorem 5.4.28**

- (i) For all  $m \geq 6$ ,  $\ell(3m, 3) \leq 155 \cdot 2^{m-6} - 2$ .  
For all  $m \geq 9$ ,  $\ell(3m, 3) \leq 152 \cdot 2^{m-6} - 1$ .
- (ii) For all  $m \geq 7$ ,  $\ell(3m + 1, 3) \leq 3 \cdot 2^m - 1$ .
- (iii) For all  $m \geq 4$ ,  $\ell(3m + 2, 3) \leq 1024 \cdot 2^{m-8} - 1$ .  
For all  $m \geq 8$ ,  $\ell(3m + 2, 3) \leq 822 \cdot 2^{m-8} - 2$ .  
For all  $m \geq 13$ ,  $\ell(3m + 2, 3) \leq 821 \cdot 2^{m-8} - 1$ .

□

**Theorem 5.4.29**

- (i) For  $m = 5$  and for all  $m \geq 11$ ,  $\ell(4m, 4) \leq 47 \cdot 2^{m-4} - 1$ .
- (ii) For all  $m \geq 8$ ,  $\ell(4m + 1, 4) \leq 896 \cdot 2^{m-8} - 2$ .  
For all  $m \geq 10$ ,  $\ell(4m + 1, 4) \leq 896 \cdot 2^{m-8} - 3$ .  
For all  $m \geq 15$ ,  $\ell(4m + 1, 4) \leq 895 \cdot 2^{m-8} - 1$ .
- (iii) For all  $m \geq 8$ ,  $\ell(4m + 2, 4) \leq 992 \cdot 2^{m-8} - 2$ .  
For all  $m \geq 10$ ,  $\ell(4m + 2, 4) \leq 992 \cdot 2^{m-8} - 3$ .  
For all  $m \geq 15$ ,  $\ell(4m + 2, 4) \leq 991 \cdot 2^{m-8} - 1$ .
- (iv) For all  $m \geq 10$ ,  $\ell(4m + 3, 4) \leq 1248 \cdot 2^{m-8} - 3$ .  
For  $m = 8$  and for all  $m \geq 15$ ,  $\ell(4m + 3, 4) \leq 1247 \cdot 2^{m-8} - 1$ .

□

We remind the reader — see (2.1.4) — that  $\mu(C)$  is the *density* of a  $q$ -ary code  $C$  of length  $n$  and covering radius  $R$ , i.e.,  $\mu(C) = V_q(n, R) \cdot |C|/q^n$ . In terms of density, Theorems 5.4.27, 5.4.28 and 5.4.29 imply that there exist infinite families of binary linear codes  $C_n$ ,  $D_n$  and  $E_n$  of length  $n$  and covering radius 2, 3 and 4, respectively, such that

$$\liminf_{n \rightarrow \infty} \mu(C_n) = 27^2/2^9 = 1.4238\dots, \quad (5.4.30)$$

$$\liminf_{n \rightarrow \infty} \mu(D_n) = 821^3/(3 \cdot 2^{27}) = 1.3743\dots, \quad (5.4.31)$$

$$\liminf_{n \rightarrow \infty} \mu(E_n) = 991^4/(3 \cdot 2^{37}) = 2.3391\dots. \quad (5.4.32)$$

For more results on asymptotic densities of coverings, linear or not, see Section 12.4.

These constructions can easily be extended to nonbinary codes over the field  $\mathbb{F}_q$ , by considering linear combinations of columns, with coefficients in  $\mathbb{F}_q$ , and replacing elements of  $\mathbb{F}_{2^m}$  by elements of  $\mathbb{F}_{q^m}$ , written as  $q$ -ary columns of length  $m$ . The length of the resulting code  $C$  is now  $n = q^m n_0 + n_1(m)$ .

**Example 5.4.33**  $q = 3, R = 2$ . Let the starting code  $C_0$  be the ternary Golay  $[11, 6]2, 0$  code with parity check matrix  $\mathbf{H}(C_0) = (\mathbf{x}_1 \mathbf{x}_2 \dots \mathbf{x}_{11})$ . Let  $\mathbf{g} = (1, 1) \in G_1(2, 1, 1)$ ,  $\lambda = 0$ , so that matrix  $\mathbf{D}(\chi, \mathbf{g}, \rho)$  is the direct sum of twice a parity check matrix,  $\mathbf{A}_1$ , of the ternary Hamming  $[(3^m-1)/2, (3^m-1)/2-m]1$  code. Let  $\xi = 0$ . Then, if  $M = 3^m$  :

$$\mathbf{B}(\xi, \mathbf{b}) = \left( \begin{array}{cccc} \mathbf{f}_1 & \mathbf{f}_2 & \dots & \mathbf{f}_M \\ \mathbf{b}\mathbf{f}_1 & \mathbf{b}\mathbf{f}_2 & \dots & \mathbf{b}\mathbf{f}_M \end{array} \right),$$

and

$$\mathbf{H}(C) = \left( \begin{array}{cc|ccc} \mathbf{0} & & \mathbf{P}(\mathbf{x}_1) & \dots & \mathbf{P}(\mathbf{x}_{11}) \\ \mathbf{A}_1 & \mathbf{0} & \mathbf{B}(0, \mathbf{b}_1) & \dots & \mathbf{B}(0, \mathbf{b}_{11}) \\ \mathbf{0} & \mathbf{A}_1 & & & \end{array} \right)$$

is a  $(5 + 2m) \times (12 \cdot 3^m - 1)$  parity check matrix of a code  $C$  with parameters  $q = 3, n = 12 \cdot 3^m - 1, k = n - (5 + 2m)$ . If  $11 \leq 3^m - 1$  (i.e.,  $m \geq 3$ ) and  $\mathbf{b}_i \neq \mathbf{0}^m$  ( $1 \leq i \leq 11$ ), we are in the ternary version of Case (v) in Lemma 5.4.21 and  $C$  has covering radius at most 2.  $\square$

## 5.5 Notes

§5.1 Theorem 5.1.7 and Lemmas 5.1.9, 5.1.11 and 5.1.13 (the latter in a slightly different version) were proved by Cohen, Karpovsky, Mattson and Schatz [156]. The ADS of two codes was defined for linear codes by Graham and Sloane [265], and extended to the nonlinear case by Cohen, Lobstein and Sloane [165] (see also Notes on Section 4.1). Example 5.1.15 is by Struik [630].

§5.2 Theorem 5.2.3 was proved by Cohen, Karpovsky, Mattson and Schatz [156].

For Theorem 5.2.7, it was proved in [156] that  $t[n, 4] \geq \lfloor \frac{n-4}{2} \rfloor$  for  $n \geq 4$ , with equality when  $n$  is even or  $n = 7, 9, 11, 13, 15$  and  $17$ , and that  $t[n, 5] \leq \lfloor \frac{n-5}{2} \rfloor$  for  $n \geq 5$ ,  $n \neq 6$ , with equality for  $n = 7, \dots, 12$  and  $14$ . The case of dimensions  $4$  and  $5$  was completely settled by Graham and Sloane [265], who also proved Theorems 5.2.10 and 5.2.16 and stated Conjecture 5.2.13. Inequalities (5.2.18) and (5.2.19) in Theorem 5.2.16 can be very slightly improved using a recent small amendment by Hou [344] on  $N$  in (5.2.20).

In [218], Encheva gives classes of codes achieving  $t[n, 2]$ ,  $t[n, 3]$ ,  $t[n, 4]$  and  $t[n, 5]$ .

§5.3 For Theorem 5.3.4 and inequality (5.3.6), see again [265].

Theorem 5.3.7 was proved by Brualdi, Pless and Wilson [105].

§5.4 Lemma 5.4.21 and Theorems 5.4.12 and 5.4.24 are due to Davydov [179] (1990). Theorems 5.4.27, 5.4.28 and 5.4.29 are in [179] and Davydov and Drozhzhina-Labinskaya [189], but some of these results had been stated earlier by Gabidulin, Davydov and Tombak [244] and Davydov and Drozhzhina-Labinskaya [186], [187], [188].

Variations on the binary linear case. Variations on Davydov's basic construction, with their explicit matrix constructions, can be found in [179, Sec. 4] and in Gabidulin, Davydov and Tombak [245]. There are further developments in, e.g., [189].

Large covering radius. In [179], infinite families of binary linear codes with covering radius  $R = 2, 3, 4, 5$  but also  $R \geq 16$  are constructed.

Taking  $d$  into account. Sometimes, a constraint on the minimum distance of the code is set or its value can be easily computed (see Davydov and Tombak [190], Gabidulin, Davydov and Tombak [245], Struik [630, Sec. 4.4]; see also Etzion and Greenberg [222], Struik [630, Sec. 4.3] for the nonlinear case). In [245], the authors describe infinite families of binary linear codes with covering radius  $2$  and minimum distance  $4$ . Their construction is a variation on Davydov's basic construction, inspired by Szönyi [632]: a parity check matrix of a code with covering radius  $2$  and minimum distance  $4$  is seen as a complete cap in projective geometry (or maximal 3-independent set).

For instance, for  $m \geq 5$ , there exist  $[n = 15 \cdot 2^{m-3} - 3, n - 2m, 4]_2$  and  $[n = 23 \cdot 2^{m-3} - 3, n - (2m + 1), 4]_2$  codes  $C_n$ , which leads to  $\liminf_{n \rightarrow \infty} \mu(C_n) = 15^2/2^7 = 1.7578\dots$ , whereas — see equality (5.4.30) —  $1.4238\dots$  can be achieved.

See also Section 18.3 for the connection between  $[n, n - r, 4]_2$  codes and maximal sum-free sets.

The above family of  $[n = 23 \cdot 2^{m-3} - 3, n - (2m + 1), d = 4]_R = 2$  codes, as well as a family of  $[n = 5 \cdot 2^{m-1} - 1, n - (2m + 1), d = 3]_R = 2$  codes ([245]) achieving the upper bound of Theorem 5.4.27-(ii), are used in the proof of Theorem 4.5.8.

**The nonbinary linear case.** Davydov [179] mentions the possible extension of his construction to the  $q$ -ary case and gives one example, which is our example 5.4.33. It yields, for  $m \geq 5$ , a family of ternary  $[n = 12 \cdot 3^{m-2} - 1, n - (2m + 1)]_2$  codes  $C_n$ , which implies that  $\liminf_{n \rightarrow \infty} \mu(C_n) = 32/27 = 1.1851\dots$

Other references deal with  $q$ -ary linear codes: Davydov [180] describes infinite families of ternary, quaternary and  $q$ -ary ( $q \geq 5$ ) codes with covering radius 2, 3, ... In [181], for  $q = 4$  and covering radius 2, he provides a table of the best codes for redundancy (or codimension) up to 20. In [183], other infinite families of  $q$ -ary codes are described and, for  $q = 3$  and covering radius 2 or 3, a table of the best codes can be found for redundancy up to 24. In [184], nonbinary linear codes with covering radius 2 are considered, with tables of bounds for  $q = 3, 4$  and redundancy up to 32. In particular, a family of ternary codes  $C_n$  is given, with  $\liminf_{n \rightarrow \infty} \mu(C_n) = 1.1778\dots$  In these works, parity check matrices are considered as saturated sets (or spanning sets) of points in projective geometries over finite fields, but the basic ideas of Section 5.4 remain the same.

**The nonlinear case.** A nonlinear code is treated as the union of cosets of a linear code. As already mentioned,  $(R_0^*, R_1^*)$ -subsets can also be defined in the nonlinear case. Davydov ([182], [185]) constructed the following nonlinear codes:

- binary codes  $C_n$  with length  $n = 3 \cdot 2^{2t} + 2^{t+1+\delta} - 4$  (where  $\delta = t \pmod{2}$ ), size  $2^{n-4t-2}$  and covering radius 2, for  $t \geq 4$ :  $\liminf_{n \rightarrow \infty} \mu(C_n) = 9/8$  (but it is known that 1 can be achieved via blockwise direct sums, see Theorem 4.5.8);
- binary codes  $D_n$  with length  $n = 2^{2t+2} + 27 \cdot 2^{t-3+2\delta} - 2$  (where  $\delta = t \pmod{2}$ ), size  $2^{n-6t-3}$  and covering radius 3, for  $t \geq 4$ :  $\liminf_{n \rightarrow \infty} \mu(D_n) = 4/3$ ;
- ternary codes  $E_n$  with length  $n = 71.5 \cdot 3^{t-4} - 5$ , size  $34 \cdot 3^{n-2t-3}$  and covering radius 2, for  $t \geq 9$ :  $\liminf_{n \rightarrow \infty} \mu(E_n) = 2 \cdot 34 \cdot (71.5)^2/3^{11} = 1.9623\dots$ ;
- ternary codes  $F_n$  with length  $n = 418 \cdot 3^{t-5} - 1$ , size  $3^{n-3t-1}$  and covering radius 3, for  $t \geq 8$ :  $\liminf_{n \rightarrow \infty} \mu(F_n) = 4 \cdot (418)^3/3^{17} = 2.2621\dots$

# Chapter 6

## Lower bounds

The basic issue studied in this chapter is to find lower bounds on  $K_q(n, R)$ , the minimum number of codewords in any  $q$ -ary code of length  $n$  and covering radius  $R$ . In this problem  $q$  may be arbitrary. However, we shall mainly deal with binary codes and present a number of different techniques for obtaining lower bounds on  $K(n, R)$ . Most of these methods can be generalized to nonbinary and mixed codes. These generalizations are briefly discussed in Section 6.7 and in the Notes.

The first natural approach is simply to ask how many points can be covered by a given number of Hamming spheres of radius  $R$ . It turns out that such bounds can be obtained by using embedded error-correcting codes and information about  $A(n, d)$ , the maximum cardinality of a binary code of length  $n$  and minimum distance  $d$ . These bounds are discussed in Section 6.1.

In Section 6.2 we give bounds based on the fact that the best codes cannot be too unbalanced, but the zeros and ones should be fairly uniformly distributed.

In Sections 6.3 and 6.4 we discuss the method of excess counting. Instead of the whole space, we consider  $B_s(\mathbf{x})$  for some small  $s$ , and study if it can be covered perfectly, i.e., in such a way that every point in it is covered by exactly one codeword. If not, then we know that there has to be some excess already in this small set  $B_s(\mathbf{x})$ . In Sections 6.3 and 6.4 we discuss the cases  $R = 1$  and  $R > 1$ , respectively.

Linear inequalities provide the most efficient method of obtaining lower bounds on  $K(n, R)$ . They are discussed in Section 6.5. In this approach bounds on coverings of pairs by  $k$ -tuples and other similar problems are very important.

In Section 6.6 we give an updated table of the best currently known lower and upper bounds on the function  $K(n, R)$  when  $n \leq 33$  and  $R \leq 10$ .

## 6.1 Bounds for the cardinality of the union of $K$ spheres

It is interesting in its own right to study what is the largest number of points in  $\mathbb{F}^n$  that can be covered using a given number of Hamming spheres, say  $K$ , of a given radius  $r > 0$ . We denote this number by  $p(n, K, r)$ . The discussion below shows that all the values of  $A(n, d)$  and  $K(n, R)$  can be deduced from the values of  $p(n, K, r)$ . Each Hamming sphere of radius  $r$  in  $\mathbb{F}^n$  contains  $\sum_{i=0}^r \binom{n}{i}$  points, and therefore

$$p(n, K, r) \leq K \sum_{i=0}^r \binom{n}{i}. \quad (6.1.1)$$

Equality holds if and only if there are  $K$  non-intersecting Hamming spheres of radius  $r$  in  $\mathbb{F}^n$ , i.e., if there exists an  $(n, K, 2r+1)$  code. Therefore equality holds in (6.1.1) if and only if  $K \leq A(n, 2r+1)$ . Trivially,

$$p(n, K, r) \leq 2^n,$$

and equality holds if and only if there exists a binary  $(n, K)$  code with covering radius at most  $r$ . By Theorem 2.1.14,  $K(n, r)$  is therefore the smallest  $K$  such that  $p(n, K, r) = 2^n$ . This can be used to derive lower bounds on  $K(n, R)$ . For instance, (6.1.1) yields the following familiar result.

**Theorem 6.1.2 (Sphere-covering bound)**

$$K(n, R) \geq \frac{2^n}{\sum_{i=0}^R \binom{n}{i}}.$$

□

Recall that the cardinality of a Hamming sphere of radius  $r$  in  $\mathbb{F}^n$  is denoted by

$$V(n, r) = \sum_{i=0}^r \binom{n}{i}.$$

When  $K > A(n, 2r+1)$ , we can no longer have  $K$  non-intersecting Hamming spheres of radius  $r$  in  $\mathbb{F}^n$ . The following results illustrate how this fact can be used to improve on (6.1.1) and Theorem 6.1.2.

**Theorem 6.1.3** *If  $n \geq 2r+1$ , then*

$$p(n, K, r) \leq KV(n, r) - (K - A(n, 2r+1)) \binom{2r}{r}.$$

**Proof.** Assume that  $C$  is the code of length  $n$  consisting of the centres of the  $K$  spheres of radius  $r$ . Let  $C_0$  be a maximal subcode of  $C$  with minimum distance at least  $2r+1$ . Then for every  $\mathbf{c} \in C \setminus C_0$  there is a word  $\mathbf{c}_0 \in C_0$  such that  $d(\mathbf{c}, \mathbf{c}_0) \leq 2r$  and by Lemma 2.4.6,  $\mathbf{c}$  covers at most  $V(n, r) - \binom{2r}{r}$  points that are not already covered by the words in  $C_0$ . Since  $|C_0| \leq A(n, 2r+1)$ , the  $K$  codewords therefore cover altogether at most  $A(n, 2r+1)V(n, r) + (K - A(n, 2r+1))(V(n, r) - \binom{2r}{r})$  points.  $\square$

**Corollary 6.1.4** *If  $R > 0$  and  $n \geq 2R+1$ , then*

$$K(n, R) \geq \frac{2^n - A(n, 2R+1)\binom{2R}{R}}{V(n, R) - \binom{2R}{R}}.$$

**Proof.** The right hand side is the lower bound obtained for  $K$  when we require that  $p(n, K, R) = 2^n$ . Because of the assumption  $n \geq 2R+1$ , the denominator is positive.  $\square$

Notice that the condition  $n \geq 2R+1$  is not an essential restriction because all the values of  $K(n, R)$  are known when  $n \leq 2R+1$ . If the exact value of  $A(n, 2R+1)$  is not known, an upper bound on it may be used.

**Example 6.1.5** Assume that  $C \subseteq \mathbb{F}^n$  has covering radius  $R$  and let  $C_0$  be a maximal subcode of  $C$  with minimum distance at least  $2R+1$ . If  $C$  is not a perfect code, the set  $C \setminus C_0$  is nonempty. We show that if  $|C_0| = A(n, 2R+1)$  and  $A(n, 2R+1) = 2A(n-1, 2R+1)$ , then every  $\mathbf{c} \in C \setminus C_0$  is within distance  $2R$  from at least two words of  $C_0$ . Otherwise, for some  $\mathbf{c} \in C \setminus C_0$ , there is a unique codeword  $\mathbf{c}_0 \in C_0$  such that  $d(\mathbf{c}, \mathbf{c}_0) \leq 2R$  and also the code  $C'_0 = (C_0 \setminus \{\mathbf{c}_0\}) \cup \{\mathbf{c}\}$  has minimum distance  $2R+1$ . Because  $A(n, 2R+1) = 2A(n-1, 2R+1)$ , exactly half of the codewords in  $C_0$  — and in  $C'_0$  as well — have 0 in any particular coordinate. However, changing  $\mathbf{c}$  to  $\mathbf{c}_0 \neq \mathbf{c}$  violates this property for at least one coordinate of  $C'_0$ .

For  $n = 9$  we know that  $A(9, 3) = 40$  and Corollary 6.1.4 gives the lower bound

$$K(9, 1) \geq \frac{2^9 - 40 \cdot 2}{10 - 2} = 54.$$

However, such a 54-element code certainly is not perfect, and  $A(9, 3) = 2A(8, 3)$ , implying that equality cannot hold. Hence  $K(9, 1) \geq 55$ .  $\square$

The following result is based on using two embedded error-correcting codes.

**Theorem 6.1.6** *If  $n \geq 2r + 3$ , then*

$$p(n, K, r) \leq K \left( V(n, r) - 2 \binom{2r}{r} + 1 \right) + A(n, 2r + 1) \left( 3 \binom{2r}{r} - 2 \right).$$

**Proof.** Assume that  $C$  is the code of length  $n$  consisting of the centres of the  $K$  spheres of radius  $r$ , and let again  $C_0$  be a maximal subcode of minimum distance at least  $2r + 1$ . Let  $C_1$  be a maximal subcode of minimum distance at least  $2r + 1$  contained in the set  $E = \{\mathbf{c} \in C \setminus C_0 : d(\mathbf{c}, C_0) \geq 2r - 1\}$ . If  $E = \emptyset$ , let  $C_1 = \emptyset$ . Denote further  $L = C \setminus (C_0 \cup C_1)$ . Let  $I(t)$  denote the cardinality of the set  $B_r(\mathbf{x}) \cap B_r(\mathbf{y})$  when  $d(\mathbf{x}, \mathbf{y}) = t$ .

If  $\mathbf{c}_1 \in C_1$ , then as in the proof of Theorem 6.1.3, we see that  $\mathbf{c}_1$  covers at most  $V(n, r) - I(2r)$  points in  $\mathbb{F}^n$  not already covered by  $C_0$ .

Suppose  $\mathbf{c}_2 \in L$ . There are now two possibilities. First, if  $d(\mathbf{c}_2, C_0 \cup C_1) \leq 2r - 2$ , then by Lemma 2.4.6, the codeword  $\mathbf{c}_2$  covers at most  $V(n, r) - I(2r - 2)$  points not already covered by the codewords in  $C_0 \cup C_1$ , and  $I(2r - 2) = 2 \binom{2r-2}{r} + \binom{2r-2}{r-1} (n - 2r + 3) \geq 2I(2r) = 2 \binom{2r}{r}$  by our assumption  $n \geq 2r + 3$ .

The second possibility is that we can find words  $\mathbf{c}_0 \in C_0$  and  $\mathbf{c}_1 \in C_1$  such that  $d(\mathbf{c}_2, \mathbf{c}_0), d(\mathbf{c}_2, \mathbf{c}_1) \in \{2r - 1, 2r\}$ . If  $d(\mathbf{c}_0, \mathbf{c}_1) < 2r + 1$ , then by the definition of  $C_1$ ,  $d(\mathbf{c}_0, \mathbf{c}_1) \in \{2r - 1, 2r\}$  and in every case there is exactly one point that is covered by all the codewords  $\mathbf{c}_0, \mathbf{c}_1, \mathbf{c}_2$ . Therefore, in this case the number of points in  $\mathbb{F}^n$  covered by  $\mathbf{c}_2$  but not by  $C_0 \cup C_1$  is at most  $V(n, r) - 2I(2r) + 1$ . If  $d(\mathbf{c}_0, \mathbf{c}_1) \geq 2r + 1$ , this clearly holds as well.

Therefore,

$$\begin{aligned} p(n, K, r) &\leq |C_0|V(n, r) + |C_1|(V(n, r) - I(2r)) \\ &\quad + (K - |C_0| - |C_1|)(V(n, r) - 2I(2r) + 1), \end{aligned}$$

proving our claim. □

**Corollary 6.1.7** *If  $R > 0$  and  $n \geq 2R + 3$ , then*

$$K(n, R) \geq \frac{2^n - A(n, 2R + 1)(3 \binom{2R}{R} - 2)}{V(n, R) - 2 \binom{2R}{R} + 1}.$$

**Proof.** The right hand side is the lower bound obtained for  $K$  when we require that  $p(n, K, R) = 2^n$ . By the previous proof,  $V(n, R) - 2I(2R) + 1 \geq I(2R - 2) - 2I(2R) + 1 \geq 1$ , so the denominator is positive. □

## 6.2 Balanced codes

A binary code  $C$  with  $K$  codewords is called *balanced* if in each coordinate both 0 and 1 appear at least  $\lfloor K/2 \rfloor$  times. It is conjectured that among the binary  $(n, K)R$  codes with  $K = K(n, R)$  there is always a balanced one.

We denote by  $K_i(a)$  the number of times  $a$  appears in the  $i$ -th coordinate in the codewords of  $C$ , and similarly by  $K_{ij}(ab)$  the number of times the pair  $ab$  appears in the coordinates  $i$  and  $j$ .

**Theorem 6.2.1** *If  $C$  is an  $(n, K)R$  code and  $n > R$ , then for  $a = 0, 1$ ,*

$$K_i(a) \geq \frac{2^{n-1} - K V(n-1, R-1)}{\binom{n-1}{R}}.$$

**Proof.** We consider how the  $2^{n-1}$  vectors with a zero in the  $i$ -th coordinate are covered by the codewords of  $C$ . The  $K_i(0)$  codewords with a zero in the  $i$ -th coordinate each cover  $V(n-1, R)$  such vectors whereas the other codewords cover  $V(n-1, R-1)$  such vectors each. Hence  $K_i(0)V(n-1, R) + K_i(1)V(n-1, R-1) \geq 2^{n-1}$ . The claim for  $a = 0$  now follows from this and the fact that  $K_i(0) + K_i(1) = K$ . The second claim follows from the first one by applying it to the code  $e_i + C$ .  $\square$

Of course the same argument can just as well be used for more than one coordinate. For instance, we get

$$\begin{aligned} K_{ij}(00)V(n-2, R) + (K_{ij}(01) + K_{ij}(10))V(n-2, R-1) \\ + K_{ij}(11)V(n-2, R-2) \geq 2^{n-2} \end{aligned}$$

by considering how the vectors  $\mathbf{x}$  for which  $x_i = x_j = 0$  are covered by the codewords of an  $(n, K)R$  code  $C$ .

**Theorem 6.2.2**  $K(2R+2, R) = 4$  for all  $R = 0, 1, \dots$

**Proof.** Assume that  $C$  is a  $(2R+2, K)$  code with  $K < 4$ . Since there are fewer than four codewords in  $C$  we can choose  $x_1x_2$  so that this pair does not appear as the first two coordinates in any codeword of  $C$ . Similarly choose the pairs  $x_3x_4, \dots, x_{2R+1}x_{2R+2}$ . Then the vector  $x_1x_2 \dots x_{2R+2}$  has distance at least  $R+1$  to  $C$ . Therefore  $K(2R+2, R) \geq 4$ . Clearly, the code  $\{0, 1\} \oplus \{0^{2R+1}, 1^{2R+1}\}$  has covering radius  $R$ , which proves that  $K(2R+2, R) = 4$ .  $\square$

If all the four different pairs 00, 01, 10 and 11 occur at least once in every two coordinates of the codewords, we call the code *2-surjective*, or *2-independent*; cf. Section 3.7.

Assume that an  $(n, K)$  code  $C$  is 2-surjective. Write the codewords in a binary  $K \times n$  array  $\mathbf{A}$  and consider the columns of  $\mathbf{A}$  as subsets of  $S = \{1, 2, \dots, K\}$ . If  $B_1$  and  $B_2$  are any two different columns of  $\mathbf{A}$ , then  $B_1 \not\subseteq B_2$ ,  $B_2 \not\subseteq B_1$ ,  $B_1 \cap B_2 \neq \emptyset$  and  $B_1 \cup B_2 \neq S$ , and it has been shown by Brace and Daykin [93] and Kleitman and Spencer [380] that

$$n \leq \binom{K-1}{\lfloor K/2 \rfloor - 1}. \quad (6.2.3)$$

For any  $n$  and  $K$  satisfying the previous inequality there is a 2-surjective  $(n, K)$  code  $C$ : choose, e.g., as the columns of  $\mathbf{A}$  any  $n$  subsets of  $S$  of cardinality  $\lfloor K/2 \rfloor$  containing the element 1.

The following theorem is based on the same idea as the previous proof.

**Theorem 6.2.4** *If  $C$  is an  $(n+2, K)R+1$  code which is not 2-surjective, then  $K \geq K(n, R)$ .*

**Proof.** We may assume that the pair 00 does not appear in the first two coordinates in any of the codewords of  $C$ . If we puncture these two coordinates, we obtain a code  $C'$  of length  $n$  whose covering radius is at most  $R$ . Indeed, if  $d(\mathbf{x}, C') > R$  for some  $\mathbf{x} \in \mathbb{F}^n$  then  $d(00\mathbf{x}, C) > R+1$ , a contradiction. Hence  $K \geq K(n, R)$ .  $\square$

**Theorem 6.2.5**  $K(2R+3, R) = 7$  for  $R = 1, 2, \dots$

**Proof.** From Example 1.1.9 we know that the  $(5, 7)1$  code given in (1.1.3) is normal. By Theorem 4.1.8, the ADS of this code and the code  $\{0^{2R-1}, 1^{2R-1}\}$  is a  $(2R+3, 7)$  code with covering radius at most  $R$ , proving that  $K(2R+3, R) \leq 7$  for all  $R \geq 1$ .

The lower bound is proved in Example 1.1.1 for  $R = 1$ . For the cases  $R = 2, 3$  we refer to Cohen, Lobstein and Sloane [165]. For  $R \geq 4$  we use induction. Assume that the lower bound is true for  $R-1$  and that  $C$  is a  $(2R+3, K)R$  code with  $K \leq 6$ . Then by (6.2.3),  $C$  is not 2-surjective, and by Theorem 6.2.4,  $K \geq K(2R+1, R-1) \geq 7$ , a contradiction.  $\square$

**Theorem 6.2.6**  $K(2R+4, R) \geq 8$  for all  $R = 0, 1, \dots$

**Proof.** The case  $R = 0$  is trivial, the case  $R = 1$  follows from the sphere-covering bound and the case  $R = 2$  from Corollary 6.1.4. For the case  $R = 3$  we refer to Cohen, Lobstein and Sloane [165] and for the cases  $R = 4$  and  $R = 5$  to Honkala [312]. For  $R \geq 6$  the result follows by induction in exactly the same way as in the previous theorem.  $\square$

## 6.3 Excess bounds for codes with covering radius one

We now discuss the excess counting method. We start with some general definitions. In the remainder of this section we study lower bounds for codes with covering radius one. As usual in the context of covering codes, this case is essentially easier to deal with. In the next section we consider the other cases. The basic idea is very simple: we study how the points in a given sphere  $B_s(\mathbf{x})$  are covered, and try to show that at least one of them is covered by more than one codeword.

We first need some basic definitions. Assume that  $C \subseteq \mathbb{F}^n$  has covering radius  $R$ . Denote

$$Z_i = \{\mathbf{x} \in \mathbb{F}^n : |B_R(\mathbf{x}) \cap C| = i + 1\} \quad (6.3.1)$$

for  $i = 0, 1, \dots$ . If  $\mathbf{x} \in Z_i$ , i.e.,  $\mathbf{x}$  is covered by exactly  $i + 1$  codewords, we say that the *excess*  $E(\mathbf{x})$  on  $\mathbf{x}$  (by  $C$ ) is  $i$ . In general, the excess  $E(V)$  on a subset  $V \subseteq \mathbb{F}^n$  is defined as the sum

$$E(V) = \sum_{\mathbf{x} \in V} E(\mathbf{x}). \quad (6.3.2)$$

Clearly,

$$E(V) = \sum_{i \geq 0} i |Z_i \cap V|, \quad (6.3.3)$$

$$= \sum_{\mathbf{x} \in V} (|B_R(\mathbf{x}) \cap C| - 1)$$

$$= \sum_{\mathbf{x} \in V} |B_R(\mathbf{x}) \cap C| - |V|$$

$$= \sum_{\mathbf{c} \in C} |B_R(\mathbf{c}) \cap V| - |V|. \quad (6.3.4)$$

It is also useful to define

$$Z = \bigcup_{i > 0} Z_i = \{\mathbf{x} \in \mathbb{F}^n : |B_R(\mathbf{x}) \cap C| > 1\}, \quad (6.3.5)$$

i.e.,  $Z$  is the set of points that are covered by more than one codeword.

We see immediately from the definition of excess, (6.3.3) and (6.3.4) that

$$E(\mathbb{F}^n) = \sum_{\mathbf{x} \in \mathbb{F}^n} E(\mathbf{x}) = \sum_{i \geq 0} i |Z_i| = |C| V(n, R) - 2^n. \quad (6.3.6)$$

From now on in this section we assume that  $R = 1$  and that  $C$  is an  $(n, K)1$  code.

Consider a sphere  $B_1(\mathbf{x})$  around any deep hole  $\mathbf{x} \in A := \mathbb{F}^n \setminus C$ . If  $\mathbf{c}$  is a codeword of  $C$  and  $d(\mathbf{c}, \mathbf{x}) \geq 3$  then by the triangle inequality  $\mathbf{c}$  does not cover any of the  $n + 1$  points in  $B_1(\mathbf{x})$ . However, if  $d(\mathbf{x}, \mathbf{c}) = 1$  or 2 then we immediately verify that the intersection  $B_1(\mathbf{x}) \cap B_1(\mathbf{c})$  consists of exactly two points. In other words, every codeword that covers any of the points in  $B_1(\mathbf{x})$  covers exactly two of them. If  $n$  is even, the cardinality of  $B_1(\mathbf{x})$  is odd, and therefore at least one of the points in  $B_1(\mathbf{x})$  is covered by more than one codeword. Using the terminology just introduced,

$$E(B_1(\mathbf{x})) \geq 1 \text{ for all } \mathbf{x} \in A, \quad (6.3.7)$$

which leads to the following result, *the first excess bound for  $R = 1$* .

**Theorem 6.3.8** *If  $n$  is even, then*

$$K(n, 1) \geq \frac{2^n}{n}.$$

**Proof.** If  $\mathbf{z} \in Z$ , then  $\mathbf{z}$  is covered by at least two codewords of  $C$  and there are at most  $n - 1$  elements in the set  $A \cap B_1(\mathbf{z})$ . Therefore by (6.3.7), (6.3.3) and (6.3.6),

$$\begin{aligned} 2^n - |C| &\leq \sum_{\mathbf{x} \in A} E(B_1(\mathbf{x})) \\ &= \sum_{\mathbf{x} \in A} \sum_{i>0} i |Z_i \cap B_1(\mathbf{x})| \\ &= \sum_{i>0} i \sum_{\mathbf{x} \in A} |Z_i \cap B_1(\mathbf{x})| \\ &= \sum_{i>0} i \sum_{\mathbf{z} \in Z_i} |A \cap B_1(\mathbf{z})| \\ &\leq (n - 1) \sum_{i>0} i |Z_i| = (n - 1)(|C|V(n, 1) - 2^n), \end{aligned}$$

from which the claim follows.  $\square$

The following corollary illustrates the strength of this result.

**Corollary 6.3.9**  $K(2^m, 1) = 2^{2^m - m}$  for all  $m = 1, 2, \dots$

**Proof.** The lower bound of Theorem 6.3.8 is attained by the direct sum of the alphabet  $\mathbb{F}$  and the Hamming code of length  $2^m - 1$ .  $\square$

For many even values of  $n$ , Theorem 6.3.8 gives the strongest currently known lower bound on  $K(n, 1)$ , cf. Table 6.1.

The previous argument can be generalized in a number of ways. For example, let  $\mathbf{x} \in \mathbb{F}^n$  and  $s \geq 1$  be arbitrary, and consider how the points in  $B_s(\mathbf{x})$ , instead of  $B_1(\mathbf{x})$ , are covered by the codewords  $\mathbf{c} \in C$ . Clearly every sphere  $B_1(\mathbf{c})$  intersects  $B_s(\mathbf{x})$  in exactly 0,  $s+1$  or  $n+1$  points — depending on whether  $d(\mathbf{c}, \mathbf{x})$  is greater than  $s+1$ , equal to  $s$  or  $s+1$ , or smaller than  $s$ . If we assume that  $s+1$  divides  $n+1$ , then by (6.3.4)

$$E(B_s(\mathbf{x})) \equiv -V(n, s) \pmod{s+1}. \quad (6.3.10)$$

We can now prove the following result, *the general excess bound for  $R = 1$* .

**Theorem 6.3.11** *If  $n+1$  is divisible by an odd prime  $s+1$ , then*

$$K(n, 1) \geq \frac{(V(n, s) + s)2^n}{V(n, s)(n+1)}.$$

**Proof.** By (6.3.10),

$$\begin{aligned} E(B_s(\mathbf{x})) &\equiv -V(n, s) \pmod{s+1} \\ &= -\sum_{i=0}^s \binom{n}{i} \\ &= -1 - \sum_{i=1}^{s/2} \binom{n+1}{2i} \\ &\equiv -1 \pmod{s+1}, \end{aligned} \quad (6.3.12)$$

since all the binomial coefficients  $\binom{n+1}{2i}$  with  $2i \leq s$  are divisible by the prime  $s+1$ . In particular,

$$E(B_s(\mathbf{x})) \geq -1.$$

Therefore by (6.3.6),

$$\begin{aligned} 2^n s &\leq \sum_{\mathbf{x} \in \mathbb{F}^n} E(B_s(\mathbf{x})) \\ &= V(n, s) \sum_{\mathbf{x} \in \mathbb{F}^n} E(\mathbf{x}) \\ &= V(n, s)(|C|(n+1) - 2^n) \end{aligned}$$

and our claim follows.  $\square$

For instance, if  $s = 2$  we get

$$K(n, 1) \geq \frac{(V(n, 2) + 2)2^n}{V(n, 2)(n+1)} \quad \text{if } n \equiv 2 \pmod{3}. \quad (6.3.13)$$

Because for even values of  $n$  we can use Theorem 6.3.8, we only need this bound when  $n \equiv 5 \pmod{6}$ . It can be further improved by using the function  $A(n, 3)$ .

**Theorem 6.3.14** *For every  $n$  with  $n \equiv 5 \pmod{6}$ ,*

$$K(n, 1) \geq \frac{(V(n, 2) + 5)2^{n+1} - 9A(n, 3)(n+1)}{(2V(n, 2) - 3)(n+1)}.$$

**Proof.** We know from (6.3.12) for  $s = 2$  that for all  $\mathbf{x} \in \mathbb{F}^n$ ,

$$E(B_2(\mathbf{x})) \equiv 2 \pmod{3}, \quad (6.3.15)$$

and in particular

$$E(B_2(\mathbf{x})) \geq 2. \quad (6.3.16)$$

Next we show that for every  $\mathbf{x}$  such that

$$|B_2(\mathbf{x}) \cap Z| \geq 2 \quad (6.3.17)$$

we have

$$E(B_2(\mathbf{x})) \geq 5. \quad (6.3.18)$$

By (6.3.15) it suffices to show that  $E(B_2(\mathbf{x})) \geq 3$  and hence we may assume that  $|B_2(\mathbf{x}) \cap Z| = 2$ . Given any two points in  $B_2(\mathbf{x})$  we can find  $\mathbf{y} \in B_1(\mathbf{x})$  such that  $B_1(\mathbf{y})$  contains exactly one of them. If  $\mathbf{z}$  and  $\mathbf{z}'$  are the two points in  $B_2(\mathbf{x}) \cap Z$  and the point  $\mathbf{y} \in B_1(\mathbf{x})$  has been chosen in such a way that  $\mathbf{z} \notin B_1(\mathbf{y})$  and  $\mathbf{z}' \in B_1(\mathbf{y})$ , then  $E(B_2(\mathbf{x})) \geq E(\mathbf{z}) + E(B_1(\mathbf{y})) \geq 1 + 2 = 3$ , since  $E(B_1(\mathbf{y})) \equiv 0 \pmod{2}$  by (6.3.10) for  $s = 1$ .

Let  $C' = \{\mathbf{c}'_1, \mathbf{c}'_2, \dots, \mathbf{c}'_{K'}\}$  be a maximal subcode of  $C$  with minimum distance 3. Then the spheres  $B_1(\mathbf{c}')$ ,  $\mathbf{c}' \in C'$ , are disjoint and every sphere  $B_1(\mathbf{c})$ ,  $\mathbf{c} \in C \setminus C'$ , intersects at least one of the spheres  $B_1(\mathbf{c}')$ ,  $\mathbf{c}' \in C'$ , in two points. The definition of  $C'$  implies that every point  $\mathbf{x} \in \mathbb{F}^n \setminus B_1(C')$  satisfies (6.3.17) and hence (6.3.18).

We now estimate the sum

$$\sum_{\mathbf{x} \in B_1(C')} E(B_2(\mathbf{x})).$$

Define

$$f_i = |B_2(\mathbf{c}'_i) \cap (C \setminus C')|, \text{ for } i = 1, 2, \dots, K'$$

and further

$h_i =$  the number of indices  $j \in \{1, 2, \dots, K'\}$  for which  $f_j = 2i$  or  $2i - 1$ .

Clearly

$$\sum_{i \geq 0} h_i = K' \quad (6.3.19)$$

and

$$\sum_{i \geq 0} 2ih_i \geq K - K' \quad (6.3.20)$$

because  $|B_2(\mathbf{c}) \cap C'| \geq 1$  for every  $\mathbf{c} \in C \setminus C'$ .

Consider a fixed  $j$  and assume that  $B_2(\mathbf{c}'_j) \cap (C \setminus C') = \{\mathbf{c}_1, \dots, \mathbf{c}_{f_j}\}$ . Then for every  $\mathbf{x} \in B_1(\mathbf{c}'_j)$  and  $h = 1, 2, \dots, f_j$  we have  $|B_1(\mathbf{c}'_j) \cap B_1(\mathbf{c}_h) \cap B_2(\mathbf{x})| \geq 2$  because  $d(\mathbf{c}'_j, \mathbf{c}_h) \leq 2$  implies that there are two points  $\mathbf{y}_1, \mathbf{y}_2 \in B_1(\mathbf{c}'_j) \cap B_1(\mathbf{c}_h)$  and  $d(\mathbf{y}_1, \mathbf{x}) \leq 2$  and  $d(\mathbf{y}_2, \mathbf{x}) \leq 2$ . Consequently,

$$E(B_2(\mathbf{x})) \geq \sum_{h=1}^{f_j} |B_1(\mathbf{c}'_j) \cap B_1(\mathbf{c}_h) \cap B_2(\mathbf{x})| \geq 2f_j. \quad (6.3.21)$$

In particular, (6.3.17) holds if  $f_j \geq 1$ .

We now claim that if  $f_j = 2i$  or  $2i - 1$ , and  $\mathbf{x} \in B_1(\mathbf{c}'_j)$ , then

$$E(B_2(\mathbf{x})) \geq 3i + 2.$$

Indeed, for  $i = 0, 1, 2, 3$  this follows from (6.3.15), (6.3.16), (6.3.18) and (6.3.21). When  $i \geq 4$ , this immediately follows from (6.3.21) because  $2(2i - 1) \geq 3i + 2$ .

Therefore

$$\begin{aligned} \sum_{\mathbf{x} \in B_1(C')} E(B_2(\mathbf{x})) &\geq \sum_{i \geq 0} (n+1)(3i+2)h_i \\ &\geq 3(n+1)(K - K')/2 + 2(n+1)K'. \end{aligned}$$

All in all we get

$$\begin{aligned} &5(2^n - K'(n+1)) + 3(n+1)(K - K')/2 + 2(n+1)K' \\ &\leq \sum_{\mathbf{x} \notin B_1(C')} E(B_2(\mathbf{x})) + \sum_{\mathbf{x} \in B_1(C')} E(B_2(\mathbf{x})) = V(n, 2)(K(n+1) - 2^n), \end{aligned}$$

and hence

$$(V(n, 2) - 3/2)(n+1)K \geq (V(n, 2) + 5)2^n - 9A(n, 3)(n+1)/2$$

as claimed.  $\square$

## 6.4 Excess bounds for codes with arbitrary covering radius

We now study how the arguments used in the previous section can be generalized to arbitrary covering radius. We assume that  $C$  is a binary code of length  $n$  and covering radius  $R$ ,  $1 \leq R \leq n$ , and use the same notations as in the previous section.

Assume first that  $\mathbf{x} \in \mathbb{F}^n$  and  $d(\mathbf{x}, C) = R$ , and study how the points in  $B_1(\mathbf{x})$  are covered by the codewords of  $C$ . Every sphere  $B_R(\mathbf{c})$  intersects  $B_1(\mathbf{x})$  in exactly 0 or  $R + 1$  points, depending on whether  $d(\mathbf{c}, \mathbf{x})$  is greater than  $R + 1$  or belongs to the set  $\{R, R + 1\}$ . By (6.3.4),

$$E(B_1(\mathbf{x})) \equiv -|B_1(\mathbf{x})| \equiv -n - 1 \pmod{R + 1}. \quad (6.4.1)$$

Since  $E(B_1(\mathbf{x}))$  is a nonnegative integer, we have proved the following lemma.

**Lemma 6.4.2** *If  $d(\mathbf{x}, C) = R$ , then*

$$E(B_1(\mathbf{x})) \geq \varepsilon := (R + 1) \lceil \frac{n + 1}{R + 1} \rceil - (n + 1).$$

□

Let  $A$  again stand for the set of deep holes, i.e.,  $A = \{\mathbf{x} \in \mathbb{F}^n : d(\mathbf{x}, C) = R\}$ . As in the previous section,  $Z_i$  denotes the set of points covered by exactly  $i + 1$  codewords of  $C$ ,  $i = 0, 1, \dots$ , and  $Z$  the set of all points covered by at least two codewords of  $C$ .

**Lemma 6.4.3** *If  $\mathbf{z} \in Z$ , then*

$$|A \cap B_1(\mathbf{z})| \leq n - R.$$

**Proof.** If  $d(\mathbf{z}, C) \leq R - 2$ , then none of the points in  $B_1(\mathbf{z})$  can belong to  $A$  and the claim holds. The point  $\mathbf{z}$  is covered by (at least) two different codewords  $\mathbf{a}, \mathbf{b} \in C$ , and we can now assume that  $d(\mathbf{a}, \mathbf{z}), d(\mathbf{b}, \mathbf{z}) \in \{R - 1, R\}$ . Assume that  $d(\mathbf{a}, \mathbf{z}) = d(\mathbf{b}, \mathbf{z}) = R$ . Since  $\mathbf{a} + \mathbf{z} \neq \mathbf{b} + \mathbf{z}$ , the union of the supports of  $\mathbf{a} + \mathbf{z}$  and  $\mathbf{b} + \mathbf{z}$  contains at least  $R + 1$  elements  $i$ , and the points  $\mathbf{z} + \mathbf{e}_i$  cannot belong to  $A$ . The claim is proved similarly in the other two cases. □

If we know that the minimum distance of  $C$  is  $d$ , then in the same way as in the previous proof we can show that  $|A \cap B_1(\mathbf{z})| \leq n + 1 - R - \lceil d/2 \rceil$ .

Lemmas 6.4.2 and 6.4.3 lead to the *first excess bound for arbitrary  $R$* .

**Theorem 6.4.4** *If  $n > R$ , then*

$$K(n, R) \geq \frac{(n - R + \varepsilon)2^n}{(n - R)V(n, R) + \varepsilon V(n, R - 1)},$$

where  $\varepsilon = (R + 1)\lceil(n + 1)/(R + 1)\rceil - (n + 1)$ .

**Proof.** By Lemma 6.4.2,  $E(B_1(\mathbf{x})) \geq \varepsilon$  for all  $\mathbf{x} \in A$  and trivially  $|A| \geq 2^n - |C|V(n, R - 1)$ . Therefore by (6.3.3), Lemma 6.4.3 and (6.3.6),

$$\begin{aligned} \varepsilon(2^n - |C|V(n, R - 1)) &\leq \sum_{\mathbf{x} \in A} E(B_1(\mathbf{x})) \\ &= \sum_{\mathbf{x} \in A} \sum_{i > 0} i|Z_i \cap B_1(\mathbf{x})| \\ &= \sum_{i > 0} i \sum_{\mathbf{z} \in Z_i} |A \cap B_1(\mathbf{z})| \\ &\leq \sum_{i > 0} i(n - R)|Z_i| \\ &= (n - R)(|C|V(n, R) - 2^n), \end{aligned}$$

proving our claim.  $\square$

When  $R = 1$ , the previous theorem reduces to Theorem 6.3.8.

Theorem 6.4.4 can be slightly improved by dividing the set  $Z$  into several classes, obtaining improved estimates for some of the classes and then using a suitable averaging argument. The proof is somewhat complicated and is omitted.

**Theorem 6.4.5** *If  $R \geq 2$ ,  $n \geq 2R + 1$  and*

$$\varepsilon = (R + 1)\lceil(n + 1)/(R + 1)\rceil - (n + 1) \leq R - 1,$$

*then*

$$K(n, R) \geq \frac{(\rho + \varepsilon)2^n}{\rho V(n, R) + \varepsilon V(n, R - 1)},$$

*where*

$$\rho = \begin{cases} n - 3 + 2/n & \text{if } R = 2 \\ n - R - 1 & \text{if } R \geq 3. \end{cases}$$

$\square$

## 6.5 The method of linear inequalities

Let again  $C$  be an  $(n, K)R$  code and denote

$$\mathcal{A}_i(\mathbf{x}) = |\{\mathbf{c} \in C : d(\mathbf{c}, \mathbf{x}) = i\}|$$

and

$$\mathcal{A}_i = \mathcal{A}_i(\mathbf{0}).$$

In this section we compute lower bounds on the cardinality of  $C$  by deriving linear inequalities on the quantities  $\mathcal{A}_i$  and  $\mathcal{A}_i(\mathbf{x})$ .

The first inequalities are obtained by considering separately how the vectors of each weight  $i$  in  $\mathbb{F}^n$  are covered. When  $R = 1$ , it is clear that each codeword of weight  $i + 1$  covers  $i + 1$  of them, a codeword of weight  $i$  covers just itself, and a codeword of weight  $i - 1$  covers  $n - i + 1$  of them. Therefore

$$(n - i + 1)\mathcal{A}_{i-1} + \mathcal{A}_i + (i + 1)\mathcal{A}_{i+1} \geq \binom{n}{i}. \quad (6.5.1)$$

Since we may always consider a translate  $\mathbf{x} + C$  instead of  $C$ , we immediately obtain

$$(n - i + 1)\mathcal{A}_{i-1}(\mathbf{x}) + \mathcal{A}_i(\mathbf{x}) + (i + 1)\mathcal{A}_{i+1}(\mathbf{x}) \geq \binom{n}{i} \quad (6.5.2)$$

for every  $\mathbf{x}$ .

The easy proof of the following lemma is omitted.

**Lemma 6.5.3** *If the vectors  $\mathbf{x}, \mathbf{y} \in \mathbb{F}^n$  have distance  $d(\mathbf{x}, \mathbf{y}) = h$ , then the number of vectors  $\mathbf{z} \in \mathbb{F}^n$  such that  $d(\mathbf{x}, \mathbf{z}) = i$  and  $d(\mathbf{z}, \mathbf{y}) = j$  is  $\binom{h}{\frac{1}{2}(i-j+h)} \binom{n-h}{\frac{1}{2}(i+j-h)}$  if  $i + j + h$  is even, and zero otherwise.  $\square$*

Using the previous lemma, similar inequalities can easily be derived for arbitrary covering radius  $R$ . To determine how many vectors of weight  $i$  a codeword  $\mathbf{c}$  of weight  $h$  covers, we choose  $\mathbf{x} = \mathbf{0}$ ,  $\mathbf{y} = \mathbf{c}$  and let  $j$  range from 0 to  $R$ .

The following lemma gives a lower bound on  $K$  based on a single inequality.

**Lemma 6.5.4** *If a code  $C$  with  $K$  codewords satisfies the inequality*

$$\lambda_0\mathcal{A}_0(\mathbf{x}) + \lambda_1\mathcal{A}_1(\mathbf{x}) + \dots + \lambda_n\mathcal{A}_n(\mathbf{x}) \geq \beta \quad (6.5.5)$$

for all  $\mathbf{x} \in \mathbb{F}^n$ , where  $\lambda_0, \lambda_1, \dots, \lambda_n \in \mathbb{R}$ , then

$$K \geq \frac{\beta 2^n}{\sum_{i=0}^n \lambda_i \binom{n}{i}},$$

provided that the denominator is positive.

**Proof.** The claim follows by adding together the inequalities (6.5.5) for all  $\mathbf{x} \in \mathbb{F}^n$ , because  $\sum_{\mathbf{x} \in \mathbb{F}^n} \mathcal{A}_i(\mathbf{x}) = K \binom{n}{i}$ .  $\square$

Using the following lemma we can exploit information about pair covering designs from Section 2.7. In the remainder of this section it is convenient to extend the definition of the function  $F(v, s)$  and define

$$F(v, s) = \begin{cases} 1 & \text{if } 2 \leq v \leq s \\ 0 & \text{if } v < 2. \end{cases}$$

**Lemma 6.5.6** *Assume that  $C \subseteq \mathbb{F}^n$  has covering radius  $R$ . If  $\mathcal{A}_0 = \mathcal{A}_1 = \dots = \mathcal{A}_{R-2} = 0$  and  $\mathcal{A}_{R-1} + \mathcal{A}_R = i$ , then*

$$\mathcal{A}_{R+1} + \mathcal{A}_{R+2} \geq F(n - iR + 1, R + 2).$$

**Proof.** Assume first that there is a codeword of weight  $R - 1$  in  $C$ , and denote by  $T$  the union of the supports of the codewords of weight  $R - 1$  and  $R$ . Clearly,  $|T| \leq iR - 1$ . All the vectors of weight two that have at least one 1 in a coordinate that belongs to  $T$  and all the vectors of weight one are covered by the codewords of weight  $R - 1$  and  $R$ . The remaining vectors of weight two, whose supports are subsets of  $\{1, 2, \dots, n\} \setminus T$ , must be covered by the codewords of weight  $R + 1$  and  $R + 2$ . Clearly it is more efficient to use only codewords of weight  $R + 2$ , and we need at least  $F(n - iR + 1, R + 2)$  of them. Notice that if  $n - iR + 1 \leq R + 2$  our claim is trivial.

Assume then that there are no codewords of weight  $R - 1$ , and denote by  $T$  the union of the supports of the codewords of weight  $R$ . Clearly  $|T| \leq iR$ . The codewords of weight  $R + 1$  and  $R + 2$  must cover all the vectors of weight one and two whose supports are subsets of the set  $\{1, 2, \dots, n\} \setminus T$ . Append 1 to the codewords of weight  $R + 1$  and 0 to the codewords of weight  $R + 2$ . Together these new words of length  $n + 1$  and weight  $R + 2$  cover all the vectors of weight two whose supports are subsets of the set  $\{1, 2, \dots, n + 1\} \setminus T$ , and therefore there are at least  $F(n + 1 - iR, R + 2)$  of them.  $\square$

Using Lemma 6.5.6 we can get inequalities on the  $\mathcal{A}_i$ 's in the following way. Choose an arbitrary positive number  $m_1$  and define

$$m_0 = \min_{i \geq 1} \{m_1 i + F(n - iR + 1, R + 2)\}. \quad (6.5.7)$$

Lemma 6.5.6 implies that for any code  $C \subseteq \mathbb{F}^n$  with covering radius  $R$ ,

$$\sum_{i=0}^{R-2} m_0 \mathcal{A}_i + m_1 (\mathcal{A}_{R-1} + \mathcal{A}_R) + (\mathcal{A}_{R+1} + \mathcal{A}_{R+2}) \geq m_0.$$

Replacing  $C$  by the translate  $\mathbf{x} + C$ , we get the same inequality for the  $\mathcal{A}_i(\mathbf{x})$ 's, i.e.,

$$\sum_{i=0}^{R-2} m_0 \mathcal{A}_i(\mathbf{x}) + m_1 (\mathcal{A}_{R-1}(\mathbf{x}) + \mathcal{A}_R(\mathbf{x})) + (\mathcal{A}_{R+1}(\mathbf{x}) + \mathcal{A}_{R+2}(\mathbf{x})) \geq m_0$$

for all  $\mathbf{x} \in \mathbb{F}^n$ . Lemma 6.5.4 now implies that

$$K(n, R) \geq \frac{m_0 2^n}{\sum_{i=0}^{R-2} m_0 \binom{n}{i} + m_1 (\binom{n}{R-1} + \binom{n}{R}) + (\binom{n}{R+1} + \binom{n}{R+2})}. \quad (6.5.8)$$

**Theorem 6.5.9 (Pair covering inequality)** *If  $C \subseteq \mathbb{F}^n$  has covering radius  $R$ , then for all  $\mathbf{x} \in \mathbb{F}^n$ ,*

$$\sum_{i=0}^{R-2} m_0 \mathcal{A}_i(\mathbf{x}) + m_1 (\mathcal{A}_{R-1}(\mathbf{x}) + \mathcal{A}_R(\mathbf{x})) + (\mathcal{A}_{R+1}(\mathbf{x}) + \mathcal{A}_{R+2}(\mathbf{x})) \geq m_0,$$

where

$$m_1 = \max_{i \geq 2} \frac{F(n - R + 1, R + 2) - F(n - iR + 1, R + 2)}{i - 1},$$

and

$$m_0 = m_1 + F(n - R + 1, R + 2).$$

**Proof.** The choices for  $m_0$  and  $m_1$  satisfy (6.5.7) because for every  $i \geq 2$ ,

$$\begin{aligned} & m_1 i + F(n - iR + 1, R + 2) \\ &= m_1 + m_1(i - 1) + F(n - iR + 1, R + 2) \\ &\geq m_1 + (F(n - R + 1, R + 2) - F(n - iR + 1, R + 2)) \\ &\quad + F(n - iR + 1, R + 2) \\ &= m_0. \end{aligned}$$

□

Notice that  $m_0 > m_1 > 0$  when  $R < n$ .

We can also derive new inequalities from old ones. Assume that the inequality

$$\lambda_0 \mathcal{A}_0(\mathbf{z}) + \lambda_1 \mathcal{A}_1(\mathbf{z}) + \dots + \lambda_n \mathcal{A}_n(\mathbf{z}) \geq \beta \quad (6.5.10)$$

holds for all  $\mathbf{z} \in \mathbb{F}^n$ . An *induced inequality* is obtained by adding together (6.5.10) for all  $\mathbf{z} \in S_i(\mathbf{x})$ , where  $\mathbf{x} \in \mathbb{F}^n$  is fixed, and using Lemma 6.5.3. Given  $\mathbf{x}$  and a codeword  $\mathbf{y} \in C$  with  $d(\mathbf{x}, \mathbf{y}) = h$ , the number of vectors

$\mathbf{z} \in S_i(\mathbf{x})$  such that  $d(\mathbf{z}, \mathbf{y}) = j$  equals  $\binom{h}{\frac{1}{2}(i-j+h)} \binom{n-h}{\frac{1}{2}(i+j-h)}$  if  $i+j+h$  is even, and zero otherwise. In the induced inequality the coefficient of  $\mathcal{A}_h(\mathbf{x})$  is

$$\sum_j \lambda_j \binom{h}{\frac{1}{2}(i-j+h)} \binom{n-h}{\frac{1}{2}(i+j-h)}$$

where  $j$  ranges over integers such that  $i+j+h$  is even. Hence the induced inequality is

$$\sum_h \mathcal{A}_h(\mathbf{x}) \sum_j \lambda_j \binom{h}{\frac{1}{2}(i-j+h)} \binom{n-h}{\frac{1}{2}(i+j-h)} \geq \binom{n}{i} \beta, \quad (6.5.11)$$

and this again holds for all  $\mathbf{x} \in \mathbb{F}^n$ .

The induced inequalities obtained by adding together the sphere-covering inequalities

$$\mathcal{A}_0(\mathbf{z}) + \mathcal{A}_1(\mathbf{z}) + \dots + \mathcal{A}_R(\mathbf{z}) \geq 1$$

for all  $\mathbf{z} \in S_i(\mathbf{x})$  are just the inequalities discussed at the beginning of this section. If we add together the sphere-covering inequalities for all  $\mathbf{z} \in S_0(\mathbf{x}) \cup S_1(\mathbf{x})$ , we get the induced inequality

$$\sum_{i=0}^{R-1} (n+1) \mathcal{A}_i(\mathbf{x}) + (R+1) \mathcal{A}_R(\mathbf{x}) + (R+1) \mathcal{A}_{R+1}(\mathbf{x}) \geq n+1.$$

Since all the quantities are integers, this further implies that

$$\sum_{i=0}^{R-1} \lceil \frac{n+1}{R+1} \rceil \mathcal{A}_i(\mathbf{x}) + \mathcal{A}_R(\mathbf{x}) + \mathcal{A}_{R+1}(\mathbf{x}) \geq \lceil \frac{n+1}{R+1} \rceil, \quad (6.5.12)$$

which is essentially the result of Lemma 6.4.2.

**Example 6.5.13** Assume that  $C \subseteq \mathbb{F}^{16}$  has covering radius 3. We first derive the pair covering inequality for  $C$ . From Table 2.4 we obtain the values

$F(17 - 3i, 5)$		12	7	4	1	1	0
$i$		1	2	3	4	5	6

and get  $m_1 = 5$  and  $m_0 = 17$ . Hence the pair covering inequality becomes

$$17\mathcal{A}_0(\mathbf{z}) + 17\mathcal{A}_1(\mathbf{z}) + 5\mathcal{A}_2(\mathbf{z}) + 5\mathcal{A}_3(\mathbf{z}) + \mathcal{A}_4(\mathbf{z}) + \mathcal{A}_5(\mathbf{z}) \geq 17. \quad (6.5.14)$$

Now (6.5.8) gives the lower bound

$$K(16, 3) \geq 113,$$

compared to the sphere-covering bound  $K(16, 3) \geq 95$ . The induced inequality obtained by adding together (6.5.14) for all  $\mathbf{z} \in S_0(\mathbf{x}) \cup S_1(\mathbf{x})$  gives

$$\begin{aligned} 289\mathcal{A}_0(\mathbf{x}) + 109\mathcal{A}_1(\mathbf{x}) + 109\mathcal{A}_2(\mathbf{x}) + 33\mathcal{A}_3(\mathbf{x}) + 33\mathcal{A}_4(\mathbf{x}) \\ + 6\mathcal{A}_5(\mathbf{x}) + 6\mathcal{A}_6(\mathbf{x}) \geq 289. \end{aligned} \quad (6.5.15)$$

From (6.5.12) we obtain

$$5\mathcal{A}_0(\mathbf{x}) + 5\mathcal{A}_1(\mathbf{x}) + 5\mathcal{A}_2(\mathbf{x}) + \mathcal{A}_3(\mathbf{x}) + \mathcal{A}_4(\mathbf{x}) \geq 5.$$

Multiplying this by 3 and adding to (6.5.15) gives

$$\begin{aligned} 304\mathcal{A}_0(\mathbf{x}) + 124\mathcal{A}_1(\mathbf{x}) + 124\mathcal{A}_2(\mathbf{x}) + 36\mathcal{A}_3(\mathbf{x}) \\ + 36\mathcal{A}_4(\mathbf{x}) + 6\mathcal{A}_5(\mathbf{x}) + 6\mathcal{A}_6(\mathbf{x}) \geq 304. \end{aligned}$$

Application of Lemma 6.5.4 still gives the same lower bound  $K(16, 3) \geq 113$ . Dividing by 6 and using the fact that all the quantities are integers we obtain

$$51\mathcal{A}_0(\mathbf{x}) + 21\mathcal{A}_1(\mathbf{x}) + 21\mathcal{A}_2(\mathbf{x}) + 6\mathcal{A}_3(\mathbf{x}) + 6\mathcal{A}_4(\mathbf{x}) + \mathcal{A}_5(\mathbf{x}) + \mathcal{A}_6(\mathbf{x}) \geq 51,$$

and now Lemma 6.5.4 gives the lower bound

$$K(16, 3) \geq 114.$$

The process of finding good induced inequalities is discussed in more detail in Zhang [704].  $\square$

Once we have a set of inequalities for  $\mathcal{A}_i$  (or similarly for  $\mathcal{A}_i(\mathbf{x})$  or  $\mathcal{B}_i$ ) we can use linear programming to determine the minimum of  $\mathcal{A}_0 + \mathcal{A}_1 + \dots + \mathcal{A}_n$ , which gives a lower bound on the cardinality of the code.

Many of the best currently known lower bounds on  $K(n, R)$  have been obtained by studying how a code  $C$  covers the vectors in a sphere of radius three. The bounds become technically much more involved, and we refer the reader to Zhang and Lo [705] and Li and Chen [423].

For another approach using linear inequalities, see Section 13.4.

We conclude this section by discussing some bounds that use linear inequalities and excess arguments.

Assume that  $C \subseteq \mathbb{F}^n$  has covering radius 1. Consider the inequality (6.5.2) which resulted from the fact that all the vectors at distance  $i$  from  $\mathbf{x}$  are covered at least once. The difference between the left hand side and the right hand side is simply the excess on  $S_i(\mathbf{x})$ , i.e.,

$$E(S_i(\mathbf{x})) = (n - i + 1)\mathcal{A}_{i-1}(\mathbf{x}) + \mathcal{A}_i(\mathbf{x}) + (i + 1)\mathcal{A}_{i+1}(\mathbf{x}) - \binom{n}{i}. \quad (6.5.16)$$

Using these equations we can find congruences for suitable linear combinations of the quantities  $E(S_i(\mathbf{x}))$ . We denote

$$E_i(\mathbf{x}) := E(S_i(\mathbf{x})).$$

Take, for example,  $E(\mathbf{x}) = E_0(\mathbf{x})$ ,  $E_1(\mathbf{x})$  and  $E_2(\mathbf{x})$ . We get

$$\begin{aligned} E(\mathbf{x}) &= \mathcal{A}_0(\mathbf{x}) & +\mathcal{A}_1(\mathbf{x}) & & -1 \\ E_1(\mathbf{x}) &= n\mathcal{A}_0(\mathbf{x}) & +\mathcal{A}_1(\mathbf{x}) & +2\mathcal{A}_2(\mathbf{x}) & -n \\ E_2(\mathbf{x}) &= (n-1)\mathcal{A}_1(\mathbf{x}) & +\mathcal{A}_2(\mathbf{x}) & +3\mathcal{A}_3(\mathbf{x}) & -\frac{1}{2}n(n-1). \end{aligned}$$

Consider these equations modulo 3. We easily verify the following congruences

$$E_1(\mathbf{x}) + E_2(\mathbf{x}) \equiv 0 \pmod{3} \quad \text{if } n \equiv 0 \pmod{3} \quad (6.5.17)$$

$$2E(\mathbf{x}) + E_1(\mathbf{x}) + E_2(\mathbf{x}) \equiv 0 \pmod{3} \quad \text{if } n \equiv 1 \pmod{3} \quad (6.5.18)$$

$$E(\mathbf{x}) + E_1(\mathbf{x}) + E_2(\mathbf{x}) \equiv 2 \pmod{3} \quad \text{if } n \equiv 2 \pmod{3}. \quad (6.5.19)$$

Notice that (6.5.19) is the special case  $s = 2$  of (6.3.12).

In the same way we obtain the congruences

$$E_2(\mathbf{x}) + E_3(\mathbf{x}) \equiv 0 \pmod{4} \quad \text{if } n \equiv 1 \pmod{4}$$

$$E(\mathbf{x}) + E_1(\mathbf{x}) + E_2(\mathbf{x}) + E_3(\mathbf{x}) \equiv 0 \pmod{4} \quad \text{if } n \equiv 3 \pmod{4}.$$

**Lemma 6.5.20** *If  $n \equiv 2, 4 \pmod{6}$ , then*

$$\frac{1}{2}nE(\mathbf{x}) + E_1(\mathbf{x}) + E_2(\mathbf{x}) \geq \frac{1}{2}n + 1. \quad (6.5.21)$$

**Proof.** Assume that  $n \equiv 2 \pmod{6}$ . If  $E(\mathbf{x}) \geq 2$ , there is nothing to prove; if  $E(\mathbf{x}) = 1$ , the claim follows from (6.5.19). Assume that  $E(\mathbf{x}) = 0$ . There are at least  $n-1$  vectors  $\mathbf{y} \in S_1(\mathbf{x})$  such that  $\mathbf{y} \notin C$  and hence  $E(B_1(\mathbf{y})) \geq 1$  by (6.3.7). Therefore

$$n-1 \leq \sum_{\mathbf{y} \in S_1(\mathbf{x})} E(B_1(\mathbf{y})) \leq E(S_1(\mathbf{x})) + 2E(S_2(\mathbf{x}))$$

and  $E_1(\mathbf{x}) + E_2(\mathbf{x}) \geq \frac{1}{2}(n-1)$ , and the claim follows from (6.5.19). If  $n \equiv 4 \pmod{6}$ , we use (6.5.18) instead of (6.5.19).  $\square$

**Theorem 6.5.22** *If  $n \equiv 20, 40 \pmod{60}$ , then*

$$K(n, 1) \geq \frac{(n+1)(n+2)(n^2+n+12)+96}{(n+1)(n+2)(n^2+n+12)n} 2^n.$$

**Proof.** Writing (6.5.21) in terms of the  $\mathcal{A}_i(\mathbf{x})$ 's and dividing by 3, we get the inequality

$$\frac{n}{2}(\mathcal{A}_0(\mathbf{x}) + \mathcal{A}_1(\mathbf{x})) + \mathcal{A}_2(\mathbf{x}) + \mathcal{A}_3(\mathbf{x}) - \frac{(n+1)(n+2)}{6} \geq 0 \quad (6.5.23)$$

for all  $\mathbf{x} \in \mathbb{F}^n$ . Let  $\mathbf{y} \in \mathbb{F}^n$  be arbitrary. Adding together the inequalities (6.5.23) for all  $\mathbf{x} \in B_2(\mathbf{y})$  and using Lemma 6.5.3 or (6.5.11), we get

$$\begin{aligned} n^2(\mathcal{A}_0(\mathbf{y}) + \mathcal{A}_1(\mathbf{y})) + \left(\frac{9n}{2} - 5\right)(\mathcal{A}_2(\mathbf{y}) + \mathcal{A}_3(\mathbf{y})) + 10(\mathcal{A}_4(\mathbf{y}) + \mathcal{A}_5(\mathbf{y})) \\ \geq V(n, 2) \frac{(n+1)(n+2)}{6}. \end{aligned}$$

To make the coefficient of  $\mathcal{A}_2(\mathbf{y}) + \mathcal{A}_3(\mathbf{y})$  divisible by 10, we add (6.5.23) for  $\mathbf{x} = \mathbf{y}$  multiplied by 5 to obtain

$$\begin{aligned} (n^2 + \frac{5n}{2})(\mathcal{A}_0(\mathbf{y}) + \mathcal{A}_1(\mathbf{y})) + \frac{9n}{2}(\mathcal{A}_2(\mathbf{y}) + \mathcal{A}_3(\mathbf{y})) + 10(\mathcal{A}_4(\mathbf{y}) + \mathcal{A}_5(\mathbf{y})) \\ \geq (V(n, 2) + 5) \frac{(n+1)(n+2)}{6}. \end{aligned}$$

Now the left hand side is divisible by 10, and the right hand side is congruent to 2  $(\bmod 10)$ . Therefore in fact

$$\begin{aligned} (n^2 + \frac{5n}{2})(\mathcal{A}_0(\mathbf{y}) + \mathcal{A}_1(\mathbf{y})) + \frac{9n}{2}(\mathcal{A}_2(\mathbf{y}) + \mathcal{A}_3(\mathbf{y})) + 10(\mathcal{A}_4(\mathbf{y}) + \mathcal{A}_5(\mathbf{y})) \\ \geq (V(n, 2) + 5) \frac{(n+1)(n+2)}{6} + 8. \end{aligned}$$

The claim now follows from Lemma 6.5.4. □

## 6.6 Table on $K(n, R)$

In the next table we give the best currently known lower and upper bounds on the function  $K(n, R)$ . Many of the upper bounds are attained by a linear code or have been obtained using the ADS construction. Some upper bounds are also obtained using the trivial formula  $K(n+1, R) \leq 2K(n, R)$ , the result  $K(2n+1, 1) \leq 2^n K(n, 1)$  (Theorem 3.4.3) or the corresponding result for  $R > 1$  (Theorem 3.4.5). In most of the other cases the table entry gives the earliest reference, but the reader should also consult the Notes of Chapter 3.

For the lower bounds, we try to refer to the earliest source where the numerical bound has been documented, but we have not made any calculations to see which of the current records should be attributed to the early paper by S. M. Johnson [354].

The exact values are known in the following cases:

$$K(n, 0) = 2^n \text{ for all } n;$$

$$K(R, R) = 1 \text{ for all } R \geq 1;$$

$$K(n, R) = 2 \text{ when } R < n \leq 2R + 1;$$

$$K(2R + 2, R) = 4 \text{ for all } R \geq 1;$$

$$K(2R + 3, R) = 7 \text{ for all } R \geq 1;$$

$$K(2R + 4, R) = 12 \text{ for } R = 1 \text{ and } R = 2;$$

$$K(2^m - 1, 1) = 2^{2^m - m - 1} \text{ for all } m \geq 3;$$

$$K(2^m, 1) = 2^{2^m - m} \text{ for all } m \geq 3;$$

$$K(23, 3) = 4096.$$

In all the other cases the exact value is not known.

Notice that although  $K(23, 2) \leq 2^{15}$ ,  $K(24, 2) \leq 2^{16}$  and  $K(15+2i, 4+i) \leq 32$  for all  $i \geq 0$ , we know that no linear  $[23, 15]2$ ,  $[24, 16]2$ ,  $[15+2i, 5]4+i$  codes exist by the tables for linear codes and Theorem 5.2.7.

Table 6.1: Bounds on  $K(n, R)$ , Part I.

$n$	$R = 1$	$R = 2$	$R = 3$
1	1		
2	2	1	
3	2	2	1
4	c 4 L	2	2
5	c 7 S	2	2
6	f 12 S	c 4 L	2
7	a 16 L	c 7 Q	2
8	d 32 L	p 12 Q	c 4 L
9	k 55–62 W	j 15–16 L	c 7 Q
10	h 105–120 X	h 23–30 Y	h 9–12 Q
11	e 178–192 S	h 36–44 R	h 12–16 L
12	d 342–380 T	d 61–78 T	i 18–28 T
13	b 598–736 T	g 97–128 L	j 28–42 T
14	m 1172–1408 T	b 157–256 L	j 44–64 L
15	a 2048 L	j 309–384 U	j 70–112 R
16	d 4096 L	h 512–768 P	h 114–192 T
17	e 7399–8192 L	b 859–1536 P	i 186–320 T
18	d 14564–16384 L	h 1702–2944 T	i 316–512 L
19	n 26261–31744 R	g 2897–4096 L	h 511–1024 L
20	m 52456–63488 P	h 5328–8192 L	d 889–2048 L
21	k 95330–122880 R	d 9893–14336 U	g 1475–3072 Q
22	d 190651–245760 P	h 17316–24576 U	j 2539–4096 L
23	n 352448–393216 R	j 30677–32768 U	a 4096 L
24	d 699051–786432 P	d 60350–65536 P	h 8123–8192 L
25	k 1290562–1556480 R	g 107203–131072 P	h 13896–16384 L
26	d 2581111–3112960 P	j 190775–262144 P	h 24210–32768 L
27	n 4793641–6029312 R	j 380328–524288 L	h 40675–65536 L
28	m 9587064–12058624 P	g 683910–1048576 L	h 80720–131072 L
29	n 17988086–23068672 R	a 1231356–2097152 L	g 140567–262144 L
30	d 35791395–46137344 P	j 2461754–4194304 L	g 248218–524288 L
31	a $2^{26}$ L	g 4464613–8388480 R	j 443248–524288 U
32	d $2^{27}$ L	j 8168458–16776960 P	d 854890–1048576 P
33	k 252645140–268435456 L	d 16207424–32505856 Q	g 1516050–2097152 P

Table 6.1: Bounds on  $K(n, R)$ , Part II.

$n$	$R = 4$	$R = 5$	$R = 6$
4	1		
5	2	1	
6	2	2	1
7	2	2	2
8	2	2	2
9	2	2	2
10	c 4 L	2	2
11	c 7 Q	2	2
12	c 8 - 12 Q	c 4 L	2
13	h 11 - 16 L	c 7 Q	2
14	g 15 - 28 Q	c 8 - 12 Q	c 4 L
15	i 22 - 32 V	g 9 - 16 L	c 7 Q
16	i 33 - 64 L	g 13 - 28 Q	c 8 - 12 Q
17	j 52 - 112 Q	i 19 - 32 Q	c 8 - 16 L
18	h 83 - 192 Q	i 27 - 64 L	g 11 - 28 Q
19	j 128 - 256 L	i 40 - 64 L	i 16 - 32 Q
20	j 208 - 512 L	j 62 - 128 L	h 23 - 64 L
21	j 336 - 896 Q	j 95 - 256 L	j 33 - 64 L
22	j 553 - 1536 Q	j 150 - 512 L	j 49 - 128 L
23	h 903 - 2048 L	j 235 - 640 U	j 73 - 224 Q
24	j 1505 - 4096 L	j 376 - 1024 L	j 113 - 384 Q
25	h 2554 - 4096 L	j 608 - 2048 L	j 172 - 512 L
26	j 4263 - 8192 L	j 981 - 4096 L	i 272 - 1024 L
27	j 7176 - 14336 Q	j 1601 - 4096 L	j 419 - 1984 Q
28	h 12370 - 24576 Q	j 2629 - 8192 L	j 663 - 3584 Q
29	j 21098 - 32768 L	j 4354 - 14336 Q	j 1068 - 4096 L
30	d 37973 - 65536 L	j 7307 - 24576 Q	j 1727 - 8192 L
31	g 64680 - 126976 Q	j 12220 - 32768 L	j 2808 - 14336 Q
32	g 110215 - 245760 Q	j 20556 - 61440 Q	j 4597 - 24576 Q
33	h 193045 - 393216 Q	j 34731 - 90112 Q	j 7476 - 32768 L

Table 6.1: Bounds on  $K(n, R)$ , Part III.

$n$	$R = 7$	$R = 8$	$R = 9$	$R = 10$
7	1			
8	2	1		
9	2	2	1	
10	2	2	2	1
11	2	2	2	2
12	2	2	2	2
13	2	2	2	2
14	2	2	2	2
15	2	2	2	2
16	c 4 L	2	2	2
17	c 7 Q	2	2	2
18	c 8 - 12 Q	c 4 L	2	2
19	c 8 - 16 L	c 7 Q	2	2
20	g 10 - 28 Q	c 8 - 12 Q	c 4 L	2
21	i 14 - 32 Q	c 8 - 16 L	c 7 Q	2
22	j 20 - 64 L	g 9 - 28 Q	c 8 - 12 Q	c 4 L
23	j 29 - 64 L	i 13 - 32 Q	c 8 - 16 L	c 7 Q
24	j 41 - 128 L	i 18 - 64 L	i 9 - 28 Q	c 8 - 12 Q
25	j 60 - 224 Q	j 25 - 64 L	i 12 - 32 Q	c 8 - 16 L
26	j 88 - 384 Q	j 35 - 128 L	i 16 - 56 V	d 8 - 28 Q
27	j 132 - 512 L	j 50 - 224 Q	j 22 - 64 L	i 11 - 32 Q
28	j 202 - 960 Q	j 73 - 384 Q	g 30 - 128 L	g 14 - 56 Q
29	j 311 - 1408 Q	j 106 - 512 L	h 42 - 224 Q	i 19 - 64 L
30	j 483 - 2048 L	j 158 - 896 Q	j 61 - 384 Q	j 27 - 128 L
31	j 743 - 2048 L	j 238 - 1344 Q	j 88 - 512 L	g 37 - 224 Q
32	j 1179 - 4096 L	j 336 - 2048 L	j 127 - 896 Q	h 51 - 384 Q
33	j 1878 - 8192 L	j 557 - 2048 L	j 188 - 1024 Q	j 74 - 512 L

## Key to Table 6.1

Lower bounds:

- a sphere-covering bound
- b Corollary 6.1.4
- c Theorems 6.2.2, 6.2.5 and 6.2.6 and  $K(n+1, R) \geq K(n, R)$
- d Theorem 6.3.8 and 6.4.4
- e Theorem 6.3.14
- f Stanton and Kalbfleisch [617]
- g Theorem 6.4.5 or Honkala [312]
- h Theorem 6.5.9 and (6.5.8), or Zhang [704]
- i Zhang and Lo [705]
- j Li and Chen [423]
- k Habsieger [269]
- m Habsieger [272]
- n Honkala [321]
- p Blass and Litsyn [85]

Upper bounds:

- L linear code, see Table 7.1
- P  $K(n+1, R) \leq 2K(n, R)$
- Q amalgamated direct sum
- R Theorems 3.4.3 and 3.4.5
- S piecewise constant code (Section 3.3)
- T matrix construction (Theorem 3.5.1) and local search:  
Hämäläinen, Honkala, Kaikkonen and Litsyn [275]:  $K(12, 3) \leq 28$ ,  
 $K(13, 3) \leq 42$ ;  
Hämäläinen, Honkala, Litsyn and Östergård [276]:  $K(16, 3) \leq 192$ ;  
Östergård [516]:  $K(12, 2) \leq 78$ ;  
Östergård [522]:  $K(14, 1) \leq 1408$ ;  
Östergård and Hämäläinen [525]:  $K(13, 1) \leq 736$ ;  
G. Exoo in [524], [525], Wille [688]:  $K(12, 1) \leq 380$   
Östergård and Kaikkonen [526]:  $K(18, 2) \leq 2944$ ,  $K(17, 3) \leq 320$ .
- U blockwise direct sum:  
Example 3.6.2, Theorems 4.5.4 and 4.5.6; or  
[526]:  $K(15, 2) \leq 384$ ,  $K(23, 5) \leq 640$ ;
- V from an Hadamard matrix [526]:  $K(15, 4) \leq 32$ ,  $K(26, 9) \leq 56$ ;
- W Wille [686], [687], [688]
- X Wille [686], [687], Östergård [511]
- Y Hämäläinen and Rankinen [278], Östergård and Hämäläinen [525]

## 6.7 Lower bounds for nonbinary codes

A number of lower bounds have also been obtained in the nonbinary case. Many of the methods presented in the binary case can be generalized, but the proofs are often much more complicated, and here we only give some examples of the flavour of the nonbinary case.

**Example 6.7.1** Assume that  $C$  is an  $(n, K)_31$  code and  $n \equiv 2 \pmod{3}$ . As in the binary case, we define  $E(\mathbf{x}) = |B_1(\mathbf{x}) \cap C| - 1$  and for an arbitrary subset  $V \subseteq \mathbb{F}_3^n$ ,

$$E(V) = \sum_{\mathbf{c} \in C} |B_1(\mathbf{c}) \cap V| - |V|. \quad (6.7.2)$$

As before,

$$E(\mathbb{F}_3^n) = K(2n + 1) - 3^n$$

and

$$\sum_{\mathbf{x} \in \mathbb{F}_3^n} E(S_i(\mathbf{x})) = 2^i \binom{n}{i} \sum_{\mathbf{x} \in \mathbb{F}_3^n} E(\mathbf{x}) = 2^i \binom{n}{i} (K(2n + 1) - 3^n).$$

Let  $\mathbf{x} \in \mathbb{F}_3^n$  be arbitrary, and consider the sphere  $B_2(\mathbf{x})$ . We count the number of vectors in  $S_i(\mathbf{x})$  that a codeword  $\mathbf{c} \in C$  covers when  $i = 0, 1, 2$ . We immediately verify that  $(|S_0(\mathbf{x}) \cap B_1(\mathbf{c})|, |S_1(\mathbf{x}) \cap B_1(\mathbf{c})|, |S_2(\mathbf{x}) \cap B_1(\mathbf{c})|)$  equals  $(1, 2n, 0)$ ,  $(1, 2, 2n - 2)$ ,  $(0, 2, 3)$ ,  $(0, 0, 3)$  or  $(0, 0, 0)$  depending on whether  $d(\mathbf{x}, \mathbf{c}) = 0, 1, 2, 3$  or  $d(\mathbf{x}, \mathbf{c}) \geq 4$ . Since the second component is always even, so is  $E(S_1(\mathbf{x}))$ , and we see that the sum

$$|S_0(\mathbf{x}) \cap B_1(\mathbf{c})| + \frac{3}{2} |S_1(\mathbf{x}) \cap B_1(\mathbf{c})| + |S_2(\mathbf{x}) \cap B_1(\mathbf{c})|$$

is always an integer and divisible by three, except when  $\mathbf{c} = \mathbf{x}$ , in which case it is congruent to 1  $\pmod{3}$ . By (6.7.2) we therefore get

$$\varphi(\mathbf{x}) := E(\mathbf{x}) + \frac{3}{2} E(S_1(\mathbf{x})) + E(S_2(\mathbf{x})) \quad (6.7.3)$$

$$\begin{aligned} &\equiv \mathcal{A}_0(\mathbf{x}) - \left( 1 \cdot 1 + \frac{3}{2} \cdot 2n + 1 \cdot 2^2 \binom{n}{2} \right) \pmod{3} \\ &\equiv 1 + \mathcal{A}_0(\mathbf{x}) \pmod{3}. \end{aligned} \quad (6.7.4)$$

If  $\mathbf{x} \in C$ , then  $\varphi(\mathbf{x}) \geq 2$ . Moreover, if  $\mathbf{x} \in C$ , and  $d(\mathbf{x}, \mathbf{c}) \leq 2$  for some other codeword  $\mathbf{c} \in C$ , then  $|S_1(\mathbf{x}) \cap B_1(\mathbf{c})| \geq 2$ . Thus  $E(S_1(\mathbf{x})) \geq 2$ ,  $\varphi(\mathbf{x}) \geq 3$  and hence  $\varphi(\mathbf{x}) \geq 5$  by (6.7.4). So, if we let  $C_0$  be a maximum subcode of  $C$  with minimum distance three, then  $\varphi(\mathbf{x}) \geq 5$  if  $\mathbf{x} \in C \setminus C_0$ .

If  $\mathbf{x} \notin C$  and  $\varphi(\mathbf{x}) = 1$ , then  $E(S_1(\mathbf{x})) = 0$ . If  $E(\mathbf{x}) = 1$  and  $E(S_2(\mathbf{x})) = 0$ , then for any  $\mathbf{y} \in S_1(\mathbf{x})$ , the excess  $E(S_1(\mathbf{y})) = 1$  is odd, a contradiction.

Similarly,  $E(\mathbf{x}) = 0$ ,  $E(S_2(\mathbf{x})) = 1$  leads to a contradiction. Therefore  $\varphi(\mathbf{x}) \geq 4$  whenever  $\mathbf{x} \notin C$ .

Consequently,

$$(2n^2 + n + 1)(K(2n + 1) - 3^n) = \sum_{\mathbf{x} \in \mathbb{F}_3^n} \varphi(\mathbf{x})$$

$$\geq 4(3^n - K) + 2|C_0| + 5(K - |C_0|) \geq 4 \cdot 3^n + K - 3A_3(n, 3),$$

which leads to the lower bound

$$K \geq \frac{(2n^2 + n + 5)3^n - 3A_3(n, 3)}{(2n + 1)(2n^2 + n + 1) - 1}.$$

Using the upper bounds  $A_3(8, 3) \leq 340$ ,  $A_3(11, 3) \leq 7029$  and  $A_3(14, 3) \leq 153527$  we obtain the lower bounds  $K_3(8, 1) \geq 397$ ,  $K_3(11, 1) \geq 7822$  and  $K_3(14, 1) \geq 166526$ .  $\square$

In the next two examples we prove the optimality of some small covering codes.

**Example 6.7.5** We show that the ternary code of length six and covering radius three with six codewords constructed in Example 15.1.4 is optimal. Let  $\{0, 1, 2\}$  be the ternary alphabet.

We first prove that if  $C \subseteq \{0, 1, 2\}^4$  has four codewords and  $B_1(C) \supseteq \{0, 1\}^4$ , then  $C \subseteq \{0, 1\}^4$ . Assume that the first coordinate in the first codeword is 2. Every binary pair appears in any two of the last three coordinates. Indeed, if the pair 00 does not appear in the last two coordinates, for instance, take a binary pair that does not appear in the first two coordinates to find a binary vector that has distance at least two to  $C$ . Hence  $C$  is

$$\begin{array}{cccc} 2 & 0 & 0 & 0 \\ a & 0 & 1 & 1 \\ b & 1 & 0 & 1 \\ c & 1 & 1 & 0 \end{array}$$

up to equivalence. But  $C$  1-covers  $(0, 1, 0, 0)$  and  $(1, 1, 0, 0)$ , and without loss of generality  $b = 0$  and  $c = 1$ . Because  $C$  covers  $(0, 0, 1, 0)$ , we have  $a = 0$ , but this leaves  $(1, 0, 0, 1)$  uncovered.

Assume now that there is a ternary code  $C$  of length six and covering radius three with only five codewords. In each coordinate one of the letters in the alphabet  $\{0, 1, 2\}$  appears only once. Indeed, if one of them does not appear at all, then  $|C| \geq K_3(5, 2) = 8$ ; here  $K_3(5, 2) \geq 6$  from Lobstein and van Wee [455] is enough. There has to be a codeword that contains at least two such

letters. Without loss of generality, the first codeword is 222222, and 2 appears only once in the first and once in the second coordinate. Consequently the first two coordinates in all the other codewords belong to the set  $\{0, 1\}$ . Because  $C$  covers all the vectors  $(2, 2, \mathbf{x})$  where  $\mathbf{x} \in \{0, 1\}^4$ , all the other codewords belong to  $\{0, 1\}^6$  by the beginning of the proof.

By (6.2.3), a binary code with four codewords can be 2-surjective only if  $n \leq 3$ . Rearranging the coordinates if necessary we can therefore assume that some binary pair, say  $(a, b)$  does not appear in the first two coordinates. Considering only the last four coordinates (again rearranging the coordinates if necessary) we can assume that some binary pair  $(a', b')$  does not appear in the last two coordinates. But then the vector  $(a, b, 2, 2, a', b')$  has distance at least four to  $C$ , a contradiction. Therefore  $K_3(6, 3) = 6$ .

Using the 2-surjectivity argument for ternary codes we immediately obtain the lower bounds  $K_3(8, 4) \geq 6$  and  $K_3(10, 5) \geq 6$ . Indeed, assume that  $C$  is an  $(8, 5)_3 4$  code. Because the number of codewords is less than  $3^2$ , we can find two coordinates in which some ternary pair does not occur. Puncturing these two coordinates we obtain a ternary code of length six and covering radius at most three with at most five codewords, a contradiction. Hence  $K_3(8, 4) \geq 6$ . In the same way  $K_3(10, 5) \geq 6$ .  $\square$

**Example 6.7.6** In this example we show that  $K_4(4, 2) = 7$ . We know from Theorem 3.7.7 that  $K_4(4, 2) \leq 7$ .

Assume first that  $C \subseteq \{0, 1, 2, 3\}^3$ ,  $|C| = 5$  and that  $B_1(C) \supseteq \{0, 1, 2\}^3$ . We claim that then  $C \subseteq \{0, 1, 2\}^3$  and in fact  $C$  is unique up to equivalence. Clearly, each letter 0, 1, 2 appears at least once in every coordinate in such a code  $C$ . Without loss of generality, 2 appears only once in the first coordinate. There can obviously be at most one 3 in the codeword that begins with 2, otherwise  $|C| \geq 3^2$ . We may assume that the first codeword is 22a where  $a = 2$  or  $a = 3$ . Because all the vectors  $2xy$  are covered where  $x, y \in \{0, 1\}$ , we know that the codewords of  $C$  are

$$\begin{array}{ccc} 2 & 2 & a \\ * & 0 & 0 \\ * & 0 & 1 \\ * & 1 & 0 \\ * & 1 & 1. \end{array}$$

Clearly  $a$  has to be 2, otherwise the vector  $(1, 2, 2)$  is not covered. But then all the pairs 00, 01, 10, 11 must also appear in the first and second (respectively, first and third) coordinates, and up to equivalence there is only one way of

choosing the \*'s, namely

$$\begin{matrix} 2 & 2 & 2 \\ 0 & 0 & 0 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 1, \end{matrix}$$

proving our claim.

Assume now that  $C$  is a  $(4, 6)_{42}$  code over the alphabet  $\{0, 1, 2, 3\}$ . We may assume that 3 appears only once in the first coordinate and that the first codeword is 3333. Now the remaining five codewords must cover all the vectors  $(3, \mathbf{x})$  where  $\mathbf{x} \in \{0, 1, 2\}^3$ . By the beginning of the proof, the codewords of  $C$  are (up to equivalence)

$$\begin{matrix} 3 & 3 & 3 & 3 \\ a & 2 & 2 & 2 \\ b & 0 & 0 & 0 \\ c & 1 & 0 & 1 \\ d & 1 & 1 & 0 \\ e & 0 & 1 & 1. \end{matrix}$$

We know that  $a \neq 3$ , so we may assume  $a = 2$ . Because all the vectors with one 3, one 2 and two coordinates in the set  $\{0, 1\}$  must be covered, we see that in every two columns all the four binary pairs 00, 01, 10, 11 appear. Hence the last four codewords are binary and form a 2-surjective code. However, by (6.2.3), a binary code with four codewords can be 2-surjective only if  $n \leq 3$ . This contradiction proves that  $K_4(4, 2) = 7$ .  $\square$

**Example 6.7.7** We show that

$$K_q(n_1 + n_2, R_1 + R_2 + 1) \geq \min\{K_q(n_1, R_1), K_q(n_2, R_2)\}. \quad (6.7.8)$$

Indeed, if  $C$  is an  $(n_1 + n_2, K)_q$  code, let  $C_1$  denote the projection of  $C$  to the first  $n_1$  coordinates, i.e., the code obtained by puncturing the last  $n_2$  coordinates, and  $C_2$  the projection of  $C$  to the last  $n_2$  coordinates. If  $K < \min\{K_q(n_1, R_1), K_q(n_2, R_2)\}$ , then  $C_1$  has covering radius at least  $R_1 + 1$  and  $C_2$  at least  $R_2 + 1$ . Consequently,  $C$  has covering radius at least  $R_1 + R_2 + 2$ , proving (6.7.8).  $\square$

We conclude this section by giving tables of the best currently known bounds on  $K_3(n, R)$ ,  $K_4(n, R)$  and  $K_5(n, R)$  for small values of  $n$  and  $R$ .

Table 6.2: Bounds on  $K_3(n, R)$ .

$n$	$R = 1$	$R = 2$	$R = 3$
1	1		
2	3	1	
3	b 5 B	3	1
4	a 9 H	3	3
5	d 27 A	k 8 M	3
6	h 63–73 S	r 14–17 M	c 6 E
7	q 153–186 R	i 26–34 M	r 9–12 M
8	p 397–486 R	r 54–81 D	r 14–27 D
9	p 1060–1341 T	p 130–219 M	i 25–54 M
10	j 2818–3645 N	i 323–558 M	i 57–108 M
11	p 7822–9477 V	a 729 G	i 115–243 M
12	p 21531–27702 V	i 1919–2187 A	i 282–729 A
13	a 59049 H	i 5062–6561 A	p 611–1215 M
14	p 166526–177147 A	p 12204–19683 A	i 1553–2187 W

$n$	$R = 4$	$R = 5$	$R = 6$	$R = 7$	$R = 8$
4	1				
5	3	1			
6	3	3	1		
7	3	3	3	1	
8	c 6–9 A	3	3	3	1
9	i 8–18 W	s 5–6 W	3	3	3
10	i 16–36 W	c 6–12 W	3	3	3
11	i 28–81 W	a 9–27 A	s 6–9 A	3	3
12	i 62–204 W	i 18–54 W	i 7–18 W	s 6 W	3
13	i 123–408 W	i 32–108 X	i 11–45 Z	s 6–12 W	3
14	p 255–729 W	i 59–243 X	i 21–81 Z	i 8–27 A	s 6–9 A

Table 6.3: Bounds on  $K_4(n, R)$ .

$n$	$R = 1$	$R = 2$	$R = 3$	$R = 4$	$R = 5$	$R = 6$
1	1					
2	4	1				
3	b 8 B	4	1			
4	e 24 K	c 7 C	4	1		
5	a 64 H	i 12-16 W	4	4	1	
6	i 228-256 A	i 28-52 X	i 8-16 A	4	4	1
7	i 748-1024 A	i 80-128 X	i 16-32 W	i 7-12 W	4	4
8	i 2731-3456 X	i 240-384 X	i 39-96 W	i 11-28 W	s 7-8 W	4
9	j 9365-12288 X	i 747-1024 L	i 108-256 W	a 21-64 W	s 8-16 W	4
10	i 34953-49152 A	i 2408-4096 A	i 315-1024 A	i 55-208 X	i 15-64 A	s 7-16 A

Table 6.4: Bounds on  $K_5(n, R)$ .

$n$	$R = 1$	$R = 2$	$R = 3$	$R = 4$	$R = 5$	$R = 6$
1	1					
2	5	1				
3	b 13 B	5	1			
4	g 46-51 K	i 9-11 W	5	1		
5	f 157-184 K	i 20-35 W	i 8-9 Y	5	1	
6	a 625 H	i 65-125 W	s 13-25 W	5	5	1
7	j 2702-3125 A	i 222-525 X	a 30-125 A	s 9-25 A	5	5
8	i 11887-15625 A	i 815-1875 X	i 98-325 Z	i 20-65 Z	s 9-20 W	5
9	j 52796-78125 A	i 3367-7500 X	i 329-1275 Z	i 53-255 Z	i 13-55 Z	s 8-15 W

## Key to Tables 6.2–6.4

## Lower bounds

unmarked	Theorem 3.7.1
a	sphere-covering bound
b	Theorem 3.7.2
c	Examples 6.7.5 and 6.7.6
d	Kamps and van Lint [361]
e	Kalbfleisch and Stanton [358]
f	Kalbfleisch and Weiland [360]
g	Kamps and van Lint [362]
h	Weber [674]
i	Chen and Honkala [134]
j	Habsieger [269]
k	Kolev and Landgev [385] and Östergård and Hääläinen [525]
p	Habsieger [270]
q	Habsieger [271]
r	Blass and Litsyn [84]
s	Example 6.7.7

## Upper bounds

unmarked	Theorem 3.7.1
A	$K_3(n+1, R) \leq 3K_3(n, R)$ or more general direct sum
B	Theorem 3.7.2
C	Theorem 3.7.7
D	Theorem 15.1.2
E	Example 15.1.4
G	Golay code
H	Hamming code
K	Stanton, Horton and Kalbfleisch [616] (Example 3.7.13)
L	Brualdi, Pless and Wilson [105]
M	Hääläinen and Rankinen [278]
N	Blokhuis and Lam [90] and [278]
R	van Laarhoven, Aarts, van Lint and Wille [402]
S	[402] and [278]
T	Östergård [523]
V	Östergård [517]
W	Östergård [512]
X	Östergård [522]
Y	Östergård [516]
Z	Bhandari and Durairajan [78] and [522]

## 6.8 Notes

§6.1 The function  $p(n, K, r)$  (in the nonbinary case) has been used, e.g., in Kalbfleisch and Stanton [358]. Theorem 6.1.3 and Corollary 6.1.4 are from Lobstein [449]; see also Cohen, Lobstein and Sloane [165] where it is discussed how one can use two embedded error-correcting codes instead of just one. Theorem 6.1.6 and Corollary 6.1.7 are from Honkala [309]. In a similar fashion, we may even use  $s$  embedded error-correcting codes for any  $s$ ; see [309]. The bound  $K(9, 1) \geq 55$  has been proved in Habsieger [269]; Example 6.1.5 is from Struik [630]. For another bound using embedded error-correcting codes, see Janwa [345].

§6.2 The conjecture mentioned at the beginning of the Section is from Cohen, Lobstein and Sloane [165]. The idea of Theorem 6.2.1 and the discussion after it is from Stanton and Kalbfleisch [618]; see also Stanton [615] and Cohen, Lobstein and Sloane [165]. Stanton and Kalbfleisch [618] showed using this method that  $K(8, 1) = 32$ . Theorems 6.2.2, 6.2.4 and 6.2.5 are from Lobstein [449]; see also Cohen, Lobstein and Sloane [165]. Theorem 6.2.6 is from Honkala [312]. The exact values of  $K(n, 1)$  for  $n = 4, 5$  were already determined in Taussky and Todd [635].

§6.3 Theorem 6.3.8 and Corollary 6.3.9 are from S. M. Johnson [354] and van Wee [675]. Our discussion uses the notations of [675]. The researchers in the field have until recently been unaware of the paper by Johnson, which includes many important ideas rediscovered later.

As in [675] we can use the following slightly more general definition of  $r$ -excess, where  $r$  is not necessarily the covering radius of  $C$ : if  $C \subseteq \mathbb{F}^n$  has covering radius  $R$  and  $0 \leq r \leq n$ , then the  $r$ -excess on  $V \subseteq \mathbb{F}^n$  by a code  $C \subseteq \mathbb{F}^n$  is defined by

$$E_C^r(V) = \sum_{\mathbf{c} \in C} |B_r(\mathbf{c}) \cap V| - \left| \bigcup_{\mathbf{c} \in C} B_r(\mathbf{c}) \cap V \right|.$$

When  $r = R$  the two definitions coincide.

Theorem 6.3.11 is from Honkala [320]; see also Habsieger [272]. The formula (6.3.13) is already in van Wee [675]. Theorem 6.3.14 was proved in two steps in van Wee [680] and Honkala [317].

§6.4 Lemmas 6.4.2 and 6.4.3 and Theorem 6.4.4 are from van Wee [675]. The bound resulting from (6.5.12) can already be found in S. M. Johnson [354]. The remark preceding Theorem 6.4.4 is from Hou [333, Lemma 1]; see also Hou [334]. For the proof of Theorem 6.4.5, see Honkala [310] and [312].

§6.5 The inequalities (6.5.1) are from Stanton and Kalbfleisch [617] where it is shown that the bounds  $K(2, 1) = 2$ ,  $K(3, 1) = 2$ ,  $K(4, 1) = 4$ ,  $K(5, 1) = 7$ ,  $K(7, 1) = 16$  already proved in Taussky and Todd [635] are attained by 2, 1, 2, 1, 1 nonequivalent codes. Moreover, they show that  $K(6, 1) = 12$  and give some other lower bounds. See also Stanton [615]. For the uniqueness of the  $(7, 16)1$  code, see already Zaremba [698].

Similar inequalities for arbitrary covering radius have been used in S. M. Johnson [354] and Cohen, Lobstein and Sloane [165].

Lemma 6.5.6 and the pair covering inequality are from S. M. Johnson [354]. They were rediscovered by Zhang [704]. The discussion of induced inequalities is from Zhang [704]. Lemma 6.5.4 is [704, Lemma 2]. Excess on spheres of radius two has also been studied in van Wee [675] and Honkala [312]. Example 6.5.13 is from Zhang [704]. For a more detailed account of how to derive good inequalities, see Zhang [704], Zhang and Lo [705] and Li and Chen [423]. The final part of the section including (6.5.16), Lemma 6.5.20 and Theorem 6.5.22, follows Habsieger [272], where it is also shown that if  $n \equiv 10, 50 \pmod{60}$ , then

$$K(n, 1) \geq \frac{(n+1)(n+2)(n^2+n+2) + 96}{(n+1)(n+2)(n^2+n+2)n} 2^n.$$

Improving on two other results in [272] it is shown in Honkala [321] that when  $n \equiv 5 \pmod{6}$ , then

$$K(n, 1) \geq \frac{(5n^2 - 13n + 66)2^n}{(5n^2 - 13n + 46)(n+1)};$$

and when  $n \equiv 19, 39 \pmod{60}$ , then

$$K(n, 1) \geq \frac{(2V(n, 4) + 5V(n, 3) + 28)2^n}{(2V(n, 4) + 5V(n, 3))(n+1)}.$$

§6.6 For recent tables that extend to  $n \leq 64$  and  $R \leq 12$ , see Östergård and Kaikkonen [526].

§6.7 Example 6.7.1 is from Habsieger [270]. Example 6.7.7 is from Bhandari and Durairajan [78] who use it together with Theorem 6 in Östergård [512] to show that  $K_3(6n, 4n-1) = 6$ .

It is shown in Kalbfleisch and Stanton [358] that every  $(4, 9)_{31}$  code is equivalent to the Hamming code.

The exact bound  $K_3(5, 1) = 27$  is proved in Kamps and van Lint [361]. In Kolev [383] it is shown that the optimal codes are the ones of the form  $(C_0 \oplus \{0\}) \cup (C_1 \oplus \{1\}) \cup (C_2 \oplus \{2\})$  where  $C_0, C_1$  and  $C_2$  are  $(4, 9)_{31}$  codes.

Rodemich [555] has proved that for all  $n \geq 2$ ,

$$K_q(n, 1) \geq \frac{q^{n-1}}{n-1}. \quad (6.8.1)$$

He also showed that

$$K_q(n, n-2) \geq \frac{q^2}{n-1},$$

and that equality can be attained if and only if  $n-1$  divides  $q$  and there are  $n-2$  mutually orthogonal Latin squares of order  $q/(n-1)$ ; cf. the Notes of Chapter 3. For the inequality (6.8.1) in the case  $n-1 < q \leq 2(n-1)$ , see Kalbfleisch and Weiland [360].

The concept of excess immediately generalizes to the nonbinary case. It is known, for example, that

$$K_q(n, 1) \geq \frac{q^n}{n(q-1)} \text{ if } q \text{ and } n \text{ are even;}$$

see S. M. Johnson [354], Chen and Honkala [134] and van Wee [679], where also other similar bounds can be found. For similar bounds on mixed binary/ternary codes, see van Lint, Jr. [440], van Wee [679] and van Lint, Jr. and van Wee [441]. For some lower bounds obtained using linear inequalities, see Lobstein and van Wee [455].

Using the nonbinary generalization of Theorem 2.4.8 and an embedded error-correcting code, Corollary 6.1.4 generalizes to

$$K_q(n, R) \geq \frac{q^n - A_q(n, 2R+1) \binom{2R}{R}}{V_q(n, R) - \binom{2R}{R}}$$

for all  $n \geq 2R$ ; see van Wee [680]. A table of lower and upper bounds on  $A_3(n, d)$  can be found in Vaessens, Aarts and van Lint [659].

Using for instance the ideas discussed in Section 6.2, it is shown in Habsieger [269] that

$$K_q(n, 1) > \lceil \frac{q^n}{V_q(n, 1)} \rceil$$

if  $(q-1)n+1$  does not divide  $q^n$  and  $(q, n) \notin \{(2, 2), (2, 4)\}$ .

For lower bounds on the mixed binary/ternary codes, see also Kolev and Landgev [385] and Kolev [384]. Let  $K_{3,2}(t, b, R)$  denote the minimum cardinality of a code with  $t$  ternary and  $b$  binary coordinates and covering radius  $R$ . In [385] it is shown, for instance, that  $K_{3,2}(1, 2R+1, R) = 6$ ,  $K_{3,2}(2, 2R-1, R) = 4$ ,  $K_{3,2}(2, 2R, R) = 6$ ,  $K_{3,2}(3, 2R-2, R) = 5$  for all  $R \geq 1$ . In [384] it is shown that  $K_{3,2}(4, 2, 1) = 36$ .

Assume that integers  $n, K, \sigma(i)$ ,  $i = 1, 2, \dots, K$ , are given. We ask if there is a code of length  $n$  with  $K$  codewords such that when the  $i$ -th codeword is

surrounded with the sphere of radius  $\sigma(i)$  for each  $i$ , then the spheres together cover the whole space. By studying this more general problem, Blass and Litsyn [84] improve four numerical lower bounds on  $K_3(n, R)$ .

Numerical lower bounds for nonbinary codes have not been studied as extensively as in the binary case — except for the ternary codes when  $R = 1$ . Upper bounds for ternary codes with  $n \leq 13$  and  $R \leq 3$  have been of great interest for a long time in connection with football pools (cf. Chapter 15).

Notice that several upper bounds in the papers that we refer to in Tables 6.2–6.4 are attributed to personal communications etc., and therefore to find who originally discovered each code it is necessary to consult the papers, as we are not reproducing the complete history here. In the same way as in the binary case, we have not made any calculations to see which of the current records should be attributed to S. M. Johnson [354].

# Chapter 7

## Lower bounds for linear codes

In the previous chapter a number of lower bounds on the minimum cardinality  $K(n, R)$  of a binary code of length  $n$  and covering radius  $R$  were discussed. If  $C$  is a binary linear  $[n, k]R$  code, then trivially

$$2^k \geq K(n, R),$$

and to obtain a lower bound on  $k$  we can use any known lower bound on  $K(n, R)$ . However, we can often do better by taking into account the linear structure of the code  $C$ , not just the fact that the cardinality is a power of 2. In this chapter we present different techniques to obtain nonexistence results for binary linear codes.

In the first section we consider excess bounds. In Section 7.2, we give nonexistence results in the case of covering radius two and three, based on restrictions on the weight distributions of the dual codes. We recall that the nonexistence of an  $[n, k]R$  code yields the lower bounds  $t[n, k] \geq R + 1$  and  $\ell(n - k, R) \geq n + 1$ .

At the end of the chapter we present updated tables of lower and upper bounds for  $t[n, k]$ , the minimum covering radius of an  $[n, k]$  code, and for  $\ell(m, R)$ , the smallest possible length  $n$  of an  $[n, n - m]R$  code.

### 7.1 Excess bounds for linear codes

Assume that  $C$  is an  $[n, k]R$  code. We use the notations of Section 6.3.

As in Section 6.4 consider a sphere  $B_1(\mathbf{x})$  and assume that  $\mathbf{x}$  is a deep hole:

$$\mathbf{x} \in A = \{\mathbf{x} \in \mathbb{F}^n : d(\mathbf{x}, C) = R\}.$$

It was shown in Lemma 6.4.2 that

$$E(B_1(\mathbf{x})) \geq \varepsilon := (R+1)\lceil \frac{n+1}{R+1} \rceil - (n+1). \quad (7.1.1)$$

In the linear case we can find an upper bound on the number of vectors  $\mathbf{x}$  for which equality holds.

**Theorem 7.1.2** *Assume that  $C$  is an  $[n, k]R$  code, and  $n+1 = a(R+1) - \varepsilon$ , where  $0 \leq \varepsilon \leq R$ . If  $a$  is odd, then the number of vectors  $\mathbf{x}$  for which  $E(B_1(\mathbf{x})) = \varepsilon$  is at most  $(V(n, \varepsilon) - V(R, \varepsilon) + 1)2^k$ .*

**Proof.** Assume that equality in (7.1.1) holds for  $\mathbf{x}$ . Then every vector in  $B_1(\mathbf{x})$  — with at most  $\varepsilon$  exceptions — is covered by exactly one codeword. The codewords that cover at least one of the words in  $B_1(\mathbf{x})$  form the set  $B_{R+1}(\mathbf{x}) \cap C$  with odd cardinality  $a = \lceil (n+1)/(R+1) \rceil$ . Clearly, a codeword  $\mathbf{c} \in B_{R+1}(\mathbf{x}) \cap C$ , which has distance  $R$  or  $R+1$  to  $\mathbf{x}$ , covers the vector  $\mathbf{x} + \mathbf{e}_i$  if and only if  $\mathbf{c}$  and  $\mathbf{x}$  disagree in the  $i$ -th coordinate. Let  $\mathbf{s} \in C$  be the sum of all codewords in  $B_{R+1}(\mathbf{x}) \cap C$ . When  $\mathbf{c}$  runs through  $B_{R+1}(\mathbf{x}) \cap C$  then for every  $i \in \{1, 2, \dots, n\}$  — with at most  $\varepsilon$  exceptions —  $\mathbf{c}$  and  $\mathbf{x}$  hence disagree only once and agree an even number of times. Consequently,  $s_i = 1 + x_i$  for at least  $n - \varepsilon$  indices  $i$ , i.e.,  $\mathbf{x} + \mathbf{s} \in B_\varepsilon(\mathbf{1})$ . Thus

$$\mathbf{x} \in (B_\varepsilon(\mathbf{1}) + C) \cap A = (B_\varepsilon(\mathbf{1}) \cap A) + C$$

by the linearity of  $C$ , and equality in (7.1.1) holds for at most  $|B_\varepsilon(\mathbf{1}) \cap A| \times |C|$  vectors  $\mathbf{x}$ .

If  $C$  contains  $\mathbf{1}$ , i.e., is a self-complementary code, and  $\varepsilon < R$ , then of course  $|B_\varepsilon(\mathbf{1}) \cap A| = 0$ . In general, let  $\mathbf{c} \in C$  be a codeword that covers  $\mathbf{1}$ . Because  $|B_\varepsilon(\mathbf{1}) \cap B_{R-1}(\mathbf{c})|$  is minimal if  $d(\mathbf{1}, \mathbf{c}) = R$  by Theorem 2.4.8, we get

$$|B_\varepsilon(\mathbf{1}) \cap B_{R-1}(\mathbf{c})| \geq \sum_{0 \leq i < j, i+j \leq \varepsilon} \binom{n-R}{i} \binom{R}{j} \geq V(R, \varepsilon) - 1$$

completing the proof.  $\square$

This theorem leads to improved lower bounds on linear codes; we use the fact that  $E(B_1(\mathbf{x})) > \varepsilon$  implies that  $E(B_1(\mathbf{x})) \geq \varepsilon + R + 1$ , by (6.4.1).

**Corollary 7.1.3** *Assume that there is an  $[n, k, d]R$  code. If  $n+1 = a(R+1) - \varepsilon$  where  $0 \leq \varepsilon \leq R$ , and  $a$  is odd, then*

$$(n + \varepsilon + 2 - \lceil d/2 \rceil)2^{n-k} \leq (n + 1 - R - \lceil d/2 \rceil)V(n, R) + (\varepsilon + R + 1)V(n, R - 1) + (R + 1)(V(n, \varepsilon) - V(R, \varepsilon) + 1).$$

**Proof.** If  $\mathbf{z} \in Z$ , then by the remark following Lemma 6.4.3,

$$|A \cap B_1(\mathbf{z})| \leq n + 1 - R - \lceil d/2 \rceil.$$

Using (6.4.1) we obtain as in the proof of Theorem 6.4.4

$$\begin{aligned} & (\varepsilon + R + 1)(2^n - 2^k V(n, R - 1)) - (V(n, \varepsilon) - V(R, \varepsilon) + 1)2^k(R + 1) \\ & \leq \sum_{\mathbf{x} \in A} E(B_1(\mathbf{x})) \leq (n + 1 - R - \lceil d/2 \rceil)(2^k V(n, R) - 2^n), \end{aligned}$$

from which the claim follows.  $\square$

Notice that if there exists an  $[n, n - m]R$  code  $C$  and  $n \leq 2^m - 1$ , then by Theorem 2.1.9 there also exists an  $[n, n - m]R'$  code  $C'$  for some  $R' \leq R$  with a parity check matrix whose columns are nonzero and distinct. In other words, we know that the minimum distance of  $C'$  is at least three.

Consider now the case  $a$  even.

**Theorem 7.1.4** *Assume that  $C$  is an  $[n, k, d]R$  code,  $n + 1 = a(R + 1) - \varepsilon$ , where  $0 \leq \varepsilon \leq R$ , and  $a$  is even. If furthermore  $\mathbf{1} \notin C$  and  $\varepsilon < d/2$ , or  $\mathbf{1} \in C$  and  $\varepsilon < d$  is odd, then the number of vectors  $\mathbf{x}$  for which  $E(B_1(\mathbf{x})) = \varepsilon$  is at most  $2^k V(n, R) - 2^n$ .*

**Proof.** We proceed as in the proof of Theorem 7.1.2. Assume that  $E(B_1(\mathbf{x})) = \varepsilon$ , and that  $\mathbf{s} \in C$  is the sum of the  $a$  codewords in the set  $B_{R+1}(\mathbf{x}) \cap C$ . The same argument as before shows that  $w(\mathbf{s}) \geq n - \varepsilon$ , and that  $s_i = 1$  if and only if the vector  $\mathbf{x} + \mathbf{e}_i$  is covered by an odd number of codewords.

Assume first that  $\mathbf{1} \in C$  and  $\varepsilon < d$  is odd. Then  $w(\mathbf{s}) \geq n - \varepsilon > n - d$  and consequently  $\mathbf{s} = \mathbf{1}$ . Hence every vector  $\mathbf{x} + \mathbf{e}_i$  is covered an odd number of times, i.e., the excess on each  $\mathbf{x} + \mathbf{e}_i$  is even. On the other hand,  $E(B_1(\mathbf{x})) = \varepsilon$  is odd, implying that  $E(\mathbf{x})$  is odd, and hence  $E(\mathbf{x}) > 0$ . Therefore the number of such vectors  $\mathbf{x}$  is at most  $E(\mathbb{F}^n) = 2^k V(n, R) - 2^n$ .

Assume then that  $\mathbf{1} \notin C$  and  $\varepsilon < d/2$ . Because  $w(\mathbf{s}) \geq n - \varepsilon > n - d/2$ , the codeword  $\mathbf{s}$  does not depend on the choice of  $\mathbf{x}$ . Let  $i$  be an index such that  $s_i = 0$ . Then  $\mathbf{x} + \mathbf{e}_i$  is covered by an even number of codewords, and hence  $E(\mathbf{x} + \mathbf{e}_i) > 0$ . Since  $i$  is fixed, the number of possible choices for  $\mathbf{x}$  is at most  $E(\mathbb{F}^n) = 2^k V(n, R) - 2^n$ .  $\square$

**Corollary 7.1.5** *Assume that there is an  $[n, k, d]R$  code and that  $n + 1 = a(R + 1) - \varepsilon$  where  $0 \leq \varepsilon \leq R$  and  $a$  is even. If furthermore  $\mathbf{1} \notin C$  and  $\varepsilon < d/2$ , or  $\mathbf{1} \in C$  and  $\varepsilon < d$  is odd, then*

$$(n + \varepsilon + R + 3 - \lceil d/2 \rceil)2^{n-k} \leq (n + 2 - \lceil d/2 \rceil)V(n, R) + (\varepsilon + R + 1)V(n, R - 1).$$

$\square$

## 7.2 Linear codes with covering radius two and three

In this section, we study the structure of linear codes with covering radius two or three in connection with their dual codes and establish lower bounds on  $t[n, k]$  and  $\ell(m, R)$ . The main idea is to find strong restrictions on the dual spectrum.

Theorem 7.2.8 makes use of MacWilliams identities (see Theorem 2.2.3). If  $C$  is an  $[n, k]$  code, we let  $\mathcal{B}_0 = 1, \mathcal{B}_1, \dots, \mathcal{B}_n$  and  $\mathcal{B}_0^\perp = 1, \mathcal{B}_1^\perp, \dots, \mathcal{B}_n^\perp$  be the weight distributions of  $C$  and  $C^\perp$ , respectively. Then obviously,

$$2^{n-k} = \sum_{i=0}^n \mathcal{B}_i^\perp. \quad (7.2.1)$$

Now, using MacWilliams transform and (2.3.11), we obtain

$$\mathcal{B}_1 = \frac{1}{2^{n-k}} \sum_{0 \leq i \leq n} \mathcal{B}_i^\perp (n - 2i),$$

i.e.,

$$2^{n-k-1} (n - \mathcal{B}_1) = \sum_{i=0}^n i \mathcal{B}_i^\perp. \quad (7.2.2)$$

Similarly,

$$2^{n-k-2} (n(n-1) - 2(n-1)\mathcal{B}_1 + 2\mathcal{B}_2) = \sum_{i=0}^n i(i-1) \mathcal{B}_i^\perp. \quad (7.2.3)$$

Before stating Theorem 7.2.8, we need three lemmas; the first one is a restatement of the Johnson bound, the following two give conditions on the weights of the dual code.

**Lemma 7.2.4** *If there exists a set  $X$  of vectors of length  $n$  and weight  $w$ , every pair of which have at most  $s$  ones in common, then*

$$|X|(w^2 - ns) \leq n(w - s), \quad (7.2.5)$$

*provided that  $w^2 \geq ns$ .*

**Proof.** Recall that  $A(n, d, w)$  denotes the maximal size of a constant weight code with length  $n$ , minimum distance  $d$  and weight  $w$ . Since  $X$  has minimum distance at least  $2(w - s)$ ,  $|X| \leq A(n, 2(w - s), w)$ . By Theorem 12.6.10,

$$A(n, 2(w - s), w) \leq \frac{2(w - s)n}{2w^2 - 2wn + 2(w - s)n} = \frac{(w - s)n}{w^2 - sn}.$$

□

**Lemma 7.2.6** Let  $C$  be an  $[n, n - m]_2$  code. The nonzero weights  $w$  in  $C^\perp$  satisfy

$$w^2 - (n + 1)w + 2^{m-1} \leq 0.$$

**Proof.** Consider a vector  $\mathbf{c} \in C^\perp$  with weight  $w > 0$  and an  $m \times n$  parity check matrix  $\mathbf{H}$  for  $C$  with the first row equal to  $\mathbf{c}$ . There are  $2^{m-1}$   $m$ -tuples (syndromes) with nonzero first coordinate, and each of these column vectors is a sum of one or two columns of  $\mathbf{H}$ , since  $R(C) = 2$ . This implies that  $w + w(n - w) \geq 2^{m-1}$ .  $\square$

**Lemma 7.2.7** Let  $C$  be an  $[n, n - m]_2$  code. Let  $\mathbf{c}_1$  and  $\mathbf{c}_2$  be two distinct nonzero vectors in  $C^\perp$ , with weights  $w_1$  and  $w_2$ , having  $s$  ones in common. Then

$$2s^2 + (n - 2(w_1 + w_2) + 1)s + w_1w_2 - 2^{m-2} \geq 0.$$

**Proof.** Consider an  $m \times n$  parity check matrix  $\mathbf{H}$  for  $C$  with the first and second rows equal to  $\mathbf{c}_1$  and  $\mathbf{c}_2$ . Without loss of generality, we can assume that

$$\mathbf{H} = \left( \begin{array}{c|c|c|c} \overbrace{w_1 - s}^{\mathbf{11}\dots\mathbf{1}} & \overbrace{s}^{\mathbf{11}\dots\mathbf{1}} & \overbrace{w_2 - s}^{\mathbf{00}\dots\mathbf{0}} & \overbrace{n - w_1 - w_2 + s}^{\mathbf{00}\dots\mathbf{0}} \\ \hline \mathbf{00}\dots\mathbf{0} & \mathbf{11}\dots\mathbf{1} & \mathbf{11}\dots\mathbf{1} & \mathbf{00}\dots\mathbf{0} \\ \hline * & * & * & * \end{array} \right),$$

where  $*$  stands for any binary matrix of suitable size. There are  $2^{m-2}$   $m$ -tuples with the first and second coordinates equal to 1, and each of these column vectors is a sum of one or two columns of  $\mathbf{H}$ . This implies that  $s + s(n - w_1 - w_2 + s) + (w_1 - s)(w_2 - s) \geq 2^{m-2}$ .  $\square$

**Theorem 7.2.8** There is no  $[32, 23]_2$  code.

**Proof.** Assume on the contrary the existence of such a code  $C$ . Note that  $C$  is optimal and that we can assume that it has minimum distance at least three (by modifying  $\mathbf{H}$  if it contains all-zero or identical columns). So  $\mathcal{B}_1 = \mathcal{B}_2 = 0$ . Now (7.2.1), (7.2.2) and (7.2.3) read, respectively:  $2^9 = \sum_{0 \leq i \leq 32} \mathcal{B}_i^\perp$ ,  $2^{13} = \sum_{0 \leq i \leq 32} i\mathcal{B}_i^\perp$  and  $2^{12} \cdot 31 = \sum_{0 \leq i \leq 32} i(i-1)\mathcal{B}_i^\perp$ .

Since  $(i-14)(i-19) = i(i-1) - 32i + 14 \cdot 19$ , we have

$$\sum_{0 \leq i \leq 32} (i-14)(i-19)\mathcal{B}_i^\perp = \sum_{0 \leq i \leq 32} i(i-1)\mathcal{B}_i^\perp - 32 \sum_{0 \leq i \leq 32} i\mathcal{B}_i^\perp +$$

$$\begin{aligned}
& + 14 \cdot 19 \sum_{0 \leq i \leq 32} \mathcal{B}_i^\perp \\
& = 2^{12} \cdot 31 - 32 \cdot 2^{13} + 14 \cdot 19 \cdot 2^9 \\
& = 2^{10}. \tag{7.2.9}
\end{aligned}$$

On the other hand, it follows from Lemma 7.2.6 that the weights  $w$  of  $C^\perp$  satisfy  $w = 0$  or  $13 \leq w \leq 20$ . Therefore  $\sum_{0 \leq i \leq 32} (i-14)(i-19)\mathcal{B}_i^\perp = 14 \cdot 19 + \sum_{13 \leq i \leq 20} (i-14)(i-19)\mathcal{B}_i^\perp \leq 14 \cdot 19 + 6(\mathcal{B}_{13}^\perp + \mathcal{B}_{20}^\perp)$ . We now upperbound  $\mathcal{B}_{13}^\perp$  and  $\mathcal{B}_{20}^\perp$ , in order to contradict (7.2.9). Let  $\mathbf{c}_1$  and  $\mathbf{c}_2$  be two distinct vectors in  $C^\perp$ , with weight 13 and  $s$  ones in common. By Lemma 7.2.7, either  $s \leq 3$  or  $s \geq 7$ . If  $s \geq 7$ , then  $w(\mathbf{c}_1 + \mathbf{c}_2) \leq 12$ ; if  $s \leq 2$ , then  $w(\mathbf{c}_1 + \mathbf{c}_2) \geq 22$ . Hence  $s = 3$ , by the weight distribution of  $C^\perp$ . So  $C^\perp$  contains  $\mathcal{B}_{13}^\perp$  codewords of length 32 and weight 13, every pair of which have exactly three ones in common. By the Johnson bound (7.2.5),  $\mathcal{B}_{13}^\perp \leq 4$ . Similarly,  $\mathcal{B}_{20}^\perp \leq 4$ .  $\square$

More lemmas, some of them restricting the weight distribution in the dual code, are needed for the next nonexistence results.

**Lemma 7.2.10** *If  $C$  is an  $[n, k]$  code with no identically zero coordinate,  $k \geq 1$  and only one nonzero weight  $d$ , then  $2^{k-1}$  divides  $d$ .*

**Proof.** Evaluate in two ways the number  $W$  of ones in the  $2^k \times n$  array representing the codewords. By columns,  $W = n2^{k-1}$ . By rows,  $W = d(2^k - 1)$ . Since  $2^{k-1}$  and  $2^k - 1$  are mutually prime for  $k \geq 1$ ,  $2^{k-1}$  divides  $d$ .  $\square$

**Lemma 7.2.11** *Let  $C_1$  and  $C_2$  be two linear codes with parity check matrices*

$$\mathbf{H}_1 = \left( \begin{array}{c|c} 1 & \mathbf{u} \\ \hline 0 & \\ \vdots & \mathbf{H} \\ 0 & \end{array} \right),$$

$$\mathbf{H}_2 = \left( \begin{array}{c|c} 1 & \bar{\mathbf{u}} \\ \hline 0 & \\ \vdots & \mathbf{H} \\ 0 & \end{array} \right);$$

then these two codes have the same dimension and covering radius.

**Proof.** The two codes are related via  $C_2 = \{(\sum_{1 \leq i \leq n} c_i, c_2, \dots, c_n) : (c_1, c_2, \dots, c_n) \in C_1\}$ . Now  $C_1$  and  $C_2$  have equivalent extended codes and the result follows from Theorem 3.1.3 (see also Example 3.1.4).  $\square$

Let  $\mathbf{A}$  be a binary  $k \times n$  matrix. A set  $S \subseteq \mathbb{F}^k$  is said to *r-cover*  $\mathbb{F}^k$  using  $\mathbf{A}$  if every  $\mathbf{x} \in \mathbb{F}^k$  can be represented as a sum of exactly one element of  $S$  and at most  $r$  columns of  $\mathbf{A}$ , i.e., the set  $\{\mathbf{s} + \mathbf{Ax}^T : \mathbf{s} \in S, \mathbf{x} \in \mathbb{F}^n, w(\mathbf{x}) \leq r\}$  is equal to  $\mathbb{F}^k$ . Note that in Section 3.5 we study the ( $q$ -ary) case of a matrix  $\mathbf{A}$  of full rank.

**Lemma 7.2.12** *If  $S$  r-covers  $\mathbb{F}^k$  using  $\mathbf{A}$ , then the code  $C = \{\mathbf{x} \in \mathbb{F}^n : \mathbf{Ax}^T \in S\}$  has covering radius at most  $r$ . Consequently,  $K(n, r) \leq |S| 2^{n-k}$ .*

**Proof.** Let  $\mathbf{z}$  be an arbitrary vector in  $\mathbb{F}^n$ . Then  $\mathbf{Az}^T \in \mathbb{F}^k$  and we can find a vector  $\mathbf{y} \in \mathbb{F}^n$  of weight at most  $r$  such that  $\mathbf{Az}^T = \mathbf{Ay}^T + \mathbf{s}$  for some  $\mathbf{s} \in S$ . Then  $\mathbf{A}(\mathbf{z}^T + \mathbf{y}^T) \in S$  and hence  $\mathbf{z} + \mathbf{y} \in C$ , with  $d(\mathbf{z}, \mathbf{z} + \mathbf{y}) \leq r$ . This proves that  $R(C) \leq r$ .

If  $\mathbf{A}$  is of full rank, we are done. We suppose that the rank of  $\mathbf{A}$  is  $a < k$ . The fact that  $S$  r-covers  $\mathbb{F}^k$  using  $\mathbf{A}$  still holds if we apply a linear transformation on the elements of  $S$  and on the columns of  $\mathbf{A}$ . Therefore we assume without loss of generality that

$$\mathbf{A} = \begin{pmatrix} \mathbf{A}_1 \\ \mathbf{0} \end{pmatrix},$$

where  $\mathbf{A}_1$  is of full rank  $a$ . For all  $\mathbf{z} \in \mathbb{F}^{k-a}$ , define  $S_{\mathbf{z}} = \{\mathbf{s} \in \mathbb{F}^a : (\mathbf{s}|\mathbf{z}) \in S\}$ . Now  $S_{\mathbf{z}}$  r-covers  $\mathbb{F}^a$  using  $\mathbf{A}_1$ . This implies that  $K(n, r) \leq |S_{\mathbf{z}}| 2^{n-a}$ . But  $|S_{\mathbf{z}}| \leq |S|/2^{k-a}$  for some  $\mathbf{z} \in \mathbb{F}^{k-a}$ , so  $K(n, r) \leq |S| 2^{n-k}$ .  $\square$

**Lemma 7.2.13** *Let  $C_1$  be an  $[n, k]_R$  code whose dual contains a nonzero vector of weight  $w$ . Then there exists an  $[n, k]_R$  code  $C_2$  whose dual contains a vector of weight  $n + 1 - w$ .*

**Proof.** Assume that the first row of a parity check matrix  $\mathbf{H}_1$  for  $C_1$  is of weight  $w > 0$ . The claim follows by Lemma 7.2.11 after suitable row operations on  $\mathbf{H}_1$ .  $\square$

**Lemma 7.2.14** *Let  $C$  be an  $[n, n-m]_2$  code. The nonzero weights  $w$  in  $C^\perp$  satisfy*

$$w 2^{n-w-m+1} \geq K(n-w, 1).$$

**Proof.** Consider a vector  $\mathbf{c} \in C^\perp$  with weight  $w > 0$  and an  $m \times n$  parity check matrix  $\mathbf{H}$  for  $C$  with the first row equal to  $\mathbf{c}$ :

$$\mathbf{H} = \left( \begin{array}{c|c} \overbrace{11 \dots 1}^w & \overbrace{00 \dots 0}^{n-w} \\ \hline \mathbf{H}_1 & \mathbf{H}_0 \end{array} \right).$$

Now the columns of  $\mathbf{H}_1$  1-cover  $\mathbb{F}^{m-1}$  using  $\mathbf{H}_0$ . Our claim follows from Lemma 7.2.12.  $\square$

**Lemma 7.2.15** *Let  $C$  be an  $[n, n-m]_2$  code. Let  $(0^{n-w}, 1^w)$  be a codeword of  $C^\perp$ , with  $w > 0$ . Let  $\mathbf{c} = (\mathbf{c}_1, \mathbf{c}_2)$  be another nonzero codeword in  $C^\perp$ , with  $\mathbf{c}_1 \in \mathbb{F}^{n-w}$  and  $\mathbf{c}_2 \in \mathbb{F}^w$ . Then the quantities  $\alpha := \min\{w(\mathbf{c}_1), n+1-w-w(\mathbf{c}_1)\}$  and  $\beta := \min\{w(\mathbf{c}_2), w-w(\mathbf{c}_2)\}$  satisfy*

$$\frac{2^{m-2} - \alpha w}{n+1-w-2\alpha} \leq \beta \leq \frac{w}{2}$$

whenever  $n+1-w-2\alpha \neq 0$ .

**Proof.** Put the parity check matrix of  $C$  in the form

$$\mathbf{H} = \left( \begin{array}{c|c|c|c} \overbrace{\mathbf{11}\dots\mathbf{1}}^{w(\mathbf{c}_1)} & \overbrace{\mathbf{00}\dots\mathbf{0}}^{n-w-w(\mathbf{c}_1)} & \overbrace{\mathbf{11}\dots\mathbf{1}}^{w(\mathbf{c}_2)} & \overbrace{\mathbf{00}\dots\mathbf{0}}^{w-w(\mathbf{c}_2)} \\ \hline \mathbf{00}\dots\mathbf{0} & \mathbf{00}\dots\mathbf{0} & \mathbf{11}\dots\mathbf{1} & \mathbf{11}\dots\mathbf{1} \\ \hline * & * & * & * \end{array} \right),$$

where  $*$  stands for any binary matrix of suitable size. We may assume without loss of generality that  $w(\mathbf{c}_1) \leq n+1-w-w(\mathbf{c}_1)$  and  $w(\mathbf{c}_2) \leq w-w(\mathbf{c}_2)$ , possibly using Lemma 7.2.11 and adding the second row of  $\mathbf{H}$  to the first one. This means that  $\alpha = w(\mathbf{c}_1)$  and  $\beta = w(\mathbf{c}_2) \leq w/2$ . Now all the syndromes with the first two coordinates equal to one are sums of at most two columns of  $\mathbf{H}$ , so  $\beta + (n-w-\alpha)\beta + \alpha(w-\beta) \geq 2^{m-2}$  and the claim follows.  $\square$

**Theorem 7.2.16** *If  $m \geq 3$ , then  $\ell(2m-1, 2) \geq 2^m + 1$ .*

**Proof.** Assume that  $C$  is an  $[n = 2^m, n-(2m-1)]_2$  code. Let  $\mathbf{c} \in C^\perp$  have weight  $w > 0$ . By Lemma 7.2.6,  $w^2 - (2^m + 1)w + 2^{2m-2} \leq 0$ . In particular, when  $m \geq 3$ ,  $w \neq n$ . By Lemma 7.2.14,  $w2^{n-w-2m+2} \geq K(n-w, 1)$ . If  $w$  is even, then by Theorem 6.3.8

$$w2^{n-w-2m+2} \geq 2^{n-w}/(n-w),$$

which implies  $w(n-w) \geq n^2/4$  and finally  $w = n/2$ . This shows that  $C_e$ , the even weight subcode of  $C^\perp$  (of dimension  $k \geq 2m-2$ ), is a one-weight code with minimum distance  $2^{m-1}$ . Assuming, without loss of generality, that  $C$  has minimum distance at least two, we can apply Lemma 7.2.10 to  $C_e$ :  $2^{k-1}$  divides  $2^{m-1}$ , but this contradicts, for  $m \geq 3$ , the fact that  $k-1 \geq 2m-3 \geq m$ .  $\square$

The case  $m = 5$ , which gives Theorem 7.2.8, is now improved:

**Theorem 7.2.17** *There is no  $[33, 24]_2$  code.*

**Proof.** Assume that  $C$  is a  $[33, 24]_2$  code. By Lemma 7.2.6, the nonzero weights  $w$  in  $C^\perp$  satisfy  $w^2 - 34w + 256 \leq 0$ , i.e.,  $12 \leq w \leq 22$ . If weight 21 occurs, then by Lemma 7.2.14,  $K(12, 1) \leq 336$ , which contradicts  $K(12, 1) \geq 342$  (see Table 6.1). By Lemma 7.2.13, weight 13 does not occur either in  $C^\perp$ . Since the minimum distance of a  $[33, 9]$  code is at most 13 (see, e.g., [96]),  $C^\perp$  has minimum distance 12 and we can assume, by Lemma 7.2.13, that it contains a codeword  $\mathbf{c}$  of weight 22, which we take as the first row for a parity check matrix  $\mathbf{H}$  for  $C$ :

$$\mathbf{H} = \left( \begin{array}{c|c} \overbrace{00 \dots 0}^{11} & \overbrace{11 \dots 1}^{22} \\ \hline \mathbf{H}_0 & \mathbf{H}_1 \end{array} \right).$$

Since  $d(C^\perp) = 12$ , the submatrix  $\mathbf{H}_0$  is of full rank and we can assume that it has the form  $(\mathbf{I}_8 | \mathbf{A})$ . If  $\mathbf{c} = (\mathbf{c}_0 | \mathbf{c}_1) \in C^\perp$ ,  $\mathbf{c}_0 \in \mathbb{F}^{11}$ ,  $\mathbf{c}_1 \in \mathbb{F}^{22}$ , and  $w(\mathbf{c}_0) \leq 3$ , then  $w(\mathbf{c}_1) = 11$  by Lemma 7.2.15. Consequently, three dependent nonzero codewords of  $C^\perp$  can never have all weight three or less in their first 11 coordinates, because the sum of three vectors of weight 11 is odd.

From Lemma 7.2.15 we can also infer that if a row of  $\mathbf{A}$  is repeated, then this row is  $1^3$ . Furthermore, two rows of  $\mathbf{A}$  differ in at least two positions unless one of them is  $1^3$ . This proves that  $1^3$  occurs at least four times in  $\mathbf{A}$  and, without loss of generality, the rows  $\mathbf{c}_1 = (10000000 111)$ ,  $\mathbf{c}_2 = (01000000 111)$  and  $\mathbf{c}_3 = (00100000 111)$  appear in  $\mathbf{H}_0$ . Then the codewords  $\mathbf{c}_1 + \mathbf{c}_2$ ,  $\mathbf{c}_1 + \mathbf{c}_3$  and  $\mathbf{c}_3 + \mathbf{c}_2$  are dependent and have weight two, which is impossible.  $\square$

The same methods can be applied to the case of codes with covering radius three.

**Lemma 7.2.18** *Let  $C$  be an  $[n, n - m]_3$  code. Let  $\mathbf{c}$  be a nonzero vector of weight  $w$  in  $C^\perp$  and  $C_w^\perp$  be a subcode of  $C^\perp$  having zeros on  $\text{supp}(\mathbf{c})$ . The nonzero weights  $a$  in  $C_w^\perp$  satisfy*

$$aw(n + 1 - w - a) \geq 2^{m-2} \quad (7.2.19)$$

and

$$aw2^{n-w-a-m+2} \geq K(n - w - a, 1). \quad (7.2.20)$$

**Proof.** Consider in  $C^\perp$  two vectors of weights  $w$  and  $a$ , without overlap. Take  $\mathbf{H}$  in the form

$$\mathbf{H} = \left( \begin{array}{c|c|c} \overbrace{00 \dots 0}^w & \overbrace{11 \dots 1}^a & \overbrace{00 \dots 0}^{n-w-a} \\ \hline \overbrace{11 \dots 1}^a & \overbrace{00 \dots 0}^w & \overbrace{00 \dots 0}^{n-w-a} \\ \hline \mathbf{H}_1 & \mathbf{H}_2 & \mathbf{H}_3 \end{array} \right).$$

All the syndromes with the first two coordinates equal to one are sums of at most three columns of  $\mathbf{H}$ , so  $aw + aw(n - w - a) \geq 2^{m-2}$ .

The set  $X = \{\mathbf{H}_1\} + \{\mathbf{H}_2\}$ , where  $\{\mathbf{H}_i\}$  denotes the set of columns of  $\mathbf{H}_i$ , 1-covers  $\mathbb{F}^{m-2}$  using  $\mathbf{H}_3$ , so from Lemma 7.2.12 and  $|X| \leq wa$ , we prove the second claim.  $\square$

**Corollary 7.2.21** *Let  $C$  be an  $[n, n - m]_3$  code. The nonzero weights  $w$  in  $C^\perp$  satisfy*

$$w(n + 1 - w)^2 \geq 2^m \text{ or } w \geq m.$$

**Proof.** Maximize the left hand side of (7.2.19) with respect to  $a$ .  $\square$

**Theorem 7.2.22** *There is no  $[37, 24]_3$  code.*

**Proof.** If such a code exists, then by Corollary 7.2.21 its dual code has minimum distance at least 13. But the minimum distance of a  $[37, 13]$  code is at most 12 (see, e.g., [96]), a contradiction.  $\square$

**Theorem 7.2.23** *There is no  $[15, 6]_3$  code.*

**Proof.** If such a code  $C$  exists, then by Corollary 7.2.21 its dual code has minimum distance at least four. But the minimum distance of a  $[15, 9]$  code is at most four (see, e.g., [96]), so there is a vector of weight four in  $C^\perp$ . The maximal subcode  $C_4^\perp$  having zeros on the support of such a vector has dimension at least five. By (7.2.19),  $a(12 - a) \geq 32$ , i.e.,  $4 \leq a \leq 8$ . If weight five occurs, then by (7.2.20),  $K(6, 1) \leq 10$ , which contradicts  $K(6, 1) = 12$  (see Table 6.1). Similarly, if weights 6 or 7 occur, then  $K(5, 1) \leq 6$  or  $K(4, 1) \leq 3$ , a contradiction. So  $C_4^\perp$  is an  $[11, k \geq 5]$  code with weights in  $\{0, 4, 8\}$ , and  $\widehat{C}_4^\perp + \{0^{12}, 1^{12}\}$  is a self-dual  $[12, 6]$  code with weights in  $\{0, 4, 8, 12\}$ . However, such a code does not exist (see Section 2.6).  $\square$

### 7.3 Tables for linear codes

This section is devoted to tables of bounds on  $t[n, k]$  and  $\ell(m, R)$ , preceded by a comment on the respective qualities of the two functions.

In Table 7.1 we give bounds on  $t[n, k]$ , for  $1 \leq n \leq 64$ ,  $1 \leq k \leq n$ ; this choice for the values of  $n$  finds its source in Graham and Sloane [265] (the very first table for  $t[n, k]$ , with  $n \leq 32$ , is due to Cohen, Karpovsky, Mattson and Schatz [156]).

Table 7.4 provides bounds on  $\ell(m, R)$ , for  $1 \leq R \leq 12$  and  $R \leq m \leq 24$ ; tables with these sizes of parameters can be found in Brualdi and Pless [102] and Lobstein and Pless [453].

Table 7.3 gives bounds on  $\ell(m, R)$ , for  $1 \leq R \leq 4$  and  $R \leq m \leq 64$  (with only upper bounds when  $m \geq 25$ ); similar tables can be found in Davydov and Drozhzhina-Labinskaya [189].

Tables 7.3 and 7.4 have a nonempty intersection.

Table 7.2, which gives bounds on  $\ell(m, R)$  when  $\ell(m, R) \leq 64$  and which also has a nonempty intersection with Tables 7.3 and 7.4, requires some explanation. The function  $\ell(m, R)$  seems to give information on the covering radius of binary linear codes in a more compact way than the function  $t[n, k]$ . For instance,  $\ell(6, 1) = 63$ ,  $\ell(6, 2) = 13$  is equivalent to:  $t[12, 6] > 2$ ,  $t[13, 7] = t[14, 8] = t[15, 9] = \dots = t[61, 55] = t[62, 56] = 2$  and  $t[63, 57] = 1$ . Table 7.2, which has 1438 entries, gives the same information as Table 7.1, which contains 2080 entries.

One can even observe that Table 7.2 could be made more compact by restricting it to  $m \geq 2R + 1$  and stating that, for all  $m$ :  $\ell(m, m) = m$  and  $\ell(m, R) = m + 1$  for  $\lceil m/2 \rceil \leq R < m$ . In terms of the function  $t[n, k]$  however, this simply reads, for all  $m$ :  $t[m+1, 1] = \lceil m/2 \rceil$  and  $t[m, 0] = m$ . For instance,  $\ell(63, 32) = \ell(63, 33) = \ell(63, 34) = \dots = \ell(63, 61) = \ell(63, 62) = 64$  and  $\ell(63, 63) = 63$  can be represented by:  $t[64, 1] = 32$  and  $t[63, 0] = 63$ .

This shows a case when the function  $t[n, k]$  gives a more efficient representation than the function  $\ell(m, R)$ . There is no other example of this phenomenon in Tables 7.1 and 7.2, but this can happen for large code lengths, since we know (see [158, Corollary 10.1]) that:

for each integer  $b \geq 1$ , for all  $k$  such that  $\lceil 2^{(k-4)/2} \rceil / (k-1) > b+1$  and for all  $n \geq 2^{k-2}$ , there is at least one value  $t[n, j]$  with  $2 \leq j \leq k$  such that  $t[n-1, j-1] \geq b+1 + t[n, j]$ . For such  $j$ , with  $t_0 := t[n, j]$ ,  $\ell(n-j, t_0) = \ell(n-j, t_0+1) = \dots = \ell(n-j, t_0+b)$ .

Thus, in a table for  $\ell(m, R)$ ,  $b+1$  entries (where  $b$  can be arbitrarily large) are replaced by 2 entries in a table for  $t[n, k]$ , *without loss of information*.

## Key to Table 7.1

unmarked Cohen, Karpovsky, Mattson and Schatz [156] for  $n \leq 32$ ,  
 Graham and Sloane [265] for  $33 \leq n \leq 64$

Lower bounds:

- a from Corollaries 7.1.3 and 7.1.5
- b Theorem 5.2.7
- c Simonis [585]
- d Calderbank and Sloane [114]
- e Hou [331] (some of these results also appeared in [334])
- f Ytrehus [696]
- g Zhang and Lo [706]
- h Example 13.4.4
- n from the nonlinear case (cf. Table 6.1 for  $n \leq 33$   
 and Zhang and Lo [705], [706] for  $34 \leq n \leq 64$ )
- p Brualdi, Pless and Wilson [105]
- r Brualdi and Pless [102]
- t  $t[n, k] \geq t[n + 1, k + 1]$ ,  $t[n, k] \geq t[n, k + 1]$ ,  $t[n, k] \geq t[n - 1, k]$
- v Struik [629] (these results can also be found in [630]  
 and were presented earlier in [626] and [627])
- x Theorem 7.2.8
- y Theorems 7.2.16, 7.2.17 and 7.2.22

Upper bounds:

- A amalgamated direct sum of two normal codes
- B Theorem 5.2.7
- C Theorem 5.2.10
- D Theorem 5.3.4
- E Theorem 5.4.27
- F Theorem 5.4.28
- H Graham and Sloane [265]
- J Davyдов [179]
- P Brualdi, Pless and Wilson [105]
- R Brualdi and Pless [102]
- T  $t[n, k] \leq t[n + 1, k]$ ,  $t[n, k] \leq t[n, k - 1]$  or  $t[n, k] \leq t[n - n', k - k'] + t[n', k']$ , in particular  $n' = 1$ ,  $k' = 1$
- U Dougherty and Janwa [209]
- V Struik [630]
- W Östergård and Kaikkonen [526]

Table 7.1: Bounds on  $t[n, k]$ , Part I.

Table 7.1: Bounds on  $t[n, k]$ , Part II.

Table 7.1: Bounds on  $t[n, k]$ , Part III.

Table 7.1: Bounds on  $t[n, k]$ , Part IV.

$k \setminus n$	38	39	40	41	42	43	44	45	46
1	19	19	20	20	21	21	22	22	23
2	18	19	19	20	20	21	21	22	22
3	18	18	19	19	20	20	21	21	22
4	17	17	18	18	19	19	20	20	21
5	16	17	17	18	18	19	19	20	20
6	e13-15	13-15	a14-16	14-16	14-17	n15-17	15-18	a16-18	16-19
7	12-14	12-15	n13-15	13-16	n14-16	14-17	14-17	n15-18	15-18
8	11-14	n12-14	12-15	12-15	n13-16	13-16	g14-17	14-17	14-18
9	10-13	11-13	11-14	n12-14	12-15	12-15	13-16	13-16	g14-17
10	10-12	10-13	e11-13	11-14	11-14	12-15	12-15	12-16	13-16
11	9-11	n10-11	10-12	10-12	11-13	11-13	11-14	12-14	12-15
12	9-10	9-11	9-11	10-12	10-12	10-13	11-13	11-14	a12-14
13	8-10	n9-10	9-11	9-11	n10-12	10-12	10-13	n11-13	11-14
14	8-9	8-9	8-10	9-10	9-11	9-11	10-12	10-12	a11-13
15	7-8	a8-9	8-9	8-10	a9-10	9-11	9-11	n10-12	10-12
16	7-8	7-8	7-9	8-9	8-10	8-10	9-10	9-11	9-11
17	6-7	7-8	7-8	7-8	8-9	8-9	8-10	n9-10	9-11
18	6-7	6-7	a7-8	7-8	7-8	7-9	8-9	8-10	8-10
19	a6	6-7	6-7	6-7A	7-8	7-8	7-9	8-9	8-10
20	5-6	5-6	6A	6-7	6-7	7-8	7-8	7-9	8-9
21	5	5-6	5-6	6	6-7	6-7	7-8	7-8	7-8A
22	4-5	5	5-6	5-6	6	6-7	6-7	a7A	7-8
23	4	4-5	5	5	5-6	n6	6	6	6-7
24	4	4	4-5	5	5	5-6	5-6	6	6
25	3-4	4	4	4-5	5	5	5-6	5-6	6
26	3V	3-4	4	4	4-5	a5	5	5-6	5-6
27	3	3T	3-4	4	4	4-5	4-5	5	5-6
28	3	3	3T	3-4	4	4	4-5	4-5	5
29	2-3	3	3	3T	3-4	4	4	4-5	4-5
30	2	2E	3	3	3	3-4	4	4	4-5
31	2	2	2T	3	3	3	3-4	4	4
32	2	2	2	2R	3	3	3	3-4	4
33	1	2	2	2	2P	3	3	3	3-4
34	1	1	2	2	2	2T	3	3	3

Table 7.1: Bounds on  $t[n, k]$ , Part V.

$k \setminus n$	38	39	40	41	42	43	44	45	46
35	1	1	1	2	2	2	2	p3	3
36	1	1	1	1	2	2	2	2	a3
37	1	1	1	1	1	2	2	2	2
38	0	1	1	1	1	1	2	2	2
39		0	1	1	1	1	1	2	2
40			0	1	1	1	1	1	2
41				0	1	1	1	1	1
42					0	1	1	1	1
43						0	1	1	1
44							0	1	1
45								0	1
46									0

Table 7.1: Bounds on  $t[n, k]$ , Part VI.

$k \setminus n$	47	48	49	50	51	52	53	54	55
1	23	24	24	25	25	26	26	27	27
2	23	23	24	24	25	25	26	26	27
3	22	23	23	24	24	25	25	26	26
4	21	22	22	23	23	24	24	25	25
5	21	21	22	22	23	23	24	24	25
6	a17-19	17-20	17-20	g18-21	18-21	n19-22	19-22	a20-23	20-23
7	e16-19	16-19	16-20	17-20	17-21	a18-21	18-22	a19-22	19-23
8	n15-18	15-19	n16-19	16-20	16-20	17-21	17-21	g18-22	18-22
9	14-17	14-18	15-18	15-19	n16-19	16-20	16-20	17-21	17-21
10	13-17	n14-17	14-18	14-18	15-19	15-19	n16-20	16-20	16-21
11	n13-15	13-16	13-16	14-17	14-17	g15-18	15-18	15-19	n16-19
12	12-15	12-15	13-16	13-16	13-17	14-17	14-18	n15-18	15-19
13	11-14	12-15	12-15	g13-16	13-16	13-17	n14-17	14-18	14-18
14	11-13	11-14	n12-14	12-15	12-15	n13-16	13-16	13-17	14-17
15	10-13	n11-13	11-14	11-14	12-15	12-15	12-16	13-16	13-17
16	10-12	10-12	a11-12	11-13	11-13	n12-14	12-14	12-15	n13-15
17	9-11	10-12	10-12	10-12	11-13	11-13	11-14	12-14	12-15
18	9-11	9-11	9-11A	10-12	10-12	a11-13	11-13	11-14	n12-14
19	8-10	9-10A	9-11	9-11	10-12	10-12	10-13	11-13	11-13
20	8-9	8-10	n9-10	9-11	9-11	n10-12	10-12	10-12A	n11-13

Table 7.1: Bounds on  $t[n, k]$ , Part VII.

Table 7.1: Bounds on  $t[n, k]$ , Part VIII.

$k \setminus n$	56	57	58	59	60	61	62	63	64
1	28	28	29	29	30	30	31	31	32
2	27	28	28	29	29	30	30	31	31
3	27	27	28	28	29	29	30	30	31
4	26	26	27	27	28	28	29	29	30
5	25	26	26	27	27	28	28	29	29
6	20-24	g21-24	21-25	n22-25	22-26	a23-26	23-27	23-27	a24-28
7	19-23	n20-24	20-24	n21-25	21-25	21-26	22-26	22-27	a23-27
8	18-23	19-23	19-24	e20-24	20-25	20-25	21-26	21-26	a22-27
9	n18-22	18-22	18-23	19-23	19-24	n20-24	20-25	20-25	21-26
10	17-21	17-22	n18-22	18-23	18-23	19-24	19-24	n20-25	20-25
11	16-20	16-20	17-21	17-21	n18-22	18-22	18-23	19-23	19-24
12	15-19	16-20	16-20	n17-21	17-21	17-22	n18-22	18-23	18-23
13	15-19	15-19	15-20	16-20	16-21	n17-21	17-22	17-22	18-23
14	14-18	14-18	15-19	15-19	e16-20	16-20	16-21	17-21	17-22
15	n14-17	14-18	14-18	n15-19	15-19	15-20	16-20	16-21	16-21
16	13-16	13-16	14-17	14-17	14-18	15-18	15-19	n16-19	16-20
17	12-15	13-16	13-16	a14-17	14-17	14-18	n15-18	15-19	15-19
18	12-15	12-15	n13-16	13-16	13-17	n14-17	14-18	14-18	15-19
19	11-14	12-14	12-15	12-15	13-16	13-16	a14-17	14-17	14-18
20	11-13	11-14	a12-14	12-15	12-15	n13-16	13-16	13-17	14-17
21	10-13	11-13	11-14	11-14	12-14	12-14	12-15	13-15	13-16
22	10-12	10-12	11-13	11-13	11-14	12-14	12-14	12-15	13-15
23	n10-11	10-12	10-12	n11-13	11-13	11-14	n12-14	12-14	12-15
24	9-11	9-11	10-12	10-12	10-13	11-13	11-14	11-14	12-14
25	9-10	9-11	9-11	10-11	10-12	10-12	11-13	11-13	11-14
26	8-10	9-10	9-11	9-11	n10-11	10-12	10-12	n11-13	11-13
27	8-9	8-10	n9-10	9-11	9-11	a10-11	10-12	10-12	10-13
28	n8-9	8-9	8-9	8-10	9-10	9-11	9-11	10-11	10-12
29	7-8	7-8	8-9	8-9	8-10	9-10	9-11	9-11	10-11
30	7-8	7-8	7-8	8-9	8-9	8-10	9-10	9-10A	9-11
31	n7	7-8	7-8	7-8	8-9	8-9	8-9A	n9-10	9-10
32	6-7	6-7	7-8	7-8	7-8	8-9	8-9	8-9	8-10
33	6-7	6-7	6-7	7	7-8	7-8	a8-9	8-9	8-9
34	n6	6-7	6-7	6-7	7	7-8	7-8	7-8	8-9
35	5-6	5-6	6-7	6-7	6-7	7	7-8	7-8	7-8
36	5-6	5-6	5-6	6A	6-7	6-7	a7	7-8	7-8

Table 7.1: Bounds on  $t[n, k]$ , Part IX.

## Key to Tables 7.2, 7.3 and 7.4

In Table 7.3, only upper bounds are given  
for  $m \geq 25$  and  $R \geq 2$

- \* in Table 7.2, stands for an entry greater than 64
- unmarked from Hamming codes (for  $R = 1$ ) or from Table 7.1

## Lower bounds:

- a from Corollaries 7.1.3 and 7.1.5
- s sphere-covering bound
- v Struik [629] (these results can also be found in [630] and were presented earlier in [626] and [627])
- y Theorem 7.2.16

## Upper bounds:

- A amalgamated direct sum of two normal codes
- E Theorem 5.4.27
- F Theorem 5.4.28
- G Theorem 5.4.29
- K Davydov and Drozhzhina-Labinskaya [186], [189]
- L [187], [189]
- M [188], [189]
- N [189]

Table 7.2: Bounds on  $\ell(m, R)$ , Part I.

$m \setminus R$	0	1	2	3	4	5	6	7	8	9	10
0	0										
1	*	1									
2	3		2								
3	7	4		3							
4	15	5	5	4							
5	31	9	6	6	5						
6	63	13	7	7	7	6					
7	*	19	11	8	8	8	7				
8	25-26	14	9	9	9	9	9	8			
9	34-39	17-18	13	10	10	10	10	9			
10	47-53	21-22	16	11	11	11	11	11	11	10	
11	*	23	17-19	15	12	12	12	12	12	12	
12	31-37	19-23	18	13	13	13	13	13	13	13	
13	38-53	23-25	19	17	14	14	14	14	14	14	
14	47-63	27-29	21-24	20	15	15	15	15	15	15	
15	60-*	32-37	23-27	21	19	16	16	16	16	16	
16	*	37-49	27-31	22-25	22	17	17	17	17	17	
17		44-62	30-35	24-29	23	21	18	18	18		
18		53-*	34-41	27-33	24-27	24	19	19	19		
19		62-*	39-47	30-36	25-30	25	23	23	20		
20		*	44-59	33-40	28-31	26-29	26	26	21		
21			51-*	37-44	30-38	27-32	27	27	25		
22			57-*	41-45	33-41	29-33	28-31	28			
23			*	46-59	37-45	31-37	29-34	29			
24				51-*	40-47	34-41	30-35	30-33			
25				57-*	43-51	37-48	32-39	31-36			
26				63-*	48-59	40-49	35-43	32-37			
27				*	53-*	43-53	37-47	34-41			
28					57-*	46-57	40-51	36-44			
29					63-*	50-63	43-55	38-48			
30					*	55-*	46-58	41-52			
31						59-*	49-62	43-53			
32						64-*	53-*	47-60			
33						*	57-*	50-64			
34							62-*	53-*			
35							*	56-*			
36								60-*			
37								64-*			
38								*			

Table 7.2: Bounds on  $\ell(m, R)$ , Part II.

$m \setminus R$	11	12	13	14	15	16	17	18
11	11							
12	13	12						
13	14	14	13					
14	15	15	15	14				
15	16	16	16	16	15			
16	17	17	17	17	17	16		
17	18	18	18	18	18	18	17	
18	19	19	19	19	19	19	19	18
19	20	20	20	20	20	20	20	20
20	21	21	21	21	21	21	21	21
21	22	22	22	22	22	22	22	22
22	23	23	23	23	23	23	23	23
23	27	24	24	24	24	24	24	24
24	30	25	25	25	25	25	25	25
25	31	29	26	26	26	26	26	26
26	32–35	32	27	27	27	27	27	27
27	33–38	33	31	28	28	28	28	28
28	34–39	34–37	34	29	29	29	29	29
29	35–43	35–40	35	33	30	30	30	30
30	37–46	36–41	36–39	36	31	31	31	31
31	40–50	37–45	37–42	37	35	32	32	32
32	42–54	39–48	38–43	38–41	38	33	33	33
33	44–55	41–49	39–47	39–44	39	37	34	34
34	47–59	43–56	41–50	40–45	40–43	40	35	35
35	50–63	45–57	43–51	41–49	41–46	41	39	36
36	53–*	48–61	45–55	42–52	42–47	42–45	42	37
37	56–*	51–*	47–59	44–53	43–51	43–48	43	41
38	59–*	53–*	49–63	46–57	44–54	44–49	44–47	44
39	63–*	56–*	51–*	48–60	46–55	45–53	45–50	45
40	*	59–*	54–*	50–61	48–59	46–56	46–51	46–49
41		62–*	57–*	53–*	50–62	48–57	47–55	47–52
42		*	60–*	55–*	52–63	49–61	48–58	48–53

Table 7.2: Bounds on  $\ell(m, R)$ , Part III.

Table 7.2: Bounds on  $\ell(m, R)$ , Part IV.

$m \setminus R$	19	20	21	22	23	24	25	26	27	28
19	19									
20	21	20								
21	22	22	21							
22	23	23	23	22						
23	24	24	24	24	23					
24	25	25	25	25	25	24				
25	26	26	26	26	26	26	25			
26	27	27	27	27	27	27	27	26		
27	28	28	28	28	28	28	28	28	27	
28	29	29	29	29	29	29	29	29	29	28
29	30	30	30	30	30	30	30	30	30	30
30	31	31	31	31	31	31	31	31	31	31
31	32	32	32	32	32	32	32	32	32	32
32	33	33	33	33	33	33	33	33	33	33
33	34	34	34	34	34	34	34	34	34	34
34	35	35	35	35	35	35	35	35	35	35
35	36	36	36	36	36	36	36	36	36	36
36	37	37	37	37	37	37	37	37	37	37
37	38	38	38	38	38	38	38	38	38	38
38	39	39	39	39	39	39	39	39	39	39
39	43	40	40	40	40	40	40	40	40	40
40	46	41	41	41	41	41	41	41	41	41
41	47	45	42	42	42	42	42	42	42	42
42	48–51	48	43	43	43	43	43	43	43	43
43	49–54	49	47	44	44	44	44	44	44	44
44	50–55	50–53	50	45	45	45	45	45	45	45
45	51–59	51–56	51	49	46	46	46	46	46	46
46	52–62	52–57	52–55	52	47	47	47	47	47	47
47	53–63	53–61	53–58	53	51	48	48	48	48	48
48	55–*	54–64	54–59	54–57	54	49	49	49	49	49
49	56–*	55–*	55–63	55–60	55	53	50	50	50	50
50	58–*	56–*	56–*	56–61	56–59	56	51	51	51	51

Table 7.2: Bounds on  $\ell(m, R)$ , Part V.

$m \setminus R$	19	20	21	22	23	24	25	26	27	28
51	60-*	58-*	57-*	57-*	57-62	57	55	52	52	52
52	62-*	60-*	58-*	58-*	58-63	58-61	58	53	53	53
53	64-*	61-*	60-*	59-*	59-*	59-64	59	57	54	54
54	*-	63-*	61-*	60-*	60-*	60-*	60-63	60	55	55
55		*-	63-*	62-*	61-*	61-*	61-*	61	59	56
56			*-	63-*	62-*	62-*	62-*	62-*	62	57
57				*-	63-*	63-*	63-*	63-*	63	61
58					*-	64-*	64-*	64-*	64-*	64
59						*-	*-	*-	*-	*-

Table 7.2: Bounds on  $\ell(m, R)$ , Part VI.

Table 7.2: Bounds on  $\ell(m, R)$ , Part VII.

Table 7.3: Bounds on  $\ell(m, R)$ , Part I.

$m \setminus R$	1	2	3	4
1	1			
2	3	2		
3	7	4	3	
4	15	5	5	4
5	31	9	6	6
6	63	13	7	7
7	127	19	11	8
8	255	25-26	14	9
9	511	34-39	17-18	13
10	1023	47-53	21-22	16
11	2047	65-79E	23	17-19
12	4095	a92-107E	31-37	19-23
13	8191	y129-159E	38-53	23-25
14	$2^{14} - 1$	v182-215E	47-63	27-29
15	$2^{15} - 1$	y257-319E	60-75L	32-37
16	$2^{16} - 1$	v363-431E	a75-95L	37-49
17	$2^{17} - 1$	y513-639E	s93-126L	44-62
18	$2^{18} - 1$	v725-863E	s117-153F	53-77A
19	$2^{19} - 1$	y1025-1279E	a148-205L	62-84M
20	$2^{20} - 1$	v1449-1727E	a187-255F	a73-93G
21	$2^{21} - 1$	y2049-2559E	a235-308F	a86-125M
22	$2^{22} - 1$	v2897-3455E	a295-383F	a103-150M
23	$2^{23} - 1$	y4097-5119E	a371-511F	a122-174K
24	$2^{24} - 1$	v5794-6911E	a467-618F	a144-190K
25	$2^{25} - 1$	-10239E	-767F	-238K
26	$2^{26} - 1$	-13823E	-820F	-301N
27	$2^{27} - 1$	-20479E	-1215F	-349N
28	$2^{28} - 1$	-27647E	-1535F	-381N
29	$2^{29} - 1$	-40959E	-1642F	-477N
30	$2^{30} - 1$	-55295E	-2431F	-605N
31	$2^{31} - 1$	-81919E	-3071F	-701N
32	$2^{32} - 1$	-110,591E	-3286F	-765N

Table 7.3: Bounds on  $\ell(m, R)$ , Part II.

$m \setminus R$	1	2	3	4
33	$2^{33} - 1$	-163,839E	-4863F	-894G
34	$2^{34} - 1$	-221,183E	-6143F	-990G
35	$2^{35} - 1$	-327,679E	-6574F	-1246G
36	$2^{36} - 1$	-442,367E	-9727F	-1533N
37	$2^{37} - 1$	-655,359E	-12287F	-1790G
38	$2^{38} - 1$	-884,735E	-13150F	-1982G
39	$2^{39} - 1$	-1,310,719E	-19455F	-2494K
40	$2^{40} - 1$	-1,769,471E	-24575F	-3038N
41	$2^{41} - 1$	-2,621,439E	-26271F	-3581G
42	$2^{42} - 1$	-3,538,943E	-38911F	-3965G
43	$2^{43} - 1$	-5,242,879E	-49151F	-4989G
44	$2^{44} - 1$	-7,077,887E	-52543F	-6015G
45	$2^{45} - 1$	-10,485,759E	-77823F	-7165G
46	$2^{46} - 1$	-14,155,775E	-98303F	-7933G
47	$2^{47} - 1$	-20,971,519E	-105,087F	-9981G
48	$2^{48} - 1$	-28,311,551E	-155,647F	-12031G
49	$2^{49} - 1$	-41,943,039E	-196,607F	-14333G
50	$2^{50} - 1$	-56,623,103E	-210,175F	-15869G
51	$2^{51} - 1$	-83,886,079E	-311,295F	-19965G
52	$2^{52} - 1$	-113,246,207E	-393,215F	-24063G
53	$2^{53} - 1$	-167,772,159E	-420,351F	-28669G
54	$2^{54} - 1$	-226,492,415E	-622,591F	-31741G
55	$2^{55} - 1$	-335,544,319E	-786,431F	-39933G
56	$2^{56} - 1$	-452,984,831E	-840,703F	-48127G
57	$2^{57} - 1$	-671,088,639E	-1,245,183F	-57341G
58	$2^{58} - 1$	-905,969,663E	-1,572,863F	-63485G
59	$2^{59} - 1$	-1,342,177,279E	-1,681,407F	-79869G
60	$2^{60} - 1$	-1,811,939,327E	-2,490,367F	-96255G
61	$2^{61} - 1$	-2,684,354,559E	-3,145,727F	-114,559G
62	$2^{62} - 1$	-3,623,878,655E	-3,362,815F	-126,847G
63	$2^{63} - 1$	-5,368,709,119E	-4,980,735F	-159,615G
64	$2^{64} - 1$	-7,247,757,311E	-6,291,455F	-192,511G

Table 7.4: Bounds on  $\ell(m, R)$ , Part I.

$m \setminus R$	2	3	4	5	6	7	8
2	2						
3		4	3				
4		5	5	4			
5		9	6	6	5		
6		13	7	7	7	6	
7		19	11	8	8	8	7
8		25–26	14	9	9	9	9
9		34–39	17–18	13	10	10	10
10		47–53	21–22	16	11	11	11
11		65–79E	23	17–19	15	12	12
12		a92–107E	31–37	19–23	18	13	13
13		y129–159E	38–53	23–25	19	17	14
14		v182–215E	47–63	27–29	21–24	20	15
15		y257–319E	60–75L	32–37	23–27	21	19
16		v363–431E	a75–95L	37–49	27–31	22–25	22
17		y513–639E	s93–126L	44–62	30–35	24–29	23
18		v725–863E	s117–153F	53–77A	34–41	27–33	24–27
19		y1025–1279E	a148–205L	62–84M	39–47	30–36	25–30
20		v1449–1727E	a187–255F	a73–93G	44–59	33–40	28–31
21		y2049–2559E	a235–308F	a86–125M	51–75A	37–44	30–38
22		v2897–3455E	a295–383F	a103–150M	57–88A	41–45	33–41
23		y4097–5119E	a371–511F	a122–174K	65–98A	46–59	37–45
24		v5794–6911E	a467–618F	a144–190K	a76–107A	51–73A	40–47

Table 7.4: Bounds on  $\ell(m, R)$ , Part II.

$m \setminus R$	9	10	11	12
9	9			
10		11	10	
11		12	12	11
12		13	13	13 12
13		14	14	14 14
14		15	15	15 15
15		16	16	16 16
16		17	17	17 17
17		18	18	18 18
18		19	19	19 19
19		23	20	20 20
20		26	21	21 21
21		27	25	22 22
22		28–31	28	23 23
23		29–34	29	27 24
24		30–35	30–33	30 25

## 7.4 Notes

**§7.1** The approach is due to Hou [333]; see also [334]. The general case is from Struik [628]; see also Struik [630].

**§7.2** Lemma 7.2.4 can be found in S. M. Johnson [353]. Lemmas 7.2.6 and 7.2.7, as well as Theorem 7.2.8, are by Brualdi, Pless and Wilson [105], who also prove  $t[45, 35] > 2$ . Lemma 7.2.10 can be found in MacDonald [461], Lemmas 7.2.13, 7.2.14, 7.2.15 and 7.2.18 in Struik [629], together with Lemma 7.2.11 which is based on an idea by Brualdi and Pless [102].

The result  $\ell(2m-1, 2) \geq 2^m + 1$  for all  $m \geq 3$  was conjectured in [105] and proved in [629]. The case  $m = 6$  gives the nonexistence of a  $[64, 53]_2$  code, first proved by Brualdi and Pless [102] (see also Ytrehus [696]). Theorem 7.2.17 is due to Struik [629], as well as more results of this type. Theorems 7.2.22 and 7.2.23 are also in [629], but the nonexistence of a  $[15, 6]_3$  code was first proved by Simonis [585] and that of a  $[37, 24]_3$  code by Zhang and Lo [706]. We gave here the proofs from [629] because of their simplicity (note however that the nonexistence of a  $[15, 6]_3$  code is also a direct consequence of the pair covering inequality, see Section 6.5). On the other hand, the improvement  $\ell(9, 3) \geq 17$  requires a long proof in [629].

The first proof of the nonexistence of a  $[12, 6]_2$  code involved a computer search. The inequality  $t[18, 11] > 2$  was first established by Ytrehus [696], also with the help of a computer. Now the method described in the proofs of Theorems 7.2.16 and 7.2.17 can be adapted to provide alternative proofs, see [629].

For nonbinary linear codes, see, e.g., Baicheva [37], [38], [39], Baicheva and Velikova [40], [41], K. N. Manev and Velikova [466], Velikova [670].

**§7.3** The proofs of two upper bounds mentioned in Brualdi and Pless [102] ( $\ell(16, 5) \leq 30$  and  $\ell(23, 7) \leq 45$ ) could not be reproduced.

This Page Intentionally Left Blank

# Chapter 8

## Upper bounds

In this chapter we discuss upper bounds on covering radius in binary space. There is an essential difference between the two notions: upper bounds on the minimal covering radius, which are given by constructions of codes having a relatively small number of words, and upper bounds on the maximal covering radius, which in a sense correspond to the worst case — a code having maximal possible covering radius among all codes of given size. To make the problem nontrivial, we should impose some restrictions on the code structure. For instance, we may require the code to be linear, to have a prescribed minimum distance, to have some spectral components bounded, etc. We address the following questions:

- What is the maximal possible covering radius among the codes of given size?
- What is the maximal possible covering radius of a linear code of given size and minimum distance?
- What can be said about covering radii of subcodes or supercodes of a code?
- What is the maximal possible covering radius of a code of given dual distance?
- What is the maximal possible covering radius of a code with a given distance distribution?

These values prove useful in bounding covering radii of several classes of error-correcting codes (see Chapters 9 and 10) and estimating the efficiency of writing on memories (see Chapter 17). Besides, the problem is (at least for the authors) of evident interest in its own right. Furthermore, given a code, estimating its covering radius is apparently an intractable problem (see Section 20.2). On the other hand, some other parameters are easier to calculate and sometimes give a reasonably good estimate of the covering radius.

The chapter is organized as follows. In Section 8.1 we obtain bounds on the

covering radius as a function of the size and minimum distance. In Section 8.2 we estimate the covering radius of subcodes of a code. In particular, we present the *supercode lemma*, a useful tool in lowerbounding the covering radius of some codes. We discuss in Section 8.3 relations between the covering radius and the dual spectrum. We develop a general approach based on the MacWilliams transform. As particular cases, we get the Delsarte bound (the covering radius is upperbounded by the number of nonzero elements in the dual spectrum) and the Norse bounds.

## 8.1 Codes with given size and minimum distance

Given  $K$  and  $n$ , what is the *maximal covering radius*  $T(n, K)$  of an  $(n, K)$  code? If we put no restrictions on the structure of a code with covering radius  $R$ , the strategy is quite clear: placing a deep hole on the all-one vector restricts codewords to having weight at most  $n - R$ . Their number thus cannot exceed  $V(n, n - R)$ , so  $T(n, K)$  is upperbounded by the largest number  $j$  such that  $V(n, n - j) \geq K$ . This upper bound is obviously attained.

**Theorem 8.1.1** *If  $j$  is the largest number such that  $V(n, n - j) \geq K$ , then  $T(n, K) = j$ .*  $\square$

Let us further fix the minimum distance  $d$ , and denote by  $T(n, K, d)$  the maximal covering radius of an  $(n, K, d)$  code.

**Theorem 8.1.2** *Let  $A(n, d, B_i)$  be the maximal size of a code of length  $n$ , minimum distance  $d$  whose codewords belong to  $B_i(\mathbf{0})$ , and  $j$  be the largest number such that  $A(n, d, B_{n-j}) \geq K$ . Then*

$$T(n, K, d) = j.$$

**Proof.** Let  $C$  be an  $(n, K, d)$  code. Without loss of generality, the all-one vector is a deep hole. Then all the codewords lie in the sphere  $B_{n-R}(\mathbf{0})$ . Therefore, the cardinality of the code does not exceed  $A(n, d, B_{n-R})$ , and  $R \leq j$ , where  $j$  is as above.

Conversely, now assume that  $C$  consists of any  $K$  codewords of a code realizing  $A(n, d, B_{n-j})$ . The covering radius of  $C$  is thus at least  $j$ . In fact, it cannot be larger. Indeed, assume that  $R(C) > j$  and  $d(\mathbf{x}, C) = R(C)$ . Hence  $\mathbf{1}$  is a deep hole (at distance  $R(C)$ ) of  $C' = C + \mathbf{x} + \mathbf{1}$ . Thus all the  $K$  codewords of  $C'$  belong to  $B_{n-R(C)}$ , contradicting the maximality of  $j$ .  $\square$

If the code is linear, then its codewords cannot occupy densely a small region of the space, so the maximal covering radius might be less than in the unrestricted case. The redundancy bound presented in the following theorem gives the exact value of  $T[n, k]$ , the maximal covering radius of an  $[n, k]$  code.

**Theorem 8.1.3**

$$T[n, k] = n - k.$$

**Proof.** Let  $\mathbf{H} = (\mathbf{I}_{n-k}, \mathbf{P})$  be a parity check matrix of an  $[n, k]R$  code  $C$ . Using the first  $n - k$  columns, we see that any syndrome can be written as a sum of at most  $n - k$  columns of  $\mathbf{H}$ . Therefore  $R \leq n - k$  by Theorem 2.1.9.

Conversely, taking  $\mathbf{P} = \mathbf{0}$ , we see that  $R = n - k$ , and we are done.  $\square$

**Corollary 8.1.4 (Redundancy bound)** *For every  $[n, k]R$  code,  $R \leq n - k$ .*

$\square$

Knowledge of the structure of the parity check matrix can improve on the redundancy bound. Let  $\mathbf{H} = (\mathbf{I}_{n-k}, \mathbf{P})$  be a parity check matrix of a linear code  $C$ .

**Theorem 8.1.5** *If  $j$  is the maximal weight of a column in  $\mathbf{P}$ , then*

$$R(C) \leq \lceil j/2 \rceil + (n - k - j).$$

**Proof.** Without loss of generality, the code has parity check matrix

$$\mathbf{H} = \left( \begin{array}{c|c|c} & 1 & | & | & * \\ & 1 & | & | & * \\ \mathbf{I}_j & : & | & | & * \\ \hline 0 & 1 & | & * & \mathbf{I}_{n-k-j} \end{array} \right).$$

Denote by  $\mathbf{H}_1$  the  $j \times (j + 1)$  block in the upper left hand corner. Let  $\mathbf{s} = (s_1, s_2)^T$  be arbitrary, where  $s_1 \in \mathbb{F}^j$  and  $s_2 \in \mathbb{F}^{n-k-j}$ . The claim is clear, because every column in  $\mathbb{F}^{n-k-j}$  is a sum of at most  $n - k - j$  columns of  $\mathbf{I}_{n-k-j}$ , and every column in  $\mathbb{F}^j$  is a sum of at most  $\lceil j/2 \rceil$  columns of  $\mathbf{H}_1$ , a parity check matrix of the binary repetition code of length  $j + 1$ .  $\square$

Let us now relate the covering radius of a code to parameters of some codes associated to it.

Let  $\mathbf{H} = (\mathbf{I}_{n-k}, \mathbf{P})$  be a parity check matrix of an  $[n, k]$  code  $C$ , with  $\mathbf{P}$  of rank  $j$ . Let  $C_1$  be the  $[k, k - j]$  code defined by the parity check matrix  $\mathbf{P}$ . Define  $C_2$  as the  $[n - k, j]$  code spanned by the columns of  $\mathbf{P}$ .

**Theorem 8.1.6**

$$R(C) \leq R(C_1) + R(C_2).$$

**Proof.** If  $\mathbf{s}$  is any  $(n - k)$ -tuple, it is at distance at most  $R(C_2)$  from some word of  $C_2$ , say  $\mathbf{x}$ . Thus  $\mathbf{s} = \mathbf{x} + \mathbf{y}$ , where  $\mathbf{y}$  is the sum of at most  $R(C_2)$  columns of  $\mathbf{I}_{n-k}$ . Now, clearly  $\mathbf{x}$  is a sum of at most  $R(C_1)$  columns of  $\mathbf{P}$ .  $\square$

With the same notations the following result holds.

**Theorem 8.1.7** *Let  $W$  be the largest weight in  $C$  which is at most  $n - k + R(C_1)$ . Then  $R(C) \leq \lfloor W/2 \rfloor + R(C_2)$ .*

**Proof.** Like in the proof of the previous theorem,  $\mathbf{x}$  can be obtained as a sum of at most  $R(C_1)$  columns of  $\mathbf{P}$ , or alternatively as a sum of at most  $n - k$  columns of  $\mathbf{I}_{n-k}$ . These two sums yield a codeword in  $C$  of weight at most  $n - k + R(C_1)$ , hence at most  $W$ , and therefore at least one of the two sums uses at most  $\lfloor W/2 \rfloor$  columns of  $\mathbf{H}$ .  $\square$

**Linear codes with a given minimum distance**

Assume now that  $C$  is an  $[n, k, d]_R$  code. Using  $d$ , the redundancy bound can be improved. We need the following auxiliary result.

**Lemma 8.1.8** *If there exists an  $[n, k, d]_R$  code, then there exists an  $[n - R, k, \lceil d/2 \rceil]$  code.*

**Proof.** Let  $\mathbf{x}$  be a deep hole of weight  $R$  (by linearity, such a deep hole always exists). We claim that puncturing  $C$  on the coordinates that belong to  $\text{supp}(\mathbf{x})$  gives a code with dimension  $k$  and minimum distance  $\lceil d/2 \rceil$ . Indeed, if  $\mathbf{c}$  is a nonzero codeword, then, denoting by  $\mathbf{x} \cap \mathbf{c}$  the vector having 1's only in the coordinates where both  $\mathbf{x}$  and  $\mathbf{c}$  have 1's, we get

$$R \leq d(\mathbf{x}, \mathbf{c}) = w(\mathbf{x}) + w(\mathbf{c}) - 2w(\mathbf{x} \cap \mathbf{c}) = R + w(\mathbf{c}) - 2w(\mathbf{x} \cap \mathbf{c}),$$

and  $w(\mathbf{c} \cap \mathbf{x}) \leq \lfloor w(\mathbf{c})/2 \rfloor$ . Consequently,

$$w(\mathbf{c}) - w(\mathbf{x} \cap \mathbf{c}) \geq w(\mathbf{c}) - \lfloor w(\mathbf{c})/2 \rfloor = \lceil w(\mathbf{c})/2 \rceil \geq \lceil d/2 \rceil,$$

proving that the minimum distance of the resulting code is at least  $\lceil d/2 \rceil$ . Clearly it has dimension  $k$  because there is no nonzero codeword  $\mathbf{c} \in C$  such that  $\text{supp}(\mathbf{c}) \subseteq \text{supp}(\mathbf{x})$ .  $\square$

Nonexistence results on the punctured code lead to bounds on  $T[n, k, d]$ , the maximal covering radius of an  $[n, k, d]$  code. Recall that  $a[n, d]$  stands for the maximal dimension of a linear code of length  $n$  and minimum distance  $d$ , and  $n[k, d]$  for the smallest length of a code having dimension  $k$  and minimum distance  $d$ .

**Theorem 8.1.9** *If  $j$  is the largest number such that  $a[n - j, \lceil d/2 \rceil] \geq k$ , then*

$$T[n, k, d] \leq j.$$

**Proof.** Obviously follows from the preceding lemma.  $\square$

Another possible formulation of the previous theorem uses the quantity  $n[k, d]$ .

**Theorem 8.1.10**

$$T[n, k, d] \leq n - n[k, \lceil d/2 \rceil].$$

$\square$

Employing known bounds on  $a[n, d]$  or  $n[k, d]$ , we derive estimates for  $T[n, k, d]$ .

We start with the Griesmer bound on  $n[k, d]$ , whose proof is based on the following lemma.

**Lemma 8.1.11**

$$n[k, d] \geq d + n[k - 1, \lceil d/2 \rceil].$$

**Proof.** It is very similar to the proof of Lemma 8.1.8. The difference is that here we puncture the original code on the support of a minimum weight codeword, so the dimension drops by one. Indeed, if we take a generator matrix

$$\mathbf{G} = \begin{pmatrix} 1^d & \mathbf{0} \\ * & \mathbf{G}_0 \end{pmatrix}$$

for  $C$ , then it is easy to see that the matrix  $\mathbf{G}_0$  generates an  $[n - d, k - 1, \geq \lceil d/2 \rceil]$  code, called the *residual code* of  $C$ .  $\square$

**Corollary 8.1.12 (Griesmer bound)**

$$n[k, d] \geq g[k, d] := \sum_{i=0}^{k-1} \lceil d/2^i \rceil.$$

**Proof.** By iterative use of the previous lemma.  $\square$

**Theorem 8.1.13**

$$\begin{aligned} T[n, k, d] &\leq n - \sum_{i=1}^k \lceil d/2^i \rceil \\ &= n - g[k, d] + d - \lceil d \cdot 2^{-k} \rceil. \end{aligned}$$

**Proof.** Combine the Griesmer bound with Theorem 8.1.10.  $\square$

**Corollary 8.1.14** For an  $[n = g[k, d], k, d]_R$  code satisfying the Griesmer bound,  $R \leq d - \lceil d \cdot 2^{-k} \rceil$ .  $\square$

Consider now the case of an  $[n, k = a[n, d], d]$  code, and, analogously, of a nonlinear  $(n, K = A(n, d), d)$  code.

**Theorem 8.1.15**

$$T[n, a[n, d], d] \leq d - 1,$$

$$T(n, A(n, d), d) \leq d - 1.$$

**Proof.** If the covering radius of an  $[n, a[n, d], d]$  code  $C$  is at least  $d$ , and  $\mathbf{x}$  is a deep hole, then  $C \cup (\mathbf{x} + C)$  is an  $[n, a[n, d] + 1, d]$  code, contradicting the definition of  $a[n, d]$ . If the covering radius of an  $(n, A(n, d), d)$  code is greater than  $d - 1$  and  $\mathbf{x}$  is a deep hole, then  $\{\mathbf{x}\} \cup C$  is an  $(n, A(n, d) + 1, d)$  code, contradicting the definition of  $A(n, d)$ .  $\square$

Assume that  $a[n, d] = a[n, d - 1] = \dots = a[n, d - j]$  for some  $j > 0$ . Then the following generalization of the previous theorem holds.

**Theorem 8.1.16** If  $j$  is the maximal nonnegative integer such that  $a[n, d] = a[n, d - j]$ , then

$$T[n, a[n, d], d] \leq d - j - 1.$$

**Proof.** Let  $C$  be a linear  $[n, a[n, d], d]$  code. Assume that  $R(C) \geq d - j$ , and  $\mathbf{x}$  is a deep hole. Then the code  $C \cup (\mathbf{x} + C)$  is a linear  $[n, a[n, d] + 1, \geq d - j]$  code, contradicting the definition of  $j$ .  $\square$

We now present a more general bound.

**Theorem 8.1.17**

$$T[n, k = a[n, d], d] \leq d - (n[k + 1, d] - n).$$

**Proof.** Let  $C$  be an  $[n, k, d]R$  code with  $k = a[n, d]$  and  $\mathbf{x}$  a deep hole of weight  $R$ . Suppose indirectly that  $R > d - (n[k + 1, d] - n)$ . Construct a code  $C'$  by appending  $n[k + 1, d] - n - 1$  zeros to all codewords in  $C$ . Appending the same number of ones to  $\mathbf{x}$ , we get a vector  $\mathbf{x}'$  at distance at least  $d$  from  $C'$ . The code spanned by  $C'$  and  $\mathbf{x}'$  is an impossible  $[n[k + 1, d] - 1, k + 1, d]$  code.  $\square$

The bound of Theorem 8.1.13 gives good results if the minimum distance of the code is relatively large. Otherwise, another approach should be adopted.

**Theorem 8.1.18** *Any  $[n, k, d]R$  code  $C$  satisfies*

- (i)  $a[R, d] + k \leq a[n, d]$ ;
- (ii)  $\log_2 A(R, d) + k \leq \log_2 A(n, d)$ .

**Proof.** Let  $\mathbf{x}$  be a deep hole of weight  $R$ . Without loss of generality, assume that the support of  $\mathbf{x}$  is  $[1, R]$ . Appending  $n - R$  zeros to every codeword of an  $[R, a[R, d], d]$  code gives an  $[n, a[R, d], d]$  code  $C'$ . We construct a new code

$$C + C' = \{\mathbf{c} + \mathbf{c}' : \mathbf{c} \in C, \mathbf{c}' \in C'\}.$$

This new linear code has length  $n$  and dimension  $k + a[R, d]$ . We prove that its minimum distance is  $d$ . Let  $\mathbf{c}'$  be a nonzero codeword of  $C'$ . Then for every  $\mathbf{c} \in C$ ,

$$d(\mathbf{c}, \mathbf{c}') \geq d(\mathbf{c}, \mathbf{x}) - d(\mathbf{c}', \mathbf{x}) \geq R - (R - d) = d.$$

For case (ii) the proof is similar: pick a nonlinear  $(R, A(R, d), d)$  code, lengthen it by appending  $n - R$  zeros. Similarly, the sum of the constructed code and the original code possesses the required parameters.  $\square$

We now apply the Hamming bound.

**Lemma 8.1.19 (Hamming bound)** *For  $d$  odd,*

$$a[n, d] \leq n - \lceil \log_2 V(n, (d - 1)/2) \rceil.$$

**Proof.** Since the distance between any two codewords in an  $[n, k, d]$  code is at least  $d$ , the spheres of radius  $(d - 1)/2$  do not intersect, so  $2^k V(n, (d - 1)/2) \leq 2^n$ .  $\square$

Theorem 8.1.18 now gives the following result.

**Theorem 8.1.20** *Let  $d$  be odd and  $j$  be the maximal number such that*

$$a[j, d] \leq (n - k) - \lceil \log_2 V(n, (d - 1)/2) \rceil.$$

*Then  $T[n, k, d] \leq j$ .*  $\square$

To find lower bounds on  $a[j, d]$ , we use known results on constructions of codes (see Section 2.6). In particular, for  $d = 3$ , the shortened Hamming codes, combined with the Hamming bound, give

$$a[n, 3] = n - 1 - \lfloor \log_2 n \rfloor.$$

**Theorem 8.1.21** *If  $j$  is the maximal integer such that  $j - \lfloor \log_2 j \rfloor \leq (n - k) - \lfloor \log_2 n \rfloor$ , then  $T[n, k, 3] \leq j$ .*  $\square$

## 8.2 Covering radii of subcodes

We now study relations between the covering radii of a code and its subcodes. In this section  $C_0$  stands for an arbitrary subcode of a code  $C$ .

**Lemma 8.2.1 (Supercode lemma)** *Let  $C_0 \subset C$  and  $D(C_0, C)$  be the maximum distance of a vector in  $C$  to  $C_0$ . Then  $R(C_0) \geq D(C_0, C)$ . In particular,  $R(C_0) \geq d(C)$ .*

*If  $C$  and  $C_0$  are linear codes, then*

$$R(C_0) \geq \max\{w(\mathbf{x} + C_0) : \mathbf{x} \in C \setminus C_0\}.$$

**Proof.** There exists a vector  $\mathbf{c} \in C$  such that for each  $\mathbf{c}_0 \in C_0$ , we have  $d(\mathbf{c}_0, \mathbf{c}) \geq D(C_0, C)$ . Hence  $R(C_0) \geq D(C_0, C)$ . If both  $C_0$  and  $C$  are linear,  $D(C_0, C)$  has the value given in the statement of the lemma.  $\square$

With the same notation we have the following bound.

**Lemma 8.2.2**

$$R(C) \leq R(C_0) \leq R(C) + D(C_0, C).$$

**Proof.** The first inequality is trivial. Let  $\mathbf{x}$  be at distance  $R(C_0)$  from  $C_0$ , and  $\mathbf{c}$  be a word in  $C$  closest to  $\mathbf{x}$ . Then  $d(\mathbf{x}, \mathbf{c}) \leq R(C)$ . Furthermore, let  $\mathbf{c}_0$  be a word in  $C_0$  closest to  $\mathbf{c}$ . Then  $d(\mathbf{c}_0, \mathbf{c}) \leq D(C_0, C)$ . So,

$$\begin{aligned} R(C_0) &\leq d(\mathbf{x}, \mathbf{c}_0) \leq d(\mathbf{x}, \mathbf{c}) + d(\mathbf{c}_0, \mathbf{c}) \\ &\leq R(C) + D(C_0, C), \end{aligned}$$

proving the second inequality.  $\square$

Now assume that  $C$  is an  $[n, k]$  code, and  $C_0$  is an  $[n, k_0]$  subcode of  $C$ . The number  $k - k_0$  is the *codimension* of  $C_0$  in  $C$ . The following theorem gives an upper bound on the covering radius of  $C_0$  in terms of the covering radius of  $C$  and the codimension of  $C_0$  in  $C$ .

**Theorem 8.2.3** *Let  $C_0$  be a subcode of codimension  $i$  in a linear code  $C$ . Then*

$$R(C_0) \leq (i+1)R(C) + i. \quad (8.2.4)$$

**Proof.** If  $i = 0$ , then (8.2.4) holds with equality. Assume that  $i \geq 1$  and let

$$\mathbf{H}_0 = \left( \frac{\mathbf{H}}{\mathbf{H}_1} \right)$$

be a parity check matrix of  $C_0$  such that  $\mathbf{H}$  is a parity check matrix for  $C$ . Let the columns of  $\mathbf{H}_0$ ,  $\mathbf{H}$  and  $\mathbf{H}_1$  be respectively,  $\mathbf{h}_0^j$ ,  $\mathbf{h}^j$  and  $\mathbf{h}_1^j$  for  $j \in [1, n]$ .

Let  $R = R(C)$  and  $R_0 = R(C_0)$ . Assume indirectly that  $R_0 > (i+1)R + i$ , that is,  $R_0 \geq (i+1)(R+1)$ . Without loss of generality, we may assume that

$$\mathbf{s}_0 = \sum_{j=1}^{R_0} \mathbf{h}_0^j,$$

and that  $\mathbf{s}_0$  is not the sum of any  $R_0 - 1$  or fewer columns of  $\mathbf{H}_0$ . Let  $J_1, J_2, \dots, J_{i+1}$  be a partition of  $\{1, 2, \dots, R_0\}$  into sets of cardinality at least  $R+1$ . Let

$$\mathbf{s}_0^r = \sum_{j \in J_r} \mathbf{h}_0^j, \quad r \in [1, i+1].$$

Since the covering radius of  $C$  equals  $R$ , there exist sets  $I_1, I_2, \dots, I_{i+1}$  of cardinality at most  $R$  such that

$$\sum_{j \in I_r} \mathbf{h}^j = \sum_{j \in J_r} \mathbf{h}_1^j, \quad r \in [1, i+1].$$

The set of  $i+1$  vectors of  $\mathbb{F}^i$

$$\left\{ \sum_{j \in I_r} \mathbf{h}_1^j - \sum_{j \in J_r} \mathbf{h}_1^j : r \in [1, i+1] \right\}$$

is linearly dependent. It follows that there exists a nonempty subset  $S$  of  $[1, i+1]$  such that

$$\sum_{j \in \cup_{i \in S} I_i} \mathbf{h}_1^j = \sum_{j \in \cup_{i \in S} J_i} \mathbf{h}_1^j.$$

But then

$$\begin{aligned}s_0 &= \sum_{r=1}^{i+1} \sum_{j \in J_r} \mathbf{h}_0^j = \sum_{r \in S} \sum_{j \in J_r} \mathbf{h}_0^j + \sum_{r \notin S} \sum_{j \in J_r} \mathbf{h}_0^j \\ &= \sum_{r \in S} \sum_{j \in I_r} \mathbf{h}_0^j + \sum_{r \notin S} \sum_{j \in J_r} \mathbf{h}_0^j.\end{aligned}$$

Since  $S$  is nonempty, this contradicts our assumption that  $s_0$  cannot be expressed as a sum of  $R_0 - 1$  or fewer columns of  $\mathbf{H}_0$ .  $\square$

If  $C$  is an even code, then a slight modification of the proof of Theorem 8.2.3 leads to an improvement of (8.2.4).

**Theorem 8.2.5** *Let  $C_0$  be a subcode of codimension  $i$  in an even binary linear code  $C$ . Then*

$$R(C_0) \leq (i+1)R(C). \quad (8.2.6)$$

**Proof.** By puncturing the first coordinate in the two even codes  $C$  and  $C_0$ , we obtain codes  $C^*$  and  $C_0^*$  with covering radius  $R(C) - 1$  and  $R(C_0) - 1$  (by Theorem 3.1.3). By Theorem 8.2.3,  $R(C_0) - 1 = R(C_0^*) \leq (i+1)R(C^*) + i = (i+1)(R(C) - 1) + i$ , proving the claim.  $\square$

An alternative approach relates the chromatic number of a graph to the covering radius. Let  $G$  be a graph with a set  $V$  of vertices and a set  $E$  of edges (unordered pairs of vertices). A *colouring* of  $G$  with colour set  $P$  is a mapping  $f : V \rightarrow P$  such that  $f(x) \neq f(y)$  whenever  $\{x, y\}$  is an edge. The *chromatic number* of  $G$  is the smallest integer  $\chi(G)$  for which  $G$  has a colouring with colour set of cardinality  $\chi(G)$ . A *stable* or *independent* set of a graph  $G$  is a collection of its vertices no two of which are adjacent. The largest size of a stable set is the *independence number* of the graph, denoted by  $\alpha(G)$ . Let  $n$  be the number of vertices and  $f$  be a colouring of  $G$ . A monochromatic subset of  $V$  is stable. Hence  $\chi(G) \geq n/\alpha(G)$ .

Let  $G(n, s)$  be the graph with vertex set  $\mathbb{F}^n$  where two vertices  $\mathbf{u}, \mathbf{v} \in \mathbb{F}^n$  form an edge if and only if their distance is greater than  $s$ . The *Kneser graph*  $\mathcal{K}(n, r+1)$  is the subgraph of  $G(n, 2r)$  induced by the subset of  $\mathbb{F}^n$  consisting of the vertices of weight  $r+1$ . Thus two elements  $\mathbf{u}, \mathbf{v} \in S_{r+1}$  are adjacent in  $\mathcal{K}(n, r+1)$  if and only if no coordinate equals 1 in both  $\mathbf{u}$  and  $\mathbf{v}$ . It is known that

$$\chi(\mathcal{K}(n, r+1)) = n - 2r \quad \text{if } n \geq 2r + 2. \quad (8.2.7)$$

**Theorem 8.2.8** *Let  $C_0$  be a subcode of codimension  $i \geq 1$  in a linear code  $C$ . Then*

$$R(C_0) \leq 2R(C) + 2^i - 1. \quad (8.2.9)$$

**Proof.** As before let

$$\mathbf{H}_0 = \left( \frac{\mathbf{H}}{\mathbf{H}_1} \right)$$

be a parity check matrix of  $C_0$  such that  $\mathbf{H}$  is a parity check matrix for  $C$ , and let the columns of  $\mathbf{H}_0$ ,  $\mathbf{H}$  and  $\mathbf{H}_1$  be respectively,  $\mathbf{h}_0^j$ ,  $\mathbf{h}^j$  and  $\mathbf{h}_1^j$  for  $j \in [1, n]$ . Assume that  $R_0 \geq 2R + 2^i$  ( $\geq 2R + 2$ ). Without loss of generality, suppose again that

$$\mathbf{s}_0 = \sum_{j=1}^{R_0} \mathbf{h}_0^j$$

cannot be expressed as a sum of  $R_0 - 1$  or fewer columns of  $\mathbf{H}_0$ . We write each vector  $\mathbf{v} \in \mathbb{F}^n$  as  $(\mathbf{v}', \mathbf{v}'')$  where  $\mathbf{v}'$  is in  $\mathbb{F}^{R_0}$ .

Since  $C$  has covering radius  $R$ , for each vector  $\mathbf{v}' \in \mathbb{F}^{R_0}$ , there is a vector  $\mathbf{x}_{\mathbf{v}'} \in C$  such that the distance between  $(\mathbf{v}', 0^{n-R_0})$  and  $\mathbf{x}_{\mathbf{v}'}$  is at most  $R$ . We define a mapping  $f$  from the vectors  $\mathbf{v}'$  of  $\mathbb{F}^{R_0}$  of weight  $R + 1$  to the  $2^i - 1$  nonzero vectors of  $\mathbb{F}^i$  by

$$f(\mathbf{v}') = \mathbf{H}_1 \mathbf{x}_{\mathbf{v}'}^T.$$

We have  $\mathbf{H}_1 \mathbf{x}_{\mathbf{v}'}^T \neq \mathbf{0}$  because otherwise, since  $\mathbf{x}_{\mathbf{v}'}$  is in  $C$ , the vector  $\mathbf{s}_0$  could be expressed as a sum of fewer than  $R_0$  columns of  $\mathbf{H}_0$ .

Let  $\{\mathbf{v}', \mathbf{w}'\}$  be an edge of the Kneser graph  $\mathcal{K}(R_0, R + 1)$ , and assume that  $f(\mathbf{v}') = f(\mathbf{w}')$ , that is,  $\mathbf{H}_1 \mathbf{x}_{\mathbf{v}'}^T = \mathbf{H}_1 \mathbf{x}_{\mathbf{w}'}^T$ . Then  $\mathbf{v}' + \mathbf{w}'$  has weight  $2R + 2$ , and the distance between  $(\mathbf{v}' + \mathbf{w}', \mathbf{0})$  and  $\mathbf{x}_{\mathbf{v}'} + \mathbf{x}_{\mathbf{w}'}$  is at most  $2R$ . Since  $\mathbf{H}_1(\mathbf{x}_{\mathbf{v}'} + \mathbf{x}_{\mathbf{w}'})^T = \mathbf{0}$ , we see that  $\mathbf{s}_0$  can be expressed as a sum of at most  $R_0 - 2$  columns of  $\mathbf{H}_0$ , a contradiction. Hence  $f(\mathbf{v}') \neq f(\mathbf{w}')$  whenever  $\{\mathbf{v}', \mathbf{w}'\}$  is an edge, and  $f$  is a colouring of the Kneser graph  $\mathcal{K}(R_0, R + 1)$  with  $2^i - 1$  colours. Applying (8.2.7) we obtain

$$R_0 - 2R = \chi(\mathcal{K}(R_0, R + 1)) \leq 2^i - 1.$$

□

The Kleitman theorem (see Theorem 2.4.16) gives an upper bound on the cardinality of a stable set of the graph  $G(n, 2r)$ , and hence a lower bound on its chromatic number.

**Theorem 8.2.10** *Let  $n$  and  $r$  be positive,  $n \geq 2r + 1$ . Then each stable set of  $G(n, 2r)$  has cardinality at most  $V(n, r)$  and hence  $\chi(G(n, 2r)) \geq 2^n / V(n, r)$ .*

□

The following theorem often improves (8.2.4) and (8.2.9).

**Theorem 8.2.11** *Let  $C_0$  be a subcode of codimension  $i \geq 1$  in a linear code  $C$ . Then*

$$\frac{2^{R_0}}{V(R_0, R)} \leq 2^i, \quad (8.2.12)$$

that is,  $R_0 \leq \log_2 (V(R_0, R)) + i$ .

**Proof.** If  $R_0 \leq 2R$ , then (8.2.12) is trivially true. Assume that  $R_0 \geq 2R+1$ . As in the proof of the preceding theorem we consider  $f$  as a mapping from the vertices of  $G(R_0, 2R)$  to  $\mathbb{F}^i$ . As before this entails that  $f$  is a colouring of  $G(R_0, 2R)$  with  $2^i$  colours and the result follows by Theorem 8.2.10.  $\square$

### 8.3 Covering radius and dual distance

In this section, we study relations between covering radius and dual spectrum.

We start with some definitions. For  $\mathbf{x} \in \mathbb{F}^n$  let the  $(n+1)$ -tuple  $\mathcal{A}(\mathbf{x}) = (\mathcal{A}_0(\mathbf{x}), \dots, \mathcal{A}_n(\mathbf{x}))$  stand for the weight distribution of the translate  $C + \mathbf{x}$ ,

$$\mathcal{A}_i(\mathbf{x}) = |\{\mathbf{a} \in C : d(\mathbf{a}, \mathbf{x}) = i\}|.$$

Then the distance distribution  $\mathcal{B} = (\mathcal{B}_0, \dots, \mathcal{B}_n)$  of the code is defined by

$$\mathcal{B}_i = \frac{1}{|C|} \sum_{\mathbf{a} \in C} \mathcal{A}_i(\mathbf{a}).$$

Evidently,

$$\mathcal{B}_i = \frac{1}{|C|} |\{\mathbf{a} \in C, \mathbf{b} \in C : d(\mathbf{a}, \mathbf{b}) = i\}|.$$

With this notation, the minimum distance of the code is

$$d(C) = d = \min_{\mathbf{a}, \mathbf{b} \in C, \mathbf{a} \neq \mathbf{b}} d(\mathbf{a}, \mathbf{b}) = \min\{j : j > 0, \mathcal{B}_j \neq 0\}.$$

The covering radius of the code is

$$R(C) = R = \min\{j : \forall \mathbf{x} \in \mathbb{F}^n \exists i : [i \leq j, \mathcal{A}_i(\mathbf{x}) \neq 0]\}. \quad (8.3.1)$$

Like in Section 2.2, we define the additive character on  $\mathbb{F}^n$ :

$$\psi_{\mathbf{x}}(\mathbf{y}) = (-1)^{\langle \mathbf{x}, \mathbf{y} \rangle}.$$

Recall that  $S_i = \{\mathbf{y} \in \mathbb{F}^n : w(\mathbf{y}) = i\}$ . If  $\mathbf{x} \in S_i$ , then (see Section 2.2)

$$\sum_{\mathbf{y} \in S_i} \psi_{\mathbf{x}}(\mathbf{y}) = P_k(i) ,$$

where  $P_k(i)$  is the  $k$ -th Krawtchouk polynomial. For arbitrary  $G \subseteq \mathbb{F}^n$  and  $\mathbf{x} \in \mathbb{F}^n$  we extend the definition of the additive character on the set  $G$ :

$$\psi_{\mathbf{x}}(G) = \sum_{\mathbf{g} \in G} \psi_{\mathbf{x}}(\mathbf{g}) .$$

Clearly,  $|\psi_{\mathbf{x}}(G)| \leq |G|$ .

The *dual spectrum* of  $C$  is the  $n$ -tuple  $\mathcal{B}^\perp$  defined by

$$\mathcal{B}_j^\perp = \frac{1}{|C|} \sum_{i=0}^n \mathcal{B}_i P_j(i) .$$

By Theorem 2.2.7,

$$\begin{aligned} \mathcal{B}_j^\perp &= \frac{1}{|C|^2} \sum_{\mathbf{y} \in S_j} \sum_{\mathbf{a} \in C} \sum_{\mathbf{b} \in C} \psi_{\mathbf{y}}(\mathbf{a} + \mathbf{b}) \\ &= \frac{1}{|C|^2} \sum_{\mathbf{y} \in S_j} |\psi_{\mathbf{y}}(C)|^2 . \end{aligned}$$

Notice that for linear codes

$$\mathcal{B}_j^\perp = \frac{1}{|C|} \sum_{\mathbf{y} \in S_j} \psi_{\mathbf{y}}(C) ,$$

and  $\mathcal{B}_j^\perp$  is just the number of vectors of weight  $j$  in the dual code.

Then the *dual distance*  $d^\perp(C)$  of a code  $C$  is defined as follows:

$$d^\perp(C) = d^\perp = \min \{j : j > 0, \mathcal{B}_j^\perp \neq 0\} ,$$

i.e., it is the first nonzero index of a nonzero component in the MacWilliams transform of the distance distribution of  $C$ .

Analogously to  $\mathcal{B}^\perp$ , define the MacWilliams transform of the weight distribution of  $C + \mathbf{x}$  by

$$\mathcal{A}_k^\perp(\mathbf{x}) = \frac{1}{|C|} \sum_{i=0}^n \mathcal{A}_i(\mathbf{x}) P_k(i) .$$

Let

$$D^\perp = \{j : j \neq 0, \mathcal{B}_j^\perp \neq 0\}$$

be the set of nonzero indices of the nonzero elements in the dual spectrum. Set

$$\overline{D}^\perp = [1, n] \setminus D^\perp$$

and  $s^\perp = |D^\perp|$ . Thus  $|\overline{D}^\perp| = n - s^\perp$ .

## Auxiliary lemmas

We need the following result relating  $\mathcal{A}^\perp$  and  $\mathcal{B}^\perp$ .

**Lemma 8.3.2** *For any  $\mathbf{x} \in \mathbb{F}^n$  and  $i \in [0, n]$ ,*

$$(i) \quad |\mathcal{A}_i^\perp(\mathbf{x})| \leq \mathcal{B}_i^\perp \quad \text{for linear codes,}$$

and

$$(ii) \quad |\mathcal{A}_i^\perp(\mathbf{x})| \leq \sqrt{\binom{n}{i} \mathcal{B}_i^\perp} \quad \text{for nonlinear codes.}$$

**Proof.** (i) We use the fact that for linear codes

$$\psi_y(C) = |C| \text{ if } y \text{ is in the dual code, and } \psi_y(C) = 0 \text{ otherwise.}$$

We have

$$\mathcal{A}_i^\perp(\mathbf{x}) = \frac{1}{|C|} \sum_{y \in S_i} \psi_y(C + \mathbf{x}).$$

Hence

$$\begin{aligned} |\mathcal{A}_i^\perp(\mathbf{x})| &= \frac{1}{|C|} \left| \sum_{y \in S_i} \psi_y(C + \mathbf{x}) \right| = \frac{1}{|C|} \left| \sum_{y \in S_i} \psi_y(C) \psi_y(\mathbf{x}) \right| \\ &\leq \frac{1}{|C|} \sum_{y \in S_i} |\psi_y(C)| = \frac{1}{|C|} \sum_{y \in S_i} \psi_y(C) = \mathcal{B}_i^\perp. \end{aligned}$$

(ii) As in (i) we have

$$\begin{aligned} |\mathcal{A}_i^\perp(\mathbf{x})| &= \frac{1}{|C|} \left| \sum_{y \in S_i} \psi_y(C + \mathbf{x}) \right| \leq \frac{1}{|C|} \sum_{y \in S_i} |\psi_y(C)| \\ &\quad (\text{by the Cauchy-Schwarz inequality}) \\ &\leq \left( \sum_{y \in S_i} 1 \right)^{\frac{1}{2}} \left( \frac{1}{|C|^2} \sum_{y \in S_i} |\psi_y(C)|^2 \right)^{\frac{1}{2}} = \sqrt{\binom{n}{i} \mathcal{B}_i^\perp}. \end{aligned}$$

This finishes the proof.  $\square$

Thus,  $\mathcal{A}_i^\perp(\mathbf{x}) = 0$  whenever  $\mathcal{B}_i^\perp = 0$ , yielding the following

**Corollary 8.3.3**  $\mathcal{A}_i^\perp(\mathbf{x}) = 0$  for all  $\mathbf{x} \in \mathbb{F}^n$  and  $i \in \overline{D}^\perp$ .  $\square$

The following lemma is crucial to our purpose.

**Lemma 8.3.4** Let  $(\alpha_0, \alpha_1, \dots, \alpha_n)$  be such that  $\alpha_i \leq 0$  for  $i \in [j+1, n]$ . If a code  $C$  satisfies

$$\sum_{i=0}^n \alpha_i \mathcal{A}_i(\mathbf{x}) > 0$$

for every  $\mathbf{x} \in \mathbb{F}^n$ , then  $R(C) \leq j$ .

**Proof.** Since the  $\mathcal{A}_i(\mathbf{x})$ 's are always nonnegative,

$$0 < \sum_{i=0}^n \alpha_i \mathcal{A}_i(\mathbf{x}) \leq \sum_{i=0}^j \alpha_i \mathcal{A}_i(\mathbf{x}).$$

Thus, for every  $\mathbf{x} \in \mathbb{F}^n$  there exists an  $i \in [0, j]$  such that  $\mathcal{A}_i(\mathbf{x}) > 0$  and, by (8.3.1),  $R(C) \leq j$ .  $\square$

## The key theorem

We need the following values:

$A(n, d, w)$  - the maximal size of a constant weight code of length  $n$ , weight  $w$  and minimum distance  $d$ ;

$A(n, D)$  - the maximal size of a code of length  $n$  and nonzero distances belonging to the set  $D$ ;

$A(n, D, w)$  - the maximal size of a constant weight code of length  $n$ , weight  $w$  and nonzero distances belonging to the set  $D$ .

We also need the value of the linear programming bound on the size of a code. Let  $A^*(n, D)$  be the solution to the following linear programming problem:

$$\text{Find } \max \sum_{i=0}^n \mathcal{B}_i,$$

subject to the constraints

$$\mathcal{B}_0 = 1, \mathcal{B}_i = 0 \text{ for } i \notin D,$$

$$\sum_{i=0}^n \mathcal{B}_i P_k(i) \geq 0, \quad k \in [0, n].$$

Clearly the solution yields an upper bound on the size of the code. If  $D = [d, n]$ , the corresponding value is denoted by  $A^*(n, d)$ .

Now we are ready to prove the key theorem.

**Theorem 8.3.5** (i) Let  $r$  be an integer and

$$\alpha(x) = \sum_{i=0}^n \alpha_i P_i(x)$$

a polynomial such that

- $\alpha(0) > s^\perp \max_{j \in D^\perp} \{|\alpha(j)| A(n, D^\perp, j)\}$  for linear codes;
- $\alpha(0) > \sqrt{s^\perp A^*(n, D^\perp)} \max_{j \in D^\perp} \left\{ |\alpha(j)| \sqrt{\binom{n}{j}} \right\}$  for nonlinear codes;
- $\alpha_i \leq 0$  for  $i \in [r+1, n]$ .

Then  $R(C) \leq r$ .

(ii) (The dual statement) Let  $r$  be an integer and

$$\beta(x) = \sum_{i=0}^n \beta_i P_i(x)$$

a polynomial such that

- $\beta_0 > s^\perp \max_{j \in D^\perp} \{|\beta_j| A(n, D^\perp, j)\}$  for linear codes;
- $\beta_0 > \sqrt{s^\perp A^*(n, D^\perp)} \max_{j \in D^\perp} \left\{ |\beta_j| \sqrt{\binom{n}{j}} \right\}$  for nonlinear codes;
- $\beta(i) \leq 0$  for  $i \in [r+1, n]$ .

Then  $R(C) \leq r$ .

**Proof.** We first prove statement (i). Let  $\mathbf{x} \in \mathbb{F}^n$ . Then by Theorem 2.3.21,

$$\begin{aligned} \frac{2^n}{|C|} \sum_{i=0}^n \alpha_i \mathcal{A}_i(\mathbf{x}) &= \frac{1}{|C|} \sum_{i=0}^n \mathcal{A}_i(\mathbf{x}) \sum_{j=0}^n \alpha(j) P_j(i) \\ &= \frac{1}{|C|} \sum_{j=0}^n \alpha(j) \sum_{i=0}^n \mathcal{A}_i(\mathbf{x}) P_j(i) \\ &= \sum_{j=0}^n \alpha(j) \mathcal{A}_j^\perp(\mathbf{x}) \\ &= \alpha(0) + \sum_{j \in D^\perp} \alpha(j) \mathcal{A}_j^\perp(\mathbf{x}) \\ &\geq \alpha(0) - \sum_{j \in D^\perp} |\alpha(j)| |\mathcal{A}_j^\perp(\mathbf{x})|. \end{aligned}$$

For linear codes, combining Lemma 8.3.2 and the hypotheses we get

$$\begin{aligned} \frac{2^n}{|C|} \sum_{i=0}^n \alpha_i \mathcal{A}_i(\mathbf{x}) &\geq \alpha(0) - \sum_{j \in D^\perp} |\alpha(j)| \mathcal{B}_j^\perp \\ &\geq \alpha(0) - s^\perp \max_{j \in D^\perp} \{ |\alpha(j)| A(n, D^\perp, j) \} > 0. \end{aligned}$$

For nonlinear codes, by using also the Cauchy-Schwarz inequality we get

$$\begin{aligned} \frac{2^n}{|C|} \sum_{i=0}^n \alpha_i \mathcal{A}_i(\mathbf{x}) &\geq \alpha(0) - \sum_{j \in D^\perp} |\alpha(j)| \sqrt{\binom{n}{j} \mathcal{B}_j^\perp} \\ &\geq \alpha(0) - \left( \sum_{j \in D^\perp} \alpha^2(j) \binom{n}{j} \right)^{1/2} \left( \sum_{j \in D^\perp} \mathcal{B}_j^\perp \right)^{1/2} \\ &\geq \alpha(0) - \sqrt{s^\perp A^*(n, D^\perp)} \max_{j \in D^\perp} \left\{ |\alpha(j)| \sqrt{\binom{n}{j}} \right\} > 0. \end{aligned}$$

Here we upperestimated  $\sum_{j \in D^\perp} \mathcal{B}_j^\perp$  by  $A^*(n, D^\perp)$ . Indeed, we are allowed to do so, since the linear programming problem can be stated for the components  $\mathcal{B}_i^\perp$  as well. The MacWilliams transform of  $\mathcal{B}^\perp$  is  $\mathcal{B}$ , so all its components are nonnegative.

In both cases the result now follows from Lemma 8.3.4.

To prove the dual statement, we notice that

$$\frac{1}{|C|} \sum_{i=0}^n \beta(i) \mathcal{A}_i(\mathbf{x}) = \frac{1}{|C|} \sum_{i=0}^n \sum_{j=0}^n \beta_j \mathcal{A}_i(\mathbf{x}) P_j(i) = \sum_{j=0}^n \beta_j \mathcal{A}_j^\perp(\mathbf{x}),$$

and the claim follows in exactly the same way as in case (i).  $\square$

**Corollary 8.3.6** (i) Let  $r$  be an integer and  $\alpha(x) = \sum_{i=0}^n \alpha_i P_i(x)$  a polynomial such that

- $\alpha(0) > n A(n, D^\perp) \max_{j \in D^\perp} |\alpha(j)|$  for linear codes;
- $\alpha(0) > 2^{n/2} \sqrt{n A^*(n, D^\perp)} \max_{j \in D^\perp} |\alpha(j)|$  for nonlinear codes;
- $\alpha_i \leq 0$  for  $i \in [r+1, n]$ .

Then  $R(C) \leq r$ .

(ii) (The dual statement) Let  $r$  be an integer and  $\beta(x) = \sum_{i=0}^n \beta_i P_i(x)$  a polynomial such that

- $\beta_0 > nA(n, D^\perp) \max_{j \in D^\perp} |\beta_j|$  for linear codes;
- $\beta_0 > 2^{n/2} \sqrt{n A^*(n, D^\perp)} \max_{j \in D^\perp} |\beta_j|$  for nonlinear codes;
- $\beta(i) \leq 0$  for  $i \in [r+1, n]$ .

Then  $R(C) \leq r$ .

**Proof.** It follows from the evident inequalities

$$s^\perp \leq n, \quad A(n, D^\perp, j) \leq A(n, D^\perp), \quad \binom{n}{j} < 2^n,$$

combined with the key theorem.  $\square$

Different choices of polynomials allow us to derive many efficient bounds.

**Theorem 8.3.7 (Delsarte bound)** *For every code  $C$ ,*

$$R(C) \leq s^\perp.$$

**Proof.** Let  $D^\perp = \{d_1^\perp, \dots, d_{s^\perp}^\perp\}$ . We choose in the direct statement of the theorem

$$\alpha(x) = \prod_{i=1}^{s^\perp} (d_i^\perp - x).$$

Note that  $\alpha(x) = 0$  for all  $x \in D^\perp$ . So, the first condition in Theorem 8.3.5 reduces to  $\alpha(0) > 0$ , which holds since  $\alpha(0) = d_1^\perp d_2^\perp \dots d_{s^\perp}^\perp > 0$ . Furthermore, the polynomial  $\alpha(x)$  is of degree  $s^\perp$ , and hence,  $\alpha_i = 0$  for  $i \geq s^\perp + 1$ . From the key theorem we conclude that  $R(C) \leq s^\perp$ .  $\square$

In many codes, e.g., duals of BCH codes,  $D^\perp \subseteq [d^\perp, n - d^\perp]$ .

**Theorem 8.3.8** *Let  $C$  be a code of length  $n$  with  $D^\perp \subseteq [d^\perp, n - d^\perp]$ ,  $d^\perp < n/2$ . Then*

$$R(C) \leq \left\lceil -\frac{(1/2) \log_2 A^*(n, d^\perp) + n/2 + (\log_2 n)/2}{\log_2(1 - 2d^\perp/n)} \right\rceil.$$

*If  $C$  is linear, then*

$$R(C) \leq \left\lceil -\frac{a[n, d^\perp] + \log_2 n}{\log_2(1 - 2d^\perp/n)} \right\rceil.$$

**Proof.** Choose in the direct statement of Corollary 8.3.6 the polynomial  $\alpha(x) = (P_1(x))^r = (n - 2x)^r$ , and compute easily

$$\alpha(0) = n^r, \quad \alpha_i = 0 \text{ for } i \geq r + 1,$$

$$\max_{j \in [d^\perp, n - d^\perp]} |\alpha(j)| = (n - 2d^\perp)^r.$$

Straightforward calculations lead to the sought result.  $\square$

Another, more efficient, choice of  $\alpha$  would be a Chebyshev polynomial. This is considered in detail in Section 12.7.

Now, let us deal with the dual statement.

**Theorem 8.3.9** *Let  $C$  be a code of length  $n$  and dual distance  $d^\perp$ . Let  $r$  be an integer and  $\beta(x) = \sum_{i=0}^{d^\perp-1} \beta_i P_i(x)$  a polynomial such that*

- $\beta_0 > 0$ ;
- $\beta(i) \leq 0$  for  $i \in [r + 1, n]$ .

*Then  $R(C) \leq r$ .*

**Proof.** Notice that for the above polynomial,  $\beta_j = 0$  for all  $j \in D^\perp$ , and, thus, in the dual statement of Theorem 8.3.5 the first condition reduces to the simple condition  $\beta_0 > 0$ .  $\square$

Now, let  $x_{j,n}(u)$  be the  $j$ -th root of  $P_u^n(x)$  (for information on the roots of Krawtchouk polynomials see Section 2.3). Then choose

$$\beta(x) = \beta(x, \varepsilon) = (x - x_{1,n-1}(u) - \varepsilon)(x - x_{2,n-1}(u))^2 \dots (x - x_{u,n-1}(u))^2 (x - n),$$

if  $d^\perp = 2u + 1$ , and

$$\beta(x) = \beta(x, \varepsilon) = -(x - x_{1,n}(u) - \varepsilon)(x - x_{2,n}(u))^2 \dots (x - x_{u,n}(u))^2,$$

if  $d^\perp = 2u$ .

**Lemma 8.3.10** *Let  $\beta(x, \varepsilon)$  be as above,*

$$\beta(x, \varepsilon) = \sum_{j=0}^{d^\perp-1} \beta_j(\varepsilon) P_j(x).$$

*Then for every positive  $\varepsilon$  we have  $\beta_0(\varepsilon) > 0$ .*

**Proof.** We give it in the even case  $d^\perp = 2u$ . The case of odd  $d^\perp$  is treated similarly.

By (2.3.24)

$$2^n \beta_0(\varepsilon) = \sum_{x=0}^n \binom{n}{x} \beta(x, \varepsilon),$$

and from the expression of  $\beta(x, \varepsilon)$  we get

$$2^n \beta_0(0) = - \sum_{x=0}^n \binom{n}{x} P_u(x) \cdot \frac{P_u(x)}{x - x_{1,n}(u)}.$$

Since  $P_u(x)/(x - x_{1,n}(u))$  is a polynomial of degree less than  $u$ , from Theorem 2.3.18 we conclude that  $\beta_0(0) = 0$ . Furthermore, differentiating yields

$$\frac{d \beta_0(\varepsilon)}{d \varepsilon} = 2^{-n} \sum_{x=0}^n \binom{n}{x} (x - x_{2,n}(u))^2 \dots (x - x_{u,n}(u))^2 > 0.$$

Thus  $\beta_0(\varepsilon) > 0$  for  $\varepsilon > 0$ . □

**Theorem 8.3.11** *Let  $C$  be a code of length  $n$  and dual distance  $d^\perp$ . Then*

$$R(C) \leq \begin{cases} x_{1,n-1}(u), & \text{if } d^\perp = 2u + 1, \\ x_{1,n}(u), & \text{if } d^\perp = 2u. \end{cases}$$

**Proof.** Use  $\beta(x)$  defined above in Theorem 8.3.9. □

Using the information on the minimal zeros of Krawtchouk polynomials, (2.3.32), we get the following corollary.

**Corollary 8.3.12** *Let  $C$  be a code of length  $n$  and dual distance  $d^\perp$ . Then*

$$R(C) \leq \begin{cases} (n-1)/2 - (\sqrt{u} - \sqrt[3]{u})\sqrt{n-1-u}, & \text{if } d^\perp = 2u + 1, \\ n/2 - (\sqrt{u} - \sqrt[3]{u})\sqrt{n-u}, & \text{if } d^\perp = 2u. \end{cases}$$

□

If a code is self-complementary, then its dual distance is even. Indeed, in every self-complementary code the distance distribution is symmetric with

respect to  $n/2$ , i.e.,  $\mathcal{B}_i = \mathcal{B}_{n-i}$  for  $i \in [0, n]$ . Now, for odd  $k$ 's, using the fact that  $P_k(x)$  is antisymmetric with respect to  $n/2$  (see (2.3.16)), we get

$$\mathcal{B}_k^\perp = \frac{1}{|C|} \sum_{i=0}^n \mathcal{B}_i P_k(i) = \frac{1}{2|C|} \left( \sum_{i=0}^n \mathcal{B}_i P_k(i) + \sum_{i=0}^n \mathcal{B}_{n-i} P_k(n-i) \right) = 0.$$

So, the odd components in the MacWilliams transform of the distance distribution of a self-complementary code vanish, and the dual distance is even.

The first two cases  $d^\perp = 2$  and  $d^\perp = 4$  are often referred to as the Norse bounds. A more direct proof of the particular case of (ii) in the following theorem is given in Section 9.2.

**Theorem 8.3.13 (Norse bounds)** (i) *The covering radius of a code with zeros and ones occurring equally often in each coordinate (i.e., having dual distance at least 2) is at most  $\lfloor n/2 \rfloor$ .*

(ii) *The covering radius of a code with  $d^\perp \geq 4$  is at most  $\lfloor (n - \sqrt{n})/2 \rfloor$ . In particular, this bound is valid for self-complementary codes with  $d^\perp > 2$ .*

**Proof.** Follows from  $x_{1,n}(1) = n/2$ ,  $x_{1,n}(2) = (n - \sqrt{n})/2$ . □

For linear codes the following result holds.

**Theorem 8.3.14** *The covering radius of a linear code without identically zero coordinate is at most  $\lfloor n/2 \rfloor$ .* □

## 8.4 Notes

**§8.1** Very little is known about the function  $A(n, d, B_i)$ . Its properties should somehow resemble the corresponding results for constant weight codes, see, e.g., Brouwer, Shearer, Sloane and W. D. Smith [95] and its extensive list of references.

Theorem 8.1.5 is by Karpovsky, see [363]. Theorems 8.1.6 and 8.1.7 are by Mattson [470], [469], Lemma 8.1.8 from Cohen, Litsyn, Lobstein and Mattson [158], and Theorem 8.1.10 by Cohen, Litsyn and Solé [161]. The Griesmer bound (Corollary 8.1.12) is from Griesmer [266]. Theorem 8.1.13 is by Janwa [346], Corollary 8.1.14 from Busschbach, Gerretzen and van Tilborg [108]. Theorem 8.1.17 is by Bhandari and Garg [80]. Theorem 8.1.18 is by Godlewski [252]. The Hamming bound (Lemma 8.1.19) is from [279]. For Theorem 8.1.21 see Zémor [700].

**§8.2** The supercode lemma is folklore. Lemma 8.2.2 is from Cohen, Karpovsky, Mattson and Schatz [156]. Theorem 8.2.3 is due independently to

Bruald and Pless [101] and Simonis [586] (see Adams [8] for the case  $i = 1$ ). Theorem 8.2.5 is by Simonis. Theorem 8.2.3 can be improved for direct sums of codes, see Bruald and Pless [102]. For bounds on covering radii of even subcodes of  $t$ -dense codes, see Janwa and Mattson [349]. The chromatic number of Kneser graphs (8.2.7) is determined by Lovász [459] (see also Bárány [48]). Theorem 8.2.8 is by Calderbank [111]. Theorem 8.2.11 is due to Hou [336].

**§8.3** The Delsarte bound is from [194]. For other proofs, see Assmus and Mattson [24], MacWilliams and Sloane [464], and, for the linear case, Assmus and Pless [27], and Wolfmann [693]. Theorem 8.3.8 is by Solé and Stokes [606]. Theorem 8.3.9 is by Tietäväinen [644], [646]. Lemma 8.3.10 is by Lahtonen [406]. Theorem 8.3.11 is by Tietäväinen [644], [646], where also the nonbinary case is considered. The Norse bounds are by Helleseth, Kløve and Mykkeltveit [300], the term “Norse bounds” was coined by Mattson. For other papers on upper bounds for covering radius as a function of dual distance, see Delorme and Solé [192], Fazekas and Levenshtein [233], Litsyn, Solé and Struik [444], Litsyn and Tietäväinen [445], Solé [602], Solé and Mehrotra [605], Struik [628].

# Chapter 9

## Reed-Muller codes

In this and the next chapters we analyze the covering radius of some classes of error-correcting codes. As already mentioned, the covering radius turns out to be an important parameter. Namely, it coincides with the maximal multiplicity of errors that can be corrected provided maximal likelihood decoding is used on a binary symmetric channel with probability of symbol error less than one half: the decoding algorithm outputs the closest codeword to the received vector. If codes are used for data compression, the covering radius is a measure of the maximum distortion. Another reason to study the covering radius of known codes is that it gives a test for maximality: a code is maximal if and only if its covering radius is strictly less than its minimum distance.

The main concern in the following two chapters is Reed-Muller and BCH codes. These families are quite well explored for error correction and contain codes with optimal or close to optimal parameters, together with very efficient decoding algorithms.

We start this chapter by giving a recursive description of Reed-Muller codes, their representation as extended cyclic codes and some information on the spectra of Reed-Muller codes of small and large orders. Section 9.2 is devoted to covering radii of first order Reed-Muller codes. We present the exact answer for the codes of length  $2^m$  with  $m$  even by giving an upper bound for the covering radius along with an explicitly constructed deep hole. For codes of length  $2^m$ ,  $m$  odd, the situation is much more enigmatic. Although the exact values are known for lengths up to 128, only bounds are available from there up. The section finishes with a discussion on normality. In Section 9.3 we investigate the covering radius of Reed-Muller codes of order two and of large orders. Evaluating the covering radius of Reed-Muller codes is trivial for the codes of length  $2^m$  and order  $m - 2$  or more. For codes of order  $m - 3$ , the covering radius is determined. Section 9.4 deals with arbitrary Reed-Muller codes, presenting partial results. Using recursion, we derive

asymptotic bounds on the covering radius of Reed-Muller codes, turning out to be surprisingly tight.

## 9.1 Definitions and properties

For  $0 \leq r \leq m$ ,  $\mathcal{RM}(r, m)$  denotes the  $r$ -th order Reed-Muller code, a linear code of length  $n = 2^m$ , dimension  $k(r, m) = V(m, r) = \sum_{i=0}^r \binom{m}{i}$  and minimum distance  $2^{m-r}$ . We give three possible definitions, (i) inductive, (ii) in terms of Boolean functions, and (iii) as extended cyclic codes. Properties of Reed-Muller codes are presented without proofs.

(i) Let  $\mathcal{RM}(0, m)$  consist of two vectors,  $\mathbf{0}$  and  $\mathbf{1}$ , and  $\mathcal{RM}(m, m)$  be the entire space of binary  $2^m$ -tuples. We inductively define Reed-Muller codes of arbitrary order. For  $0 < r < m$ ,

$$\begin{aligned} \mathcal{RM}(r, m) = & \{(\mathbf{u}, \mathbf{u} + \mathbf{v}) : \\ & \mathbf{u} \in \mathcal{RM}(r, m-1), \mathbf{v} \in \mathcal{RM}(r-1, m-1)\}. \end{aligned} \quad (9.1.1)$$

From (9.1.1) we obtain the shape of a generator matrix  $\mathbf{G}_{r, m}$  of  $\mathcal{RM}(r, m)$ . Let  $\mathbf{G}_{0, m}$  be the all-one  $2^m$ -vector, and  $\mathbf{G}_{m, m}$  be the identity matrix  $\mathbf{I}_{2^m}$ . Then

$$\mathbf{G}_{r, m} = \begin{pmatrix} \mathbf{G}_{r, m-1} & \mathbf{G}_{r, m-1} \\ \mathbf{0} & \mathbf{G}_{r-1, m-1} \end{pmatrix}. \quad (9.1.2)$$

For  $r = 1$  the generator matrix takes an especially simple form. Consider  $\mathbf{E}_m$ , the  $m \times 2^m$  matrix whose  $i$ -th column is the binary expansion of  $i$  for  $0 \leq i \leq 2^m - 1$ , and let  $\mathbf{E}_m^*$  be  $\mathbf{E}_m$  without the first (all-zero) column. Adjoin to  $\mathbf{E}_m$  the row of ones to obtain the  $(m+1) \times 2^m$  matrix  $\mathbf{G}_{1, m}$ , a generator matrix for  $\mathcal{RM}(1, m)$ .

Define the following mapping from the space of binary 0-1  $n$ -tuples to the space  $\{-1, 1\}^n$ :

$$\mathbf{u} = (u_1, \dots, u_n) \rightarrow \mathbf{u}^\pm = ((-1)^{u_1}, \dots, (-1)^{u_n}).$$

The set of vectors corresponding to  $\mathcal{RM}(1, m)$  is denoted by  $\mathcal{RM}^\pm(1, m)$ . The words of  $\mathcal{RM}^\pm(1, m)$  beginning with 1 constitute a Sylvester matrix  $\mathbf{H}_n^\pm$ , that is, a square  $\pm 1$ -matrix of size  $n \times n$  constructed as the  $m$ -th Kronecker power of

$$\mathbf{H}_2^\pm = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix};$$

as a consequence, it satisfies  $\mathbf{H}_n^\pm(\mathbf{H}_n^\pm)^T = n\mathbf{I}_n$ : Sylvester matrices are Hadamard. To obtain the complete code, take the complements of the rows of  $\mathbf{H}_n^\pm$  (cf. Hadamard codes in Section 2.6).

(ii) Reed-Muller codes can be defined in terms of Boolean functions. Let  $v_1, \dots, v_m$  be  $m$  variables taking the values 0 or 1, and  $f(v_1, \dots, v_m)$  be a Boolean function. Such a function can be expressed as a sum of terms taken among

$$1, v_1, \dots, v_m, v_1v_2, v_1v_3, \dots, v_{m-1}v_m, \dots, v_1v_2 \dots v_m. \quad (9.1.3)$$

The maximal number of variables in a summand is called the *degree* of the Boolean function. Now, let  $\mathbf{v} = (v_1, \dots, v_m)$  denote a vector which ranges over the columns of  $\mathbf{E}_m$ . Then  $f(\mathbf{v})$  is a  $2^m$ -tuple. The collection  $\{f(\mathbf{v})\}$ , where  $f$  ranges over all functions of degree  $r$  or less, is, by definition,  $\mathcal{RM}(r, m)$ . The code thus defined is clearly linear.

Using this definition, the following properties of Reed-Muller codes can be easily established.

The Reed-Muller codes are nested, i.e.,  $\mathcal{RM}(r-1, m) \subset \mathcal{RM}(r, m)$ . The dual of  $\mathcal{RM}(r, m)$  is  $\mathcal{RM}(m-r-1, m)$ , for  $0 \leq r \leq m-1$ .

Let us mention some particular cases of Reed-Muller codes:

$\mathcal{RM}(0, m)$  consists of the all-zero and the all-one vectors;

$\mathcal{RM}(m-2, m)$  coincides with the extended Hamming code;

$\mathcal{RM}(m-1, m)$  consists of all even binary  $n$ -tuples;

$\mathcal{RM}(m, m)$  is the entire space of  $n$ -tuples.

(iii) Yet another way to present a generator matrix of  $\mathcal{RM}(r, m)$  is to notice that the relevant subset of vectors from (9.1.3) constitutes a basis of the code. Thus, we form the generator matrix from  $\mathbf{E}_m$  by taking all possible componentwise products of  $r$  or fewer rows. Actually, we may change the order of the  $m$ -tuples in  $\mathbf{E}_m$ ; let  $\alpha$  be a primitive element of  $\mathbb{F}^m$ , then order the nonzero  $m$ -tuples as follows:

$$\alpha^0, \alpha^1, \dots, \alpha^{2^m-2}.$$

Let  $\mathbf{F}_m^*$  stand for the corresponding  $m \times (2^m - 1)$  matrix. Now, the set  $\{f(\mathbf{v})\}$ , where  $f$  ranges over all Boolean functions of degree  $r$  or less and  $\mathbf{v}$  ranges over the columns of  $\mathbf{F}_m^*$ , constitutes the punctured Reed-Muller code  $\mathcal{RM}^*(r, m)$ . It is a cyclic code with zeros  $\alpha^i$  for all  $i$  such that  $1 \leq i \leq 2^m - 2$  and  $1 \leq w_2(i) \leq m - r - 1$ , where  $w_2(i)$  is the number of ones in the binary expansion of  $i$ .

It is a difficult problem to determine the distance distribution of general Reed-Muller codes. For the first order Reed-Muller codes,  $\mathcal{B}_0 = \mathcal{B}_n = 1$ ,  $\mathcal{B}_{2^{m-1}} = 2^{m+1} - 2$ . For the second order Reed-Muller codes,  $\mathcal{B}_i \neq 0$  only for  $i = 0, 2^{m-1}, 2^m$ , and  $i = 2^{m-1} \pm 2^{m-1-h}$  for  $1 \leq h \leq \lfloor m/2 \rfloor$ , and

$$\mathcal{B}_0 = \mathcal{B}_n = 1;$$

$$\mathcal{B}_{2^{m-1} \pm 2^{m-1-h}} = 2^{h(h+1)} \cdot \frac{(2^m-1)(2^{m-1}-1)\dots(2^{m-2h+1}-1)}{(2^{2h}-1)(2^{2h-2}-1)\dots(2^2-1)} \quad \text{for } h \in [1, \lfloor m/2 \rfloor];$$

$$\mathcal{B}_{2^{m-1}} = 2^{k(2,m)} - \sum_{i \neq 2^{m-1}} \mathcal{B}_i.$$

The distance distributions of  $\mathcal{RM}(r, m)$  for  $r \leq 2$  determine those of their duals,  $\mathcal{RM}(m-2, m)$  and  $\mathcal{RM}(m-3, m)$ , via MacWilliams transform.

For codes of arbitrary order, only low-weight components of the distance distributions are known, but no general results so far. There are large gaps in the distance distribution of Reed-Muller codes, partly explained by the next theorem.

**Theorem 9.1.4** *All the weights in  $\mathcal{RM}(r, m)$  are multiples of  $2^{\lfloor (m-1)/r \rfloor}$ .*

**Proof.** We use the definition of Reed-Muller codes in terms of Boolean functions. Let  $f$  be a function of degree  $r$  in  $m$  variables  $v_1, \dots, v_m$ , and let  $f = f_1 + f_2 + \dots + f_s$ , where the  $f_i$ 's are monomials. Let  $\mathbf{f}$  be the  $2^m$ -tuple corresponding to the function  $f$ . Denote

$$S(f) = \sum_{v_1, \dots, v_m \in \mathbb{F}} (-1)^f.$$

Since for  $a \in \mathbb{F}$  we evidently have  $(-1)^a = 1 - 2a$ , then

$$S(f) = 2^m - 2w(\mathbf{f}). \quad (9.1.5)$$

Furthermore,

$$\begin{aligned} S(f) &= \sum_{v_1, \dots, v_m \in \mathbb{F}} (-1)^{f_1 + \dots + f_s} = \sum_{v_1, \dots, v_m \in \mathbb{F}} \prod_{i=1}^s (1 - 2f_i) \\ &= \sum_{v_1, \dots, v_m \in \mathbb{F}} \left( 1 + \sum_{j=1}^s (-2)^j \sum_{1 \leq i_1 < \dots < i_j \leq s} f_{i_1} \dots f_{i_j} \right) \\ &= 2^m + \sum_{j=1}^s \left( (-1)^j 2^j \sum_{1 \leq i_1 < \dots < i_j \leq s} \sum_{v_1, \dots, v_m \in \mathbb{F}} f_{i_1} \dots f_{i_j} \right). \end{aligned}$$

Denote by  $f(i_1, \dots, i_j) = f^*$  the monomial obtained from  $f_{i_1} \dots f_{i_j}$  after the reductions  $v_i^2 = v_i$ . Let  $r(i_1, \dots, i_j) = r^*$  stand for the degree of  $f^*$ , and assume  $I(i_1, \dots, i_j) = I^*$  is the subset of variables  $v_1, \dots, v_m$  occurring in  $f^*$ ,  $|I^*| = r^*$ . Then

$$\sum_{v_1, \dots, v_m \in \mathbb{F}} f^* = 2^{m-r^*},$$

and  $S(f)$  is divisible by  $2^{m-r^*+j}$ . Moreover,  $m-r^*+j \geq m-r^*+\lceil r^*/r \rceil$ , because the smallest number of monomials of degree at most  $r$  whose product can have degree  $r^*$  is  $\lceil r^*/r \rceil$ . Clearly the minimum is achieved when  $r^* = m$ , i.e.,  $f^* = v_1 \dots v_m$ . Hence  $S(f)$  is divisible by  $2^{\lceil m/r \rceil}$ . Use of (9.1.5) completes the proof.  $\square$

Let  $R_{RM}(r, m)$  denote the covering radius of  $\mathcal{RM}(r, m)$ . We clearly have  $R_{RM}(0, m) = 2^{m-1}$ ,  $R_{RM}(m, m) = 0$ ,  $R_{RM}(m-1, m) = 1$ ,  $R_{RM}(m-2, m) = 2$ . The last expression follows from the perfectness of Hamming codes, and the simple remark that extending a code increases its covering radius by one. So much for the easy cases.

## 9.2 First order Reed-Muller codes

In this section we estimate the covering radius of first order Reed-Muller and related codes. We start with the simple case of simplex codes.

**Theorem 9.2.1** *The covering radius of simplex codes  $\mathcal{SIM}_m$  is  $2^{m-1} - 1$ .*

**Proof.** Recall from Section 2.6 that  $\mathcal{SIM}_m$  is the shortened  $\mathcal{RM}(1, m)$ . It is also the dual of the Hamming code  $\mathcal{H}_m$ , so its dual distance is three. Applying Theorem 8.3.14 we upperestimate the covering radius as  $\lfloor n/2 \rfloor = 2^{m-1} - 1$ . Since all the nonzero codewords have weight  $2^{m-1}$ , the all-one vector is at distance  $2^{m-1} - 1$  from  $\mathcal{SIM}_m$ .  $\square$

Now, we consider  $R_{RM}(1, m)$ . For an upper bound on  $R_{RM}(1, m)$ , one could use the second Norse bound (see Theorem 8.3.13) proved in Section 8.3. However, we prefer to give here an alternative self-contained proof of what is actually needed.

**Theorem 9.2.2** *The covering radius of a binary, self-complementary code of length  $n$  and dual distance greater than two, is at most  $\lfloor \frac{1}{2}(n - \sqrt{n}) \rfloor$ .*

**Proof.** We use here the  $(-1, 1)$  notation, i.e., a binary 0-1 vector  $\mathbf{x}$  is mapped to the vector  $\mathbf{x}^\pm$  by changing 1's to  $-1$ 's and 0's to  $+1$ 's. Notice that for binary vectors  $\mathbf{x}$  and  $\mathbf{y}$  of length  $n$ ,

$$d(\mathbf{x}, \mathbf{y}) = \frac{1}{2}(n - \langle \mathbf{x}^\pm, \mathbf{y}^\pm \rangle). \quad (9.2.3)$$

Suppose that the code  $C$  consists of the words  $\mathbf{c}_1, \dots, \mathbf{c}_K$ . For an arbitrary vector  $\mathbf{x}^\pm$  we calculate the sum

$$\sum_{i=1}^K \langle \mathbf{x}^\pm, \mathbf{c}_i^\pm \rangle^2 = \sum_{i=1}^K \left( \sum_{j=1}^n x_j^\pm c_{i,j}^\pm \right)^2$$

$$\begin{aligned}
&= \sum_{i=1}^K \sum_{j,l=1}^n x_j^\pm c_{i,j}^\pm x_l^\pm c_{i,l}^\pm \\
&= \sum_{j,l=1}^n x_j^\pm x_l^\pm \sum_{i=1}^K c_{i,j}^\pm c_{i,l}^\pm.
\end{aligned}$$

Since the code has dual distance greater than two, it has strength at least two (see the last paragraph of Section 2.2) and on any two columns, each of the 2-tuples  $(-1, -1)$ ,  $(-1, 1)$ ,  $(1, -1)$ ,  $(1, 1)$ , appears exactly  $K/4$  times in  $C$ . Hence

$$\sum_{i=1}^K c_{i,j}^\pm c_{i,l}^\pm = \begin{cases} 0 & \text{if } j \neq l \\ K & \text{if } j = l. \end{cases}$$

Therefore,

$$\sum_{i=1}^K \langle \mathbf{x}^\pm, \mathbf{c}_i^\pm \rangle^2 = Kn. \quad (9.2.4)$$

Hence, there exists an index  $i$ ,  $1 \leq i \leq K$ , such that  $|\langle \mathbf{x}^\pm, \mathbf{c}_i^\pm \rangle| \geq \sqrt{n}$ . The code  $C$  is self-complementary, and, replacing  $\mathbf{c}$  by its complement if necessary, we may assume that  $\langle \mathbf{x}^\pm, \mathbf{c}_i^\pm \rangle \geq \sqrt{n}$ . Therefore

$$d(\mathbf{x}, \mathbf{c}_i) \leq (n - \sqrt{n})/2$$

by (9.2.3). □

**Corollary 9.2.5** *For  $m \geq 2$ ,  $R_{RM}(1, m) \leq 2^{m-1} - 2^{(m-2)/2}$ .*

**Proof.** The code  $\mathcal{RM}(1, m)$  is self-complementary (it contains the all-one vector), and has  $d^\perp = 4$ , the minimum distance of  $\mathcal{RM}(1, m)^\perp = \mathcal{RM}(m-2, m) = \widehat{\mathcal{H}}_m$ . □

To get a lower bound on  $R_{RM}(1, m)$  we derive an induction for covering radii of  $\mathcal{RM}(1, m)$  and  $\mathcal{RM}(1, m+2)$ .

**Lemma 9.2.6** *For  $m \geq 3$ ,*

$$R_{RM}(1, m) \geq 2R_{RM}(1, m-2) + 2^{m-2}.$$

**Proof.** We return to the conventional 0-1 notation, and let  $\bar{\mathbf{c}}$  be the complement of  $\mathbf{c}$ . From the inductive definition (9.1.1), the codewords of  $\mathcal{RM}(1, m)$  are of one of the following types:

$$(\mathbf{v}, \mathbf{v}, \mathbf{v}, \mathbf{v}), (\mathbf{v}, \bar{\mathbf{v}}, \bar{\mathbf{v}}, \mathbf{v}), (\mathbf{v}, \bar{\mathbf{v}}, \mathbf{v}, \bar{\mathbf{v}}), (\mathbf{v}, \mathbf{v}, \bar{\mathbf{v}}, \bar{\mathbf{v}}), \quad (9.2.7)$$

where  $\mathbf{v} \in \mathcal{RM}(1, m-2)$ . Consider a deep hole,  $\mathbf{x}$ , for  $\mathcal{RM}(1, m-2)$ , i.e.,

$$d(\mathbf{v}, \mathbf{x}) \geq R_{RM}(1, m-2)$$

for all  $\mathbf{v} \in \mathcal{RM}(1, m-2)$ . Because  $\mathcal{RM}(1, m-2)$  is self-complementary,  $\bar{\mathbf{x}}$  is also a deep hole. Notice that

$$d(\mathbf{x}, \bar{\mathbf{v}}) = d(\bar{\mathbf{x}}, \mathbf{v}) = 2^{m-2} - d(\mathbf{x}, \mathbf{v}) = 2^{m-2} - d(\bar{\mathbf{x}}, \bar{\mathbf{v}}).$$

Next, consider the vector  $\mathbf{y} = (\mathbf{x}, \mathbf{x}, \mathbf{x}, \bar{\mathbf{x}})$  of length  $2^m$ . Depending on the membership of a codeword  $\mathbf{c} \in \mathcal{RM}(1, m)$  to one of the four types in (9.2.7), we get

$$d(\mathbf{y}, \mathbf{c}) = 3d(\mathbf{x}, \mathbf{v}) + d(\bar{\mathbf{x}}, \mathbf{v}) = 2^{m-2} + 2d(\mathbf{x}, \mathbf{v}),$$

or

$$d(\mathbf{y}, \mathbf{c}) = d(\mathbf{x}, \mathbf{v}) + 3d(\bar{\mathbf{x}}, \mathbf{v}) = 2^{m-2} + 2d(\mathbf{x}, \bar{\mathbf{v}}).$$

In all cases,  $d(\mathbf{y}, \mathbf{c}) \geq 2^{m-2} + 2R_{RM}(1, m-2)$ .  $\square$

Now, we have  $R_{RM}(1, 1) = 0$  and  $R_{RM}(1, 2) = 1$ , thus yielding

$$R_{RM}(1, m) \geq 2^{m-1} - 2^{(m-2)/2}$$

for even  $m$ , and

$$R_{RM}(1, m) \geq 2^{m-1} - 2^{(m-1)/2}, \quad (9.2.8)$$

for odd  $m$ . Using Corollary 9.2.5, we determine the covering radius of the first order Reed-Muller codes when  $m$  is even.

**Theorem 9.2.9** *For even  $m$ ,*

$$R_{RM}(1, m) = 2^{m-1} - 2^{(m-2)/2}.$$

For odd  $m$  the situation is much more complicated. To analyze the problem we relate it to the existence of some linear codes.

**Lemma 9.2.10** *For  $m$  odd,  $m > 3$ , the covering radius of  $\mathcal{RM}(1, m)$  is  $t$  if and only if  $t$  is the maximal integer such that there exists a  $[t, m+1, d \geq t - 2^{m-2}]$  self-complementary code  $C_0$  with a generator matrix where all columns are nonzero and distinct ( $d^\perp \geq 3$ ).*

**Proof.** Let  $\mathbf{x}$  be a deep hole of weight  $t$ . The support of  $\mathbf{x}$  selects  $t$  columns from  $\mathbf{G}(1, m)$ , the generator matrix of  $\mathcal{RM}(1, m)$ . Let  $\mathbf{G}_0$  denote the  $(m+1) \times t$  matrix formed by these columns, and let  $C_0$  be the code generated by  $\mathbf{G}_0$ . Up to a permutation of columns,  $\mathbf{x} = (1^t, 0^{n-t})$  and  $\mathbf{G}(1, m) = (\mathbf{G}_0, \mathbf{G}_1)$ . We represent codewords  $\mathbf{c} \in \mathcal{RM}(1, m)$  as  $(\mathbf{c}_0, \mathbf{c}_1)$  where the two parts are of

lengths  $t$  and  $2^m - t$ . Let  $\mathbf{c}$  be a codeword of  $\mathcal{RM}(1, m)$  different from the all-zero and all-one vectors. Then

$$w(\mathbf{c}) = w(\mathbf{c}_0) + w(\mathbf{c}_1) = 2^{m-1} \quad (9.2.11)$$

and

$$d(\mathbf{x}, \mathbf{c}) = t - w(\mathbf{c}_0) + w(\mathbf{c}_1) \geq t.$$

Thus,  $w(\mathbf{c}_1) \geq w(\mathbf{c}_0)$ , and from (9.2.11) we get

$$w(\mathbf{c}_0) \leq 2^{m-2}.$$

Since  $\bar{\mathbf{c}}$  belongs to  $\mathcal{RM}(1, m)$ , so does  $\bar{\mathbf{c}}_0$  to  $C_0$ . Evidently,  $w(\bar{\mathbf{c}}_0) \geq t - 2^{m-2}$ . Hence, the weight of any codeword of  $C_0$  is at least  $t - 2^{m-2}$  and at most  $2^{m-2}$ , or equals 0 or  $t$ . Therefore, the minimum distance of  $C_0$  is at least  $t - 2^{m-2}$ . By (9.2.8),  $t - 2^{m-2} > 0$  for  $m > 3$ , so the code  $C_0$  has full dimension  $m+1$  and  $\mathbf{G}_0$  clearly cannot have identical columns. The converse statement is proved by reversing the previous argument.  $\square$

To see how the above lemma works, consider the case of  $\mathcal{RM}(1, 5)$ . From (9.2.8) we get  $R_{RM}(1, 5) \geq 12$ . If  $R_{RM}(1, 5) \geq 13$ , then there exists a linear  $[13, 6, d \geq 5]$  code. But the existence of this code would imply by Lemma 8.1.11 the existence of a  $[8, 5, d \geq 3]$  code, contradicting the Hamming bound.

To prove that  $R_{RM}(1, 7) = 56$ , it is sufficient to rule out the existence of a self-complementary  $[57, 8, d \geq 25]$  code. Actually, a linear code with these parameters does exist, but cannot be self-complementary.

**Theorem 9.2.12**  $R_{RM}(1, 7) = 56$ .  $\square$

Relying on numerical evidence, it was tempting to conjecture that the lower bound  $2^{m-1} - 2^{(m-1)/2}$  is tight for odd  $m$ . This was disproved for  $m = 15$ . Namely, it is possible to exhibit a vector at distance  $16\ 276 = 2^{14} - 2^7 + 20$  from  $\mathcal{RM}(1, 15)$ . All these results and Lemma 9.2.6 allow us to formulate the following theorem.

**Theorem 9.2.13** For  $m$  odd,

$$R_{RM}(1, m) = \begin{cases} 2^{m-1} - 2^{(m-1)/2} \\ \text{for } m = 1, 3, 5, 7; \end{cases}$$

$$2^{m-1} - 2^{(m-1)/2} \leq R_{RM}(1, m) \leq 2^{m-1} - 2^{(m-2)/2} \\ \text{for } m = 9, 11, 13;$$

$$2^{m-1} - (27/32) \cdot 2^{(m-1)/2} \leq R_{RM}(1, m) \leq 2^{m-1} - 2^{(m-2)/2} \\ \text{for } m \geq 15. \quad \square$$

Before considering the normality of  $\mathcal{RM}(1, m)$ , we give two conjectures on  $R_{RM}(1, m)$ .

**Conjecture 9.2.14**

$$\lim_{m \rightarrow \infty} \frac{2^{m-1} - R_{RM}(1, m)}{2^{(m-2)/2}} = 1.$$

**Conjecture 9.2.15** For  $m \geq 3$ ,  $R_{RM}(1, m)$  is even.

**Theorem 9.2.16** A binary, self-complementary code of length  $n$  and dual distance greater than two has norm  $[n - \sqrt{n-1}]$ .

**Proof.** Let  $\mathbf{x} \in \mathbb{F}^n$  be given. By symmetry, we may assume that the first coordinate of  $\mathbf{x}$  is 0. Let  $\mathbf{c}_1, \dots, \mathbf{c}_{K/2}$  be the codewords that begin with 0 and  $\mathbf{c}_{(K/2)+1}, \dots, \mathbf{c}_K$  be their complements. Denote

$$s_i = \langle \mathbf{x}^\pm, \mathbf{c}_i^\pm \rangle.$$

Then

$$\begin{aligned} d(\mathbf{x}, C_0^{(1)}) &= \frac{n}{2} - \frac{1}{2} \max_{1 \leq i \leq K/2} s_i, \\ d(\mathbf{x}, C_1^{(1)}) &= \frac{n}{2} - \frac{1}{2} \max_{(K/2)+1 \leq i \leq K} s_i = \frac{n}{2} + \frac{1}{2} \min_{1 \leq i \leq K/2} s_i. \end{aligned}$$

Thus, the claim is correct if

$$\begin{aligned} d(\mathbf{x}, C_0^{(1)}) + d(\mathbf{x}, C_1^{(1)}) \\ = n - \frac{1}{2} \left( \max_{1 \leq i \leq K/2} s_i - \min_{1 \leq i \leq K/2} s_i \right) \leq n - \sqrt{n-1}. \end{aligned} \quad (9.2.17)$$

All the codewords  $\mathbf{c}_1, \dots, \mathbf{c}_{K/2}$  begin with 0 and in every other coordinate  $i$ , both 0 and 1 occur equally often. Hence

$$\begin{aligned} \sum_{i=1}^{K/2} s_i &= \sum_{i=1}^{K/2} \langle \mathbf{x}^\pm, \mathbf{c}_i^\pm \rangle = \sum_{i=1}^{K/2} \sum_{j=1}^n x_j^\pm c_{i,j}^\pm \\ &= \sum_{j=1}^n x_j^\pm \sum_{i=1}^{K/2} c_{i,j}^\pm = x_1^\pm \sum_{i=1}^{K/2} c_{i,1}^\pm = \frac{1}{2} K. \end{aligned}$$

In the proof of Theorem 9.2.2 we saw that

$$\sum_{i=1}^{K/2} s_i^2 = \frac{1}{2} K n.$$

Let us introduce new variables  $y_i = s_i - 1$  for  $i = 1, \dots, K/2$ . We have

$$\sum_{i=1}^{K/2} y_i = 0, \quad (9.2.18)$$

$$\sum_{i=1}^{K/2} y_i^2 = \frac{1}{2} K(n-1). \quad (9.2.19)$$

Let  $a$  be the largest and  $-b$  the smallest among the integers  $y_i$ . Then (9.2.17) is true if  $a + b \geq 2\sqrt{n-1}$ . Denote

$$S = \sum_{y_i > 0} |y_i| = \sum_{y_i < 0} |y_i|.$$

Then

$$\left(\frac{4S}{K}\right)^2 = \left(\frac{2}{K} \sum_{i=1}^{K/2} |y_i|\right)^2 \leq \frac{2}{K} \sum_{i=1}^{K/2} |y_i|^2 = n-1,$$

and consequently,

$$K\sqrt{n-1} \geq 4S. \quad (9.2.20)$$

Furthermore,

$$\begin{aligned} \frac{1}{2} K(n-1) &= \sum_{i=1}^{K/2} y_i^2 = \sum_{y_i > 0} y_i^2 + \sum_{y_i < 0} y_i^2 \\ &\leq \frac{S}{a} a^2 + \frac{S}{b} b^2 = S(a+b), \end{aligned}$$

and therefore

$$a+b \geq \frac{K}{2S}(n-1) \geq 2\sqrt{n-1}$$

by (9.2.20).  $\square$

This theorem implies that the codes attaining the second Norse bound are normal.

**Corollary 9.2.21** *If a binary, self-complementary code of length  $n$  and dual distance greater than two has covering radius  $\lfloor \frac{1}{2}(n-\sqrt{n}) \rfloor$ , then it is normal.*

**Proof.** It is sufficient to verify that

$$\lfloor n - \sqrt{n-1} \rfloor \leq 2 \lfloor \frac{1}{2}(n-\sqrt{n}) \rfloor + 1. \quad (9.2.22)$$

If  $n-1$  is not a square, then  $\lfloor n - \sqrt{n-1} \rfloor = \lfloor n - \sqrt{n} \rfloor$  and the claim follows because  $\lfloor y \rfloor \leq 2\lfloor \frac{1}{2}y \rfloor + 1$  for any real number  $y$ . If  $n-1$  is a square, then (9.2.22) holds with equality.  $\square$

**Corollary 9.2.23** *The codes  $\mathcal{RM}(1, m)$  are normal for even  $m$ .*  $\square$

For odd  $m$  the situation is more complicated since we do not know the exact value of the covering radius, and only the first cases are settled.

**Theorem 9.2.24**  *$\mathcal{RM}(1, 3)$ ,  $\mathcal{RM}(1, 5)$  and  $\mathcal{RM}(1, 7)$  are normal.*  $\square$

### 9.3 Reed-Muller codes of order 2 and $m-3$

The codes  $\mathcal{RM}(2, m)$  and  $\mathcal{RM}(m-3, m)$  are dual of each other. The weight distribution of  $\mathcal{RM}(2, m)$  is known (see Section 9.1).

We use the following simple but essential lemma.

**Lemma 9.3.1**

$$2R_{RM}(r, m-1) \leq R_{RM}(r, m), \quad (9.3.2)$$

$$R_{RM}(r-1, m-1) \leq R_{RM}(r, m), \quad (9.3.3)$$

$$R_{RM}(r, m) \leq R_{RM}(r, m-1) + R_{RM}(r-1, m-1). \quad (9.3.4)$$

**Proof.** Reed-Muller codes are inductively defined in (9.1.1) by

$$\mathcal{RM}(r, m) = \{(\mathbf{u}, \mathbf{u} + \mathbf{v}) : \mathbf{u} \in \mathcal{RM}(r, m-1), \mathbf{v} \in \mathcal{RM}(r-1, m-1)\}.$$

Since  $\mathcal{RM}(r-1, m-1) \subset \mathcal{RM}(r, m-1)$ , we have  $\mathbf{u} + \mathbf{v} \in \mathcal{RM}(r, m-1)$ . Let  $\mathbf{x}$  be a deep hole in  $\mathcal{RM}(r, m-1)$ . Then  $(\mathbf{x}, \mathbf{x})$  guarantees (9.3.2). To prove (9.3.3), consider a vector  $(\mathbf{0}, \mathbf{y})$  where  $\mathbf{0}$  has length  $2^{m-1}$  and  $\mathbf{y}$  is a deep hole of  $\mathcal{RM}(r-1, m-1)$ . We have

$$d((\mathbf{u}, \mathbf{u} + \mathbf{v}), (\mathbf{0}, \mathbf{y})) = w(\mathbf{u}) + d(\mathbf{u} + \mathbf{v}, \mathbf{y})$$

$$\geq w(\mathbf{u}) + d(\mathbf{v}, \mathbf{y}) - w(\mathbf{u}) = d(\mathbf{v}, \mathbf{y}) \geq R_{RM}(r-1, m-1),$$

proving (9.3.3). The last claim immediately follows from Theorem 3.4.1.  $\square$

We start by considering the covering radius of  $\mathcal{RM}(2, m)$ . Clearly,

$$R_{RM}(2, 2) = 0, R_{RM}(2, 3) = 1, R_{RM}(2, 4) = 2.$$

Consider  $R_{RM}(2, 5)$ . By (9.3.3) we have  $R_{RM}(2, 5) \geq 6$ . The code  $\mathcal{RM}(2, 5)$  is a doubly-even self-dual code, so it has nonzero components  $\mathcal{B}_i = \mathcal{B}_i^\perp$  only for  $i = 0, 8, 12, 16, 20, 24, 32$ . The Delsarte bound (Theorem 8.3.7) then gives the upper bound of 6, yielding  $R_{RM}(2, 5) = 6$ .

Since  $R_{RM}(1, 5) = 12$ , from (9.3.4) we infer that  $R_{RM}(2, 6) \leq 18$ . Actually, the 64-tuple associated to the polynomial

$$\begin{aligned} v_6(v_1v_2v_3 + v_1v_4v_5 + v_2v_3 + v_2v_4 + v_3v_5) \\ + (v_6 + 1)(v_1v_2v_3 + v_1v_4v_5) \end{aligned} \quad (9.3.5)$$

has been verified to be at distance at least 18 from any codeword of  $\mathcal{RM}(2, 6)$ . Hence,  $R_{RM}(2, 6) = 18$ . Already the value of  $R_{RM}(2, 7)$  is unknown.

Using arguments similar to those of Lemma 9.2.10 it is possible to prove the following generalization for the second order Reed-Muller codes.

**Lemma 9.3.6** *For  $m \geq 6$ ,  $R_{RM}(2, m) = t$  if and only if  $t$  is the maximal integer such that there exists a self-complementary  $[t, m+1, d \geq t - R_{RM}(1, m-1)]$  code with a generator matrix where all columns are distinct and nonzero.*  $\square$

We now discuss the covering radius of  $\mathcal{RM}(m-3, m)$ . Although knowledge of the number of nonzero weights in  $\mathcal{RM}(2, m)$  along with the Delsarte theorem gives us a tight upper bound on  $R_{RM}(m-3, m)$ , we prefer another approach which allows us to present the lower and upper bounds in a uniform way.

Consider the covering radius of the punctured Reed-Muller code  $\mathcal{RM}^*(m-3, m)$ , i.e., the code with a parity check matrix  $\mathbf{H}$  coinciding with the parity check matrix of  $\mathcal{RM}(m-3, m)$  without the first all-one row and the first column. Clearly  $\mathbf{H}$  has as its rows the vectors associated to the functions  $v_1, \dots, v_m, v_1v_2, v_1v_3, \dots, v_{m-1}v_m$ , where the first (zero) coordinate is deleted. The syndrome  $\mathbf{s}$  of a vector  $\mathbf{x}$  is the product  $\mathbf{s} = \mathbf{H}\mathbf{x}^T$ . Let us present the syndrome  $\mathbf{s}$  as the  $m \times m$  symmetric matrix  $\mathbf{S}$  having as  $s_{i,j}$  the component of the syndrome corresponding to the row  $v_i v_j$  of  $\mathbf{H}$ . On the diagonal the matrix has  $s_{i,i}$  corresponding to the row  $v_i$  of  $\mathbf{H}$ . There is a one-to-one correspondence between the cosets of  $\mathcal{RM}^*(m-3, m)$  and the syndrome matrices  $\mathbf{S}$ , i.e., all symmetric binary matrices.

Notice that the row of  $\mathbf{H}$  corresponding to  $v_i v_j$  is the componentwise product of the  $i$ -th and  $j$ -th rows  $\mathbf{e}_i^*$  and  $\mathbf{e}_j^*$  of  $\mathbf{E}_m^*$ . Define  $\mathbf{B}$  as the matrix whose  $i$ -th row is the componentwise product  $\mathbf{e}_i^* * \mathbf{x}$  for  $i \in [1, m]$ . Then

$$\mathbf{S} = \mathbf{B}\mathbf{B}^T.$$

The number of nonzero columns in  $\mathbf{B}$  equals  $w(\mathbf{x})$  since the nonzero columns in  $\mathbf{B}$  are only on the positions of the support of  $\mathbf{x}$ .

Given a binary symmetric matrix  $\mathbf{S}$ , a matrix  $\mathbf{A}$  such that  $\mathbf{A}\mathbf{A}^T = \mathbf{S}$  is called a *factor* of  $\mathbf{S}$ . Denote by  $t(\mathbf{S})$  the minimal number of columns in its factor. We have reduced our problem to the following:

**Lemma 9.3.7** *The covering radius of  $\mathcal{RM}^*(m - 3, m)$  equals the maximum value of  $t(\mathbf{S})$  over all binary symmetric matrices  $\mathbf{S}$  of size  $m \times m$ .  $\square$*

Since  $t(\mathbf{S}) \geq \text{rank}(\mathbf{S})$ , an immediate lower bound for the maximum value of  $t(\mathbf{S})$  is  $m$ . Notice that

$$s_{i,i} = \sum_j b_{i,j},$$

i.e., the vector consisting of the diagonal elements of  $\mathbf{S}$  is the sum of the columns of  $\mathbf{B}$ . So, if  $\mathbf{S}$  has full rank and all-zero diagonal, then all the columns of  $\mathbf{B}$  sum up to the all-zero column and in this case  $t(\mathbf{S}) \geq m + 1$ . The symmetric matrices having all-zero diagonal can be of full rank only for  $m$  even.

Indeed, for such an  $m \times m$  matrix  $\mathbf{A} = (a_{i,j})$ ,

$$\det(\mathbf{A}) = \sum_{\sigma} \prod_{i=1}^m a_{i,\sigma(i)},$$

where the sum extends over all permutations  $\sigma$  of  $[1, m]$ . If  $\sigma = \sigma^{-1}$ , i.e.,  $\sigma^2$  is the identity permutation, then, when  $m$  is odd, there is necessarily an index  $i_0 \in [1, m]$  such that  $i_0 = \sigma(i_0)$ . Since  $a_{i_0, i_0} = 0$  by definition,  $\prod_{i=1}^m a_{i,\sigma(i)} = 0$ . The other permutations can be grouped into pairs  $(\sigma, \sigma^{-1})$  with  $\sigma \neq \sigma^{-1}$ . By the symmetry of  $\mathbf{A}$ ,

$$\prod_{i=1}^m a_{i,\sigma(i)} = \prod_{i=1}^m a_{\sigma(i),i},$$

hence

$$\prod_{i=1}^m a_{i,\sigma(i)} + \prod_{i=1}^m a_{\sigma(i),i} = 0.$$

As an example of a full rank matrix of even dimension, choose the matrix having ones on the second diagonal, and zeros elsewhere.

Summarizing:

$$\max t(\mathbf{S}) \geq m + 1 - \pi(m), \quad (9.3.8)$$

where

$$\pi(m) = \begin{cases} 0 & \text{if } m \text{ is even} \\ 1 & \text{otherwise.} \end{cases}$$

To prove that actually this bound is tight, we show that if some factor  $\mathbf{A}$  of  $\mathbf{S}$  has a proper subset of columns summing up to 0, then the number of columns in the factor can be decreased.

**Lemma 9.3.9** *The following operations do not change the property of  $\mathbf{A}$  being a factor of  $\mathbf{S}$ :*

- (i) *deleting a zero column;*
- (ii) *deleting two equal columns;*
- (iii) *if all the rows of  $\mathbf{A}$  have an even number of ones and  $\mathbf{A}$  has an even number of columns, then any row may be substituted by its complement.*

**Proof.** Routine. □

As a consequence of the previous lemma, if  $\mathbf{A}$  has all rows of even weight (i.e., the sum of its columns is the all-zero vector) and the number of columns of  $\mathbf{A}$  is even, we may complement any subset of the rows while keeping the resulting matrix a factor of  $\mathbf{S}$ . It is easy to see that complementing a subset of rows is the same as adding a fixed vector to every column of the matrix.

Assume now that we have a factor  $\mathbf{A}$  of  $\mathbf{S}$  with a number of columns greater than  $m + 1 - \pi(m)$ . Then  $\mathbf{A}$  evidently has some proper subset  $\mathbf{Q}$  of columns summing up to  $\mathbf{0}$ . Let  $\mathbf{A} = (\mathbf{L}, \mathbf{Q})$ . If the number of columns in  $\mathbf{Q}$  is odd, we adjoin the all-zero column to the matrix  $\mathbf{Q}$ , not changing the sum of the columns of  $\mathbf{Q}$ . Let  $\mathbf{l}_1$  and  $\mathbf{q}_1$  be the first columns of the matrices  $\mathbf{L}$  and  $\mathbf{Q}$ . We construct a modified matrix by adding  $\mathbf{l}_1 + \mathbf{q}_1$  to every column of  $\mathbf{Q}$ . Denote this new matrix by  $(\mathbf{L}, \mathbf{Q}_1)$ . Now,

$$\begin{aligned} (\mathbf{L}, \mathbf{Q}_1)(\mathbf{L}, \mathbf{Q}_1)^T &= \mathbf{L}\mathbf{L}^T + \mathbf{Q}_1\mathbf{Q}_1^T = \mathbf{L}\mathbf{L}^T + \mathbf{Q}\mathbf{Q}^T \\ &= (\mathbf{L}, \mathbf{Q})(\mathbf{L}, \mathbf{Q})^T = \mathbf{A}\mathbf{A}^T = \mathbf{S}. \end{aligned}$$

But  $(\mathbf{L}, \mathbf{Q}_1)$  has two equal columns, namely the first column of  $\mathbf{L}$  and the first column of  $\mathbf{Q}_1$ . Hence, by Lemma 9.3.9-(ii), we may delete them. Actually, we have proved that we may decrease the number of columns in a factor of  $\mathbf{S}$  by one or two, depending on the parity of the number of columns in the chosen proper subset of columns of the factor. Hence, by (9.3.8) we have

**Lemma 9.3.10**  $\max t(\mathbf{S}) = m + 1 - \pi(m)$ . □

Now, combining Lemmas 9.3.7 and 9.3.10 with the fact that  $R_{RM}(m - 3, m)$  is the covering radius of  $\mathcal{RM}^*(m - 3, m)$  increased by one, we get

**Theorem 9.3.11**

$$R_{RM}(m - 3, m) = \begin{cases} m + 2 & \text{for } m \text{ even,} \\ m + 1 & \text{for } m \text{ odd.} \end{cases}$$

□

## 9.4 Covering radius of Reed-Muller codes of arbitrary order

Table 9.1 gives the best known bounds for  $R_{RM}(r, m)$ ,  $1 \leq r \leq m \leq 9$ . The table exploits the inequalities (9.3.2) and (9.3.3). However, it is possible to do better than just repeatedly using (9.3.2) and (9.3.3). The proofs of the following two lemmas are quite technical and are omitted.

**Lemma 9.4.1** *If  $2 \leq k \leq m - r - 1$ , then*

$$R_{RM}(r + k, m + k) \geq R_{RM}(r, m) + 2(k - 1). \quad (9.4.2)$$

Moreover, if  $m - r \geq 4$  and  $\mathcal{RM}(r, m)$  has a coset with minimal weight  $R_{RM}(r, m)$  which does not contain any vector of weight  $R_{RM}(r, m) + 2$ , then

$$R_{RM}(r + k, m + k) \geq R_{RM}(r, m) + 2k. \quad (9.4.3)$$

□

**Example 9.4.4**  $R_{RM}(4, 8) \geq 22$  since  $\mathcal{RM}(2, 6)$  has the coset (9.3.5) with minimal weight 18 which, as can be verified by computer, does not contain any vector of weight 20. □

**Lemma 9.4.5** *For  $r \leq m - 2$ ,*

$$R_{RM}(r + 1, m + 2) \geq 2R_{RM}(r, m) + 2. \quad (9.4.6)$$

□

Although for finite lengths there are still many unknown exact values, for long Reed-Muller codes one can derive reasonably tight bounds. The lower bound is simply the sphere-covering one. The upper bound is derived from a thorough use of inequality (9.3.4) with properly chosen initial conditions. Let here  $R$  stand for  $R_{RM}(r, m)$  if it does not lead to confusion. We let  $m \rightarrow \infty$ , and consider separately several cases according to the relationship between  $r$  and  $m$ . Let  $\log$  stand for the binary logarithm and recall that the entropy function is  $H(x) := -x \log x - (1 - x) \log(1 - x)$ , for  $0 \leq x \leq 1$ .

**Lower bounds.** Since  $k(r, m) = V(m, r)$ , the sphere-covering bound reads

$$\log V(2^m, R) \geq 2^m - V(m, r) \quad (9.4.7)$$

Table 9.1: Bounds on the covering radius of Reed-Muller codes.

$r \setminus m$	1	2	3	4	5	6	7	8	9
1	0	1	2	6	12	28	56	120	240–244
2		0	1	2	6	18 <sup>s</sup>	$40^{h1}-44^{h2}$	$84^{h1}-100$	$171^c-220$
3			0	1	2	8	$20^{h1}-23^{h1}$	$43^c-67$	$111^c-167$
4				0	1	2	8	$22^{h1}-31$	$58^c-98$
5					0	1	2	10	$23^c-41$
6						0	1	2	10
7							0	1	2
8								0	1
9									0

For  $r = 1$ , Theorem 9.2.9 ( $m$  even) and Theorem 9.2.13 ( $m$  odd);

for  $r = m - 3$ , Theorem 9.3.11;

all other unmarked upper bounds are from (9.3.4);

$^c$  - sphere-covering bound;

$^{h1}$  - Hou [338];

$^{h2}$  - Hou [339];

<sup>s</sup> - upper bound (9.3.4), lower bound by constructing a deep hole corresponding to the polynomial (9.3.5).

or equivalently

$$\log V(2^m, R) \geq V(m, m - r - 1). \quad (9.4.8)$$

**Case 1**  $m - r = \text{const}$ . In this case, by (9.4.17),  $R \ll 2^m$ . Combining (9.4.8),

$$\log V(2^m, R) = mR(1 + o(1))$$

and

$$V(m, m - r - 1) = \frac{m^{m-r-1}}{(m - r - 1)!} (1 + o(1)),$$

we get

$$R \geq \frac{m^{m-r-2}}{(m - r - 1)!} (1 + o(1)). \quad (9.4.9)$$

**Case 2**  $r = \text{const}$ . By (9.4.7), we have

$$\log V(2^m, R) \geq 2^m - \frac{m^r}{r!} (1 + o(1)). \quad (9.4.10)$$

Let  $\mu < 1/2$  be an arbitrary constant. Then

$$R > \mu 2^m. \quad (9.4.11)$$

Assume on the contrary that  $R \leq \mu 2^m$ . Then (see Lemma 2.4.4)

$$\log V(2^m, R) \leq 2^m H(\mu),$$

contradicting (9.4.10). Now (9.4.11) and (9.4.18) show that  $R/2^m \rightarrow 1/2$ . Combining (9.4.10) and

$$\log V(2^m, R) \leq 2^m H(R/2^m),$$

setting  $y = 1/2 - R/2^m$  and taking into account that  $H(1/2 - y) \leq 1 - 2y^2/(\ln 2)$  when  $y \rightarrow 0$ , we get

$$R \geq 2^{m-1} - 2^{m/2} m^{r/2} ((\ln 2)/(2r!))^{1/2} (1 + o(1)). \quad (9.4.12)$$

**Case 3**  $\alpha := r/m = \text{const} > 1/2$ . In this case, by (9.4.19),  $R \ll 2^m$ . Combining (9.4.8),

$$\log V(2^m, R) = mR(1 + o(1))$$

and

$$V(m, m - r - 1) \geq \frac{1}{\sqrt{2m}} 2^{mH(1-\alpha)} (1 + o(1))$$

(cf. Lemma 2.4.4), we get

$$R \geq (2m^3)^{-1/2} 2^{mH(1-\alpha)} (1 + o(1)). \quad (9.4.13)$$

**Case 4**  $\alpha := r/m = \text{const} < 1/2$ . By (9.4.7),

$$\log V(2^m, R) \geq 2^m - 2^{mH(\alpha)}. \quad (9.4.14)$$

Let  $\mu < 1/2$  be an arbitrary constant. Then

$$R > \mu 2^m. \quad (9.4.15)$$

Assume on the contrary that  $R \leq \mu 2^m$ . Then

$$\log V(2^m, R) \leq 2^m H(\mu),$$

contradicting (9.4.14). Now (9.4.15) and (9.4.20) show that  $R/2^m \rightarrow 1/2$ . Using (9.4.14) and

$$\log V(2^m, R) \leq 2^m H(R/2^m),$$

we get

$$R \geq 2^{m-1} - ((\ln 2)/2)^{1/2} 2^{m(1+H(\alpha))/2} (1 + o(1)). \quad (9.4.16)$$

**Upper bounds.** We use repeatedly (9.3.4).

**Case 1**  $\lambda := m - r = \text{const}$ . We prove by induction on  $\lambda$  that for  $\lambda \geq 3$

$$R_{RM}(r, m) \leq \frac{m^{m-r-2}}{(m-r-2)!} + O(m^{m-r-3}). \quad (9.4.17)$$

The inequality is valid for  $\lambda = 3$  by Theorem 9.3.11. Let it be valid for  $m - r - 1$ . Then

$$\begin{aligned} R_{RM}(r, m) &\leq R_{RM}(r-1, m-1) + R_{RM}(r, m-1) \\ &\leq R_{RM}(r-1, m-1) + \frac{(m-1)^{m-r-3}}{(m-r-3)!} + O(m^{m-r-4}) \\ &\leq \sum_{i=1}^r \frac{(m-i)^{m-r-3}}{(m-r-3)!} + \sum_{i=1}^r O(m^{m-r-4}) + R_{RM}(0, m-r) \\ &= \frac{m^{m-r-2}}{(m-r-2)!} + O(m^{m-r-3}). \end{aligned}$$

**Case 2**  $r = \text{const}$ . We prove by induction on  $r$  that for  $r \geq 2$

$$R_{RM}(r, m) \leq 2^{m-1} - (\sqrt{2} + 1)^{r-1} 2^{(m-2)/2} + O(m^{r-2}). \quad (9.4.18)$$

For  $r = 2$ , using upper bounds on  $R_{RM}(1, m)$ , we have

$$\begin{aligned} R_{RM}(2, m) &\leq R_{RM}(2, m-1) + R_{RM}(1, m-1) \\ &\leq R_{RM}(2, m-1) + 2^{m-2} - 2^{(m-3)/2} \\ &\leq R_{RM}(2, 2) + \sum_{i=1}^{m-2} 2^i - \sum_{i=0}^{m-3} 2^{i/2} \leq 2^{m-1} - (\sqrt{2} + 1) 2^{(m-2)/2} + O(1). \end{aligned}$$

Let (9.4.18) be valid for  $r - 1$ . Then

$$\begin{aligned} R_{RM}(r, m) &\leq R_{RM}(r, m-1) + R_{RM}(r-1, m-1) \\ &\leq R_{RM}(r, m-1) + 2^{m-2} - 2^{(m-3)/2} (\sqrt{2} + 1)^{r-2} + O(m^{r-3}) \\ &\leq R_{RM}(r, r+1) + \sum_{i=r}^{m-2} 2^i - (\sqrt{2} + 1)^{r-2} \sum_{i=r-1}^{m-3} 2^{i/2} + O(m^{r-2}), \end{aligned}$$

yielding (9.4.18). For example, for  $r = 2$ , (9.4.18) becomes

$$R_{RM}(2, m) \leq 2^{m-1} - 1.20 \cdot 2^{m/2} (1 + o(1)).$$

**Case 3**  $\alpha := r/m = \text{const} > 1/2$ . We prove by induction that for  $r \leq m-3$ ,

$$R_{RM}(r, m) \leq \sum_{i=1}^{m-r-2} \binom{m+2}{i}.$$

The inequality holds for  $r = m-3$ , as well as for  $r = 0$ . Let it be valid for  $m-r-1$  and all  $m$ , and for  $m-r$  and all lengths less than  $2^m$ . Then

$$\begin{aligned} R_{RM}(r, m) &\leq \sum_{i=1}^{m-r-2} \binom{m+1}{i} + \sum_{i=1}^{m-r-3} \binom{m+1}{i} \\ &< \sum_{i=1}^{m-r-2} \binom{m+2}{i} \end{aligned}$$

and

$$R_{RM}(r, m) \leq 4^{H(1-\alpha)} 2^{mH(1-\alpha)} (1 + o(1)). \quad (9.4.19)$$

**Case 4**  $\alpha := r/m = \text{const} < 1/2$ . We prove by induction that for  $r \geq 1$ ,  $m \geq 8$ ,

$$R_{RM}(r, m) \leq 2^{m-1} - \binom{m}{r}.$$

The inequality holds for  $m = 8$  and  $r \in [1, 8]$  (see Table 9.1), as well as for  $r = 1$  and  $r = m$  when  $m \geq 8$ . Let it be valid for  $r - 1$  and all  $m$ , and for  $r$  and  $m - 1$ . Then

$$R_{RM}(r, m) \leq 2^{m-2} - \binom{m-1}{r} + 2^{m-2} - \binom{m-1}{r-1} = 2^{m-1} - \binom{m}{r}.$$

This gives (see Lemma 2.4.2):

$$R_{RM}(r, m) \leq 2^{m-1} - (2m)^{-1/2} 2^{mH(\alpha)}. \quad (9.4.20)$$

For  $0 < r/m \leq 1 - \sqrt{2}/2$ , (9.4.21) follows from induction (see [157] for details):

$$R_{RM}(r, m) \leq 2^{m-1} - (\sqrt{2} + 1)^{r-1} 2^{(m-2)/2} + r \binom{m}{r}. \quad (9.4.21)$$

Denoting  $R_{RM}(r, m) = 2^{m-1} - 2^{mf(\alpha)}$  and combining (9.4.16), (9.4.20) and (9.4.21), gives

$$\begin{aligned} & \frac{1}{2}(1 + H(\alpha))(1 + o(1)) \\ & \geq f(\alpha) \geq \begin{cases} \left(\frac{1}{2} + \alpha \log(\sqrt{2} + 1)\right)(1 + o(1)) & 0 < \alpha \leq 1 - \sqrt{2}/2 \approx 0.293; \\ H(\alpha)(1 + o(1)), & 1 - \sqrt{2}/2 \leq \alpha < 1/2. \end{cases} \end{aligned}$$

We now treat the case  $r/m = 1/2$ . To avoid cumbersome notations, assume that  $m$  is even. A lower bound on  $R$  is readily obtained through the sphere-covering bound, yielding

$$R \geq 2^m H^{-1}(1/2). \quad (9.4.22)$$

For the upper bound, we use the Delsarte bound. We estimate the number of nonzero weights in  $\mathcal{RM}(m - r - 1, m)$ , the dual of  $\mathcal{RM}(r, m)$ , using the fact that all of its weights, different from zero and  $2^m$ , are between  $2^{r+1}$  and  $2^m - 2^{r+1}$ . Another useful fact is that the weights do not take all possible values in this range, but have some divisibility properties (see Theorem 9.1.4). This fact along with the Delsarte bound gives

**Lemma 9.4.23** *If  $h$  is a positive integer such that*

$$(h - 1)(m - 1)/h \geq r \geq m - 2,$$

then

$$R_{RM}(r, m) \leq 2^{m-h} - 2^{r+2-h} + 2.$$

□

For  $h = 2$ , this gives

$$R_{RM}(m/2, m) \leq 2^{m-2} - 2^{m/2} + 2 \leq 2^{m-2} (1 + o(1)). \quad (9.4.24)$$

Summarizing (9.4.9)–(9.4.24), we have:

**Theorem 9.4.25** For  $m$  large enough:

If  $m - r = \text{const} \geq 3$ , then

$$\frac{m^{m-r-2}}{(m-r-1)!} (1 + o(1)) \leq R_{RM}(r, m) \leq \frac{m^{m-r-2}}{(m-r-2)!} (1 + o(1));$$

if  $r = \text{const} \geq 2$ , then

$$\begin{aligned} & 2^{m-1} - 2^{m/2} m^{r/2} ((\ln 2)/(2r!))^{1/2} (1 + o(1)) \\ & \leq R_{RM}(r, m) \leq 2^{m-1} - 2^{(m-2)/2} (\sqrt{2} + 1)^{r-1} (1 + o(1)); \end{aligned}$$

if  $r/m = \text{const}, r/m > 1/2$ , then

$$\begin{aligned} & (2m^3)^{-1/2} 2^{mH(1-r/m)} (1 + o(1)) \leq R_{RM}(r, m) \\ & \leq 4^{H(1-r/m)} 2^{mH(1-r/m)} (1 + o(1)); \end{aligned}$$

if  $r/m = \text{const}, 1 - \sqrt{2}/2 \leq r/m < 1/2$ , then

$$\begin{aligned} & 2^{m-1} - ((\ln 2)/2)^{1/2} 2^{m(1+H(r/m))/2} (1 + o(1)) \\ & \leq R_{RM}(r, m) \leq 2^{m-1} - (2m)^{-1/2} 2^{mH(r/m)} (1 + o(1)); \end{aligned}$$

if  $r/m = \text{const}, 0 < r/m \leq 1 - \sqrt{2}/2$ , then

$$\begin{aligned} & 2^{m-1} - ((\ln 2)/2)^{1/2} 2^{m(1+H(r/m))/2} (1 + o(1)) \\ & \leq R_{RM}(r, m) \leq 2^{m-1} - (\sqrt{2} + 1)^{r-1} 2^{(m-2)/2} (1 + o(1)); \end{aligned}$$

if  $r/m = 1/2$ , then

$$\begin{aligned} & 2^m H^{-1}(1/2) (1 + o(1)) \approx 0.11 \cdot 2^m (1 + o(1)) \leq R_{RM}(m/2, m) \\ & \leq 0.25 \cdot 2^m (1 + o(1)). \end{aligned}$$

□

## 9.5 Notes

§9.1 Reed-Muller codes have got a great deal of attention. See, e.g., MacWilliams and Sloane [464] and van Lint [438] for many references. The distance distribution of the second order Reed-Muller codes was determined by Sloane and Berlekamp [594]. Kasami and Tokura [368] have found the number of codewords of  $\mathcal{R}(r, m)$  with weight in the range  $d$  to  $2d$ . This was further expanded to weights at most  $2.5d$  by Kasami, Tokura and Azumi [369]. The divisibility condition for weights in Reed-Muller codes (Theorem 9.1.4) is a consequence of the Ax theorem [36], and was obtained by McEliece [476]. Our proof is due to O. Moreno and C. J. Moreno [500].

§9.2 Theorem 9.2.9 is due to Rothaus [564] and Helleseth, Kløve and Mykkeltveit [300]. The first unsettled case about  $R_{RM}(1, m)$  is whether  $R_{RM}(1, 9) = 240$ .

Lemma 9.2.10 is by Mattson and Schatz (see [569]) and Mykkeltveit [501]. Theorem 9.2.12 is by Mykkeltveit [501]. Another proof is due to Hou [340]. Theorem 9.2.13 is by Patterson and Wiedemann [531], [532]. Brualdi, Cai and Pless [99] and Patterson and Wiedemann [531] stated Conjectures 9.2.14 and 9.2.15.

Let  $R_r(1, m)$  denote the covering radius of  $\mathcal{RM}(1, m)$  in  $\mathcal{RM}(r, m)$ , i.e., the maximal distance from a vector of  $\mathcal{RM}(r, m)$  to the closest vector in  $\mathcal{RM}(1, m)$ . We have:

$$R_2(1, m) = 2^{m-1} - 2^{\lfloor(m-1)/2\rfloor} \text{ Kasami [366]; see also Tarnanen [634].}$$

$$R_{m-1}(1, m) = R_{m-2}(1, m) \text{ Hou [339].}$$

$$R_3(1, 9) > 240 \text{ Langevin [410].}$$

Several topics are related to the study of  $R_{RM}(1, m)$ . The complete weight distribution of the cosets of  $\mathcal{RM}(1, 4)$ ,  $\mathcal{RM}(1, 5)$  and  $\mathcal{RM}(1, 6)$  can be found in Sloane and Dick [595], Berlekamp and Welch [70], Kurshan and Sloane [395], Maiorana [465]. In these papers the symmetry group of  $\mathcal{RM}(1, m)$  is exploited to partition cosets into equivalence classes. This approach hardly leads to the possibility of deriving the coset weight distribution for larger lengths. The number of cosets with minimum weight up to  $2^{m-2} + 2^{m-4}$  is determined by El-Zahar and Khairat [217]. For a characterization of the cosets of the simplex code, see Helleseth and Mattson [301].

The structure of the cosets of  $\mathcal{RM}(1, m)$  is considered by Brualdi, Cai and Pless [99], Brualdi and Pless [100], [101] and Langevin [410]. An *orphan* or *urcoiset* is defined in [100], [301]: one obtains a partial order on the cosets of a linear code  $C$  by defining  $C' \leq C''$  if there is a coset leader  $\mathbf{x}'$  of the coset  $C'$  and a coset leader  $\mathbf{x}''$  of the coset  $C''$  such that  $\text{supp}(\mathbf{x}') \subseteq \text{supp}(\mathbf{x}'')$ . If

$C' < C''$  and there is no coset  $D$  such that  $C' < D < C''$ , then  $C'$  is called a child of  $C''$  and  $C''$  a parent of  $C'$ . The partially ordered set of cosets of  $C$  has a unique minimal element, namely  $C$ , but in general many maximal elements, called orphans. In [99], [100] the orphans of  $\mathcal{RM}(1, m)$  are characterized. For  $m \leq 5$ , all orphans of  $\mathcal{RM}(1, m)$  are enumerated.

Deep holes of  $\mathcal{RM}(1, m)$  for  $m$  even correspond to the so-called *bent functions*. For their construction and characterization, see, e.g., Adams and Tavares [7], Carlet [119], [120], [121], Carlet and Guillot [124], Carlet, Seberry and X. M. Zhang [125], Dillon [201], Kumar and Scholtz [394], Langevin [412], Nyberg [509], Rothaus [564], Savický [568] and references therein.

Results on norms are by Graham and Sloane [265]. It is shown in [265] that the code  $\mathcal{RM}(1, m)$  has norm  $n - \sqrt{n}$ . We obtain in fact the same result using Theorem 9.2.2 because  $n - 1 = 2^m - 1$  is never a square: if  $m \geq 2$ , then  $n - 1 \equiv 3 \pmod{4}$  whereas any square is congruent to 0 or 1 mod 4. This is slightly improved by Hou [344], who proves that for  $m$  odd the norm of  $\mathcal{RM}(1, m)$  is upperbounded by  $4\lfloor 2^{m-2} - 2^{(m-4)/2} \rfloor$ , yielding an upper bound on  $R_{RM}(1, m)$  for  $m$  odd:  $R_{RM}(1, m) \leq 2\lfloor 2^{m-2} - 2^{(m-4)/2} \rfloor$ . The normality of  $\mathcal{RM}(1, 3)$  and  $\mathcal{RM}(1, 5)$  was verified by computer, see Graham and Sloane [265]. For a non-computer proof, see Hou [338]. Note that  $\mathcal{RM}(1, 3)$  has minimum distance 4 and is therefore normal by Theorem 4.2.2(ii). Hou [343] proved the normality of  $\mathcal{RM}(1, 7)$ .

**§9.3** Lemma 9.3.1 is by Schatz [570], who also determined  $R_{RM}(2, 6)$  (for an alternative proof, see Hou [338]). Lemma 9.3.6 is from Cohen, Karpovsky, Mattson and Schatz [156].

Theorem 9.3.11, due to McLoughlin [480], is proved here using the approach of Lempel [413] and Seroussi and Lempel [578]. The statement about the full-rank symmetric matrices with zero diagonal is due to MacWilliams [463].

**§9.4** Lemmas 9.4.1 and 9.4.5 are by Hou [337], [339]. The proof of Theorem 9.4.25 follows Cohen and Litsyn [157]. The case  $r/m = 1/2$  is due to Tietäväinen [647]. For other asymptotic results, see Solé [602] and Tietäväinen [646], [648].

This Page Intentionally Left Blank

# Chapter 10

## Algebraic codes

In this chapter we consider the covering radius of BCH and other algebraic codes. These codes possess a nice algebraic structure in terms of finite fields. Their parameters may be estimated using powerful algebraic techniques, mainly exponential sums.

In Section 10.1 we give the necessary background on BCH codes and discuss their relationship with Reed-Muller codes. A short introduction to other relevant classes of error-correcting codes is provided. Among them are duals of BCH codes, Goppa, self-dual and Reed-Solomon codes. For 1-, 2- and 3-error-correcting BCH codes, the covering radii are exactly determined in Section 10.2. For other BCH codes we need the length to be large enough to provide a tight estimate, based on the analysis of the solvability of some systems of equations. Tools from algebraic number theory lead to bounds which are exact for very long BCH codes. These results are presented in Section 10.3. Section 10.4 is devoted to discussing normality of BCH codes. It is proved that long enough BCH codes are normal. If we partition the BCH code into its even and odd subcodes, then this partition provides subnormality of BCH codes under less restrictive conditions on the length. The duals of BCH codes are studied in Section 10.5. Their minimum distance and covering radius may be estimated via corresponding bounds on exponential sums in finite fields. Here we use our knowledge of the dual distance together with a technique borrowed from Section 8.3. Finally we survey known results on the covering radius of duals of BCH codes, cyclic, Goppa, self-dual and Reed-Solomon codes.

## 10.1 BCH codes: definitions and properties

We denote the *binary primitive BCH code* of length  $2^m - 1$  and *designed distance*  $2e + 1$  by  $\mathcal{BCH}(e, m)$ . It is a cyclic

$$[n = 2^m - 1, k \geq 2^m - me - 1, d \geq 2e + 1]$$

code. Let  $q = 2^m$  and  $\alpha$  be a primitive element of  $\mathbb{F}_q$ . Then the codewords of  $\mathcal{BCH}(e, m)$  have roots  $\alpha^1, \dots, \alpha^{2e-1}$  — and their conjugates — and  $\mathcal{BCH}(e, m)$  can be defined by its parity check matrix

$$\mathbf{H} = \begin{pmatrix} 1 & \alpha & \alpha^2 & \dots & \alpha^{n-1} \\ 1 & \alpha^3 & \alpha^6 & \dots & \alpha^{3(n-1)} \\ \dots & \dots & \dots & \dots & \dots \\ 1 & \alpha^{2e-1} & \alpha^{(2e-1)\cdot 2} & \dots & \alpha^{(2e-1)(n-1)} \end{pmatrix}. \quad (10.1.1)$$

For  $e = 1$  this is the Hamming code. The true minimum distance may exceed the designed distance  $2e + 1$ , and the number of information symbols may exceed  $2^m - me - 1$ . However,

$$k = 2^m - me - 1 \text{ if } 2e - 1 \leq 2^{\lceil m/2 \rceil}. \quad (10.1.2)$$

Since the roots of  $\mathcal{BCH}(e, m)$  form a subset of the roots of  $\mathcal{BCH}(e+1, m)$ , the BCH family is nested:

$$\mathcal{BCH}(e+1, m) \subseteq \mathcal{BCH}(e, m). \quad (10.1.3)$$

The maximal binary weight of the exponents of  $\alpha$  among the roots of  $\mathcal{BCH}(e, m)$  is at most  $\lfloor \log_2(2e+1) \rfloor$ . Thus, from the definition of punctured Reed-Muller codes as cyclic codes,

$$\mathcal{RM}^*(m - \lfloor \log_2(2e+1) \rfloor - 1, m) \subseteq \mathcal{BCH}(e, m). \quad (10.1.4)$$

The weight distribution is known for 1-, 2- and 3-error-correcting BCH codes, through the weight distributions of the corresponding dual codes (see below), and the relation between the spectra of a code and its dual via the MacWilliams transform (Theorem 2.2.3).

The dual code  $\mathcal{BCH}^\perp(e, m)$  can be defined using additive characters. Recall that the trace function  $Tr$  is

$$Tr(\beta) = \beta + \beta^2 + \beta^{2^2} + \dots + \beta^{2^{m-1}},$$

for  $\beta \in \mathbb{F}_q$ . This is a linear mapping from  $\mathbb{F}_q$  to  $\mathbb{F}$ , i.e.,

$$Tr(\beta + \gamma) = Tr(\beta) + Tr(\gamma) \text{ for all } \beta, \gamma \in \mathbb{F}_q.$$

Clearly,  $Tr(0) = 0$ , trace equals 0 for half of the elements of  $\mathbb{F}_q$  and 1 for the other half.  $Tr(1) = 0$  for  $m$  even, and  $Tr(1) = 1$  for  $m$  odd.

The function

$$\psi(x) = (-1)^{Tr(x)}$$

is a mapping from  $\mathbb{F}_q$  to  $\{-1, 1\}$  satisfying

$$\psi(\beta + \gamma) = (-1)^{Tr(\beta) + Tr(\gamma)} = (-1)^{Tr(\beta)}(-1)^{Tr(\gamma)} = \psi(\beta)\psi(\gamma),$$

and is therefore an additive character of  $\mathbb{F}_q$ . In fact, all possible additive characters of  $\mathbb{F}_q$  can be represented as  $\psi_\beta(x) = \psi(\beta x)$  for different choices of  $\beta \in \mathbb{F}_q$ . Thus, there are  $2^m$  possible additive characters, one of them — corresponding to  $\beta = 0$  — being called the *trivial character*. An important property (see Theorem 2.5.11) is

$$\sum_{x \in \mathbb{F}_q} \psi_\beta(x) = \begin{cases} q & \text{if } \psi \text{ is the trivial character,} \\ 0 & \text{otherwise.} \end{cases} \quad (10.1.5)$$

Let  $f(x)$  be a polynomial over  $\mathbb{F}_q$ . Denote

$$\mathbf{c}(f) = (Tr(f(1)), Tr(f(\alpha)), Tr(f(\alpha^2)), \dots, Tr(f(\alpha^{n-1}))).$$

Then  $\mathcal{BCH}^\perp(e, m)$  is the set of vectors  $\mathbf{c}(f)$ ,  $f \in P$ ,  $P$  consisting of all the polynomials of the form

$$\beta_1 x + \beta_3 x^3 + \dots + \beta_{2e-1} x^{2e-1},$$

where  $\beta_{2i-1} \in \mathbb{F}_q$ ,  $i \in [1, e]$ . To estimate the minimum distance of duals of BCH codes, consider the  $\pm 1$ -vectors

$$\begin{aligned} \mathbf{c}^\pm(f) &= ((-1)^{c_1(f)}, (-1)^{c_2(f)}, \dots, (-1)^{c_{q-1}(f)}) \\ &= (\psi(f(1)), \dots, \psi(f(\alpha^{n-1}))). \end{aligned}$$

Evidently,

$$\sum_{x \in \mathbb{F}_q^*} \psi(f(x)) = \sum_{i=1}^{q-1} c_i^\pm(f) = q - 1 - 2w(\mathbf{c}(f)), \quad (10.1.6)$$

and the minimal nonzero weight, i.e., the minimum distance of the code, corresponds to the maximum of the left hand side, taken over those polynomials  $f$  for which  $\mathbf{c}(f)$  is not the all-zero word. This maximum is upperbounded using a special case of the Weil-Carlitz-Uchiyama theorem.

**Theorem 10.1.7** Let  $f(x)$  be a polynomial of degree  $2e-1$  over  $\mathbb{F}_q$ ,  $q = 2^m$ . Then

$$\left| \sum_{x \in \mathbb{F}_q} \psi(f(x)) \right| \leq (2e-2)2^{m/2}.$$

□

Using this theorem to upperbound the left hand side of (10.1.6) and taking into account that  $\psi(0) = 1$ , we conclude that

$$d^\perp(\mathcal{BCH}(e, m)) \geq 2^{m-1} - (e-1)2^{m/2}. \quad (10.1.8)$$

The weight distributions are known for  $\mathcal{BCH}^\perp(e, m)$  when  $e = 1, 2$  and  $3$ . Namely,

$e = 1$ :

$$\mathcal{B}_{q/2} = q - 1;$$

$e = 2$ ,  $m$  odd:

$$\mathcal{B}_{q/2 \pm \sqrt{q/2}} = \frac{1}{4}\sqrt{q}(\sqrt{q} \mp \sqrt{2})(q-1),$$

$$\mathcal{B}_{q/2} = \frac{1}{2}(q-1)(q+2);$$

$e = 2$ ,  $m \geq 4$ , even:

$$\mathcal{B}_{q/2 \pm \sqrt{q}} = \frac{1}{24}\sqrt{q}(\sqrt{q} \mp 2)(q-1),$$

$$\mathcal{B}_{q/2 \pm \sqrt{q}/2} = \frac{1}{3}\sqrt{q}(\sqrt{q} \mp 1)(q-1),$$

$$\mathcal{B}_{q/2} = \frac{1}{4}(q+4)(q-1);$$

$e = 3$ ,  $m \geq 5$ , odd:

$$\mathcal{B}_{q/2 \pm \sqrt{2q}} = \frac{1}{96}\sqrt{q}(\sqrt{q} \mp 2\sqrt{2})(q-1)(q-2),$$

$$\mathcal{B}_{q/2 \pm \sqrt{q/2}} = \frac{5}{24}\sqrt{q}(\sqrt{q} \mp \sqrt{2})(q-1)(q + \frac{8}{5}),$$

$$\mathcal{B}_{q/2} = \frac{9}{16}(q-1)(q^2 + \frac{2}{3}q + \frac{16}{9});$$

$e = 3$ ,  $m \geq 6$ , even:

$$\mathcal{B}_{q/2 \pm 2\sqrt{q}} = \frac{1}{1920}\sqrt{q}(\sqrt{q} \mp 4)(q-1)(q-4),$$

$$\mathcal{B}_{q/2 \pm \sqrt{q}} = \frac{7}{96}\sqrt{q}(\sqrt{q} \mp 2)q(q-1),$$

$$\mathcal{B}_{q/2 \pm \sqrt{q}/2} = \frac{1}{5}\sqrt{q}(\sqrt{q} \mp 1)(q-1)(q + \frac{8}{3}),$$

$$\mathcal{B}_{q/2} = \frac{29}{64}(q-1)(q^2 - \frac{4}{29}q + \frac{64}{29}).$$

Hence the number of nonzero weights in the duals of BCH codes is

- 1 for  $\mathcal{BCH}^\perp(1, m)$
- 3 for  $\mathcal{BCH}^\perp(2, m)$   $m$  odd;
- 5 for  $\mathcal{BCH}^\perp(2, m)$   $m$  even;
- 5 for  $\mathcal{BCH}^\perp(3, m)$   $m$  odd;
- 7 for  $\mathcal{BCH}^\perp(3, m)$   $m$  even.

Some other algebraic codes (already presented in Section 2.6) may be defined in a similar manner. Let  $h$  be a divisor of  $2^m - 1$ . The binary *nonprimitive* BCH code  $\mathcal{BCH}_h(e, m)$  has length  $n = (2^m - 1)/h$ , designed distance  $2e + 1$ , and is defined by its parity check matrix:

$$\mathbf{H} = \begin{pmatrix} 1 & \alpha^h & \dots & \alpha^{h(n-1)} \\ 1 & \alpha^{3h} & \dots & \alpha^{3h(n-1)} \\ \dots & \dots & \dots & \dots \\ 1 & \alpha^{(2e-1)h} & \dots & \alpha^{(2e-1)h(n-1)} \end{pmatrix}. \quad (10.1.9)$$

The case  $h = 1$  corresponds to primitive BCH codes.

The BCH codes form a subclass of the cyclic codes. Goppa codes constitute another wide class of codes having primitive BCH codes as a subclass. Let  $g(x)$  be a polynomial over  $\mathbb{F}_q$  of degree  $e$ , and  $L = \mathbb{F}_q \setminus Z = \{\alpha_1, \dots, \alpha_n\}$  where  $Z$  is the set of zeros of  $g(x)$  in  $\mathbb{F}_q$ . Assume that  $g(x)$  has distinct roots. The parity check matrix of the binary Goppa code  $\mathcal{GOP}(L, g)$  of length  $|L| = n$  and minimum distance at least  $2e + 1$  is

$$\mathbf{H} = \begin{pmatrix} \frac{1}{g(\alpha_1)} & \dots & \frac{1}{g(\alpha_n)} \\ \frac{\alpha_1}{g(\alpha_1)} & \dots & \frac{\alpha_n}{g(\alpha_n)} \\ \dots & \dots & \dots \\ \frac{\alpha_1^{e-1}}{g(\alpha_1)} & \dots & \frac{\alpha_n^{e-1}}{g(\alpha_n)} \end{pmatrix}. \quad (10.1.10)$$

A code  $C$  is self-dual if  $C = C^\perp$ . The single extensions of some good cyclic codes (Golay, quadratic residue, etc.) are self-dual. Codes with all weights divisible by 4 are called doubly-even (or of type II) and exist only if their length is divisible by 8. They have parameters  $[8m, 4m, d \leq 4\lfloor m/3 \rfloor + 4]$  and are called extremal when  $d = 4\lfloor m/3 \rfloor + 4$ .

In the nonbinary case, Reed-Solomon codes and their shortenings play a special role: these  $[n, k, d]$  codes over  $\mathbb{F}_q$  meet the Singleton bound  $n = k + d - 1$  and exist for  $n \leq q - 1$ . They can be extended to  $[q, q - d + 1, d]$ ,  $[q + 1, q - d + 2, d]$ ,  $[q + 2, 3, q]$  and  $[q + 2, q - 1, 4]$  codes, called in the sequel singly, doubly and triply extended, respectively. The BCH codes are their

*subfield IF subcodes*, i.e., consist of all the codewords of the corresponding Reed-Solomon codes which have only binary coordinates.

We use the following notations for the covering radii of codes:

- $R_B(e, m)$  for the covering radius of  $\mathcal{BCH}(e, m)$ ;
- $R_B^\perp(e, m)$  for the covering radius of  $\mathcal{BCH}^\perp(e, m)$ ;
- $R_{B,h}(e, h, m)$  for the covering radius of  $\mathcal{BCH}_h(e, m)$ ;
- $R_{GOP}(L, g)$  for the covering radius of  $\mathcal{GOP}(L, g)$ ;
- $R_S(m)$  for the covering radius of extremal doubly-even self-dual codes of length  $8m$ ;
- $R_{RS}(q, d, n)$  for the covering radius of  $q$ -ary Reed-Solomon or shortened or extended Reed-Solomon codes of length  $n$  and minimum distance  $d$ .

## 10.2 2- and 3-error-correcting BCH codes

Since  $\mathcal{BCH}(1, m)$  is the Hamming code,  $R_B(1, m) = 1$ . Assume now  $e > 1$ . We start with a lower bound.

**Lemma 10.2.1** *For  $2e - 1 \leq 2^{\lceil m/2 \rceil}$ ,*

$$R_B(e, m) \geq 2e - 1.$$

**Proof.** Follows by (10.1.2), (10.1.3) and the supercode lemma (Lemma 8.2.1).  $\square$

For  $e = 2$ , the previous lemma gives  $R_B(2, m) \geq 3$  for  $m \geq 3$ . We now prove that in this case the lower bound is tight. We first need an auxiliary lemma.

**Lemma 10.2.2** *Let  $\beta \in \mathbb{F}_q$ . Then the equation*

$$x^2 + x + \beta = 0$$

*is solvable in  $\mathbb{F}_q$  if and only if  $\text{Tr}(\beta) = 0$ .*

**Proof.** If  $\gamma \in \mathbb{F}_q$  is a root of the equation, then  $\gamma^2 + \gamma + \beta = 0$ . Thus,

$$\begin{aligned} 0 &= \text{Tr}(0) = \text{Tr}(\gamma^2 + \gamma + \beta) \\ &= \text{Tr}(\gamma^2) + \text{Tr}(\gamma) + \text{Tr}(\beta) \\ &= \text{Tr}(\gamma) + \text{Tr}(\gamma) + \text{Tr}(\beta) = \text{Tr}(\beta). \end{aligned}$$

For the converse, denote by  $S$  the set of the field elements with zero trace,  $|S| = 2^{m-1}$ . The equation  $x^2 + x + \beta = 0$  has at most two solutions and hence each of the  $2^{m-1}$  elements of  $S$  can be the image of at most two elements of  $\mathbb{F}_q$  by the mapping  $f : \mathbb{F}_q \rightarrow S$  defined by  $f(\gamma) = \gamma^2 + \gamma$ . Therefore  $f$  is onto.  $\square$

**Theorem 10.2.3** For  $m \geq 3$ ,

$$R_B(2, m) = 3.$$

**Proof.** The lower bound follows from Lemma 10.2.1. The parity check matrix of  $\mathcal{BCH}(2, m)$  is

$$\mathbf{H} = \begin{pmatrix} 1 & \alpha & \dots & \alpha^{n-1} \\ 1 & \alpha^3 & \dots & \alpha^{3(n-1)} \end{pmatrix}.$$

Recall that the covering radius is the minimal number  $R$  such that every syndrome can be obtained as the sum of  $R$  or fewer columns of the parity check matrix. In our case it is therefore sufficient to prove that the system

$$\begin{aligned} x_1 + x_2 + x_3 &= \beta_1 \\ x_1^3 + x_2^3 + x_3^3 &= \beta_2 \end{aligned}$$

is solvable for every  $\beta_1, \beta_2 \in \mathbb{F}_q$ . By substituting  $y_i = x_i + \beta_1$  (for  $i = 1, 2, 3$ ) this system becomes

$$\begin{aligned} y_1 + y_2 + y_3 &= 0 \\ y_1^3 + y_2^3 + y_3^3 &= \beta \end{aligned} \tag{10.2.4}$$

where  $\beta = \beta_1^3 + \beta_2$ . Extracting  $y_3$  from the first equation and substituting it into the second one gives

$$y_1 y_2 (y_1 + y_2) = \beta.$$

Assume  $y_2 \neq 0$ . Set  $y = y_1/y_2$ . We get

$$y^2 + y + \frac{\beta}{y^3} = 0. \tag{10.2.5}$$

If  $\beta = 0$ , then this equation has the obvious solutions  $y = 0$  and  $y = 1$ . By Lemma 10.2.2, to prove that for every  $\beta \in \mathbb{F}_q^*$  this equation is solvable, it is enough to show that we can always find a nonzero  $y_2$  such that  $\text{Tr}(\beta/y_2^3) = 0$ .

If  $m$  is odd, there is no problem: choose  $y_2 = \sqrt[3]{\beta/\theta}$ , where  $\theta$  is an arbitrary nonzero element having zero trace. Indeed, every field element in this case has a unique cubic root. To see this, notice that  $2^m - 1 \equiv 1 \pmod{3}$  for  $m$  odd. Denote  $\ell = (2^m - 2)/3$ . Then

$$\begin{aligned}\sqrt[3]{\alpha^{3k}} &= \alpha^k; \\ \sqrt[3]{\alpha^{3k+1}} &= \sqrt[3]{\alpha^{3k+1+2(3\ell+1)}} = \alpha^{k+2\ell+1}; \\ \sqrt[3]{\alpha^{3k+2}} &= \sqrt[3]{\alpha^{3k+2+3\ell+1}} = \alpha^{k+\ell+1}.\end{aligned}$$

For  $m$  even,  $2^m - 1$  is always divisible by 3. So only one third of the nonzero field elements possess a cubic root. Actually, as we now show, there exist elements with zero trace of the form  $\alpha^\ell$  for any  $\ell \equiv 0, 1, 2 \pmod{3}$ .

If  $\beta = \alpha^{3k}$  we may choose  $y_2 = \alpha^k$ , and  $\text{Tr}(\beta/y_2^3) = \text{Tr}(1) = 0$ . Since there are  $(q-1)/3 < q/2$  elements of the form  $\alpha^{3k}$ , there is an element of zero trace  $\alpha^{3k+1}$  or  $\alpha^{3k+2}$  for some  $k$ . Denote it by  $\theta$ . Note that  $\theta^2 = \alpha^{3k_1+1}$  if  $\theta = \alpha^{3k+2}$ , and  $\theta^2 = \alpha^{3k_2+2}$  if  $\theta = \alpha^{3k+1}$  for some  $k$  and  $k_1$  or  $k_2$ . Since  $\text{Tr}(\theta) = \text{Tr}(\theta^2) = 0$ , we get two different field elements  $\gamma_1 = \alpha^{3k_1+1}$  and  $\gamma_2 = \alpha^{3k_2+2}$  with zero trace. Now if  $\beta = \alpha^{3k+s}$ ,  $s = 1$  or  $2$ , we choose  $y_2 = \alpha^{k-k_s}$ , and

$$\text{Tr}(\beta/y_2^3) = \text{Tr}(\alpha^{3k+s}/\alpha^{3(k-k_s)}) = \text{Tr}(\alpha^{3k_s+s}) = 0.$$

So, for all  $\beta$ , we find  $y_2$  such that equation (10.2.5) is solvable.  $\square$

Notice that for  $m$  odd, the codes  $\mathcal{BCH}^\perp(2, m)$  have only three nonzero weights, and the claim also follows from the Delsarte bound (Theorem 8.3.7). This is not true for even  $m$ .

For  $e = 3$ , a more thorough analysis is required.

**Theorem 10.2.6** *For  $m \geq 4$ ,*

$$R_B(3, m) = 5.$$

**Proof.** (sketch) The lower bound is again due to the supercode lemma. For odd  $m$ , we may use Delsarte's result (see Theorem 8.3.7), combined with the fact that the duals of BCH codes have five nonzero weights.

For even  $m$ , there are seven nonzero weights in  $\mathcal{BCH}^\perp(3, m)$  and the Delsarte bound does not work. Thus we have to prove the solvability of the system

$$\begin{aligned}x_1 + x_2 + x_3 + x_4 + x_5 &= \beta_1 \\ x_1^3 + x_2^3 + x_3^3 + x_4^3 + x_5^3 &= \beta_2 \\ x_1^5 + x_2^5 + x_3^5 + x_4^5 + x_5^5 &= \beta_3\end{aligned}$$

Table 10.1: Covering radius of binary primitive BCH codes.

$n$	$k$	$e$	$d$	$R$
7	4	1	3	1
15	11	1	3	1
15	7	2	5	3
15	5	3	7	5
31	26	1	3	1
31	21	2	5	3
31	16	3	7	5
31	11	4	11	7
31	6	6	15	11
63	57	1	3	1
63	51	2	5	3
63	45	3	7	5
63	39	4	9	7
63	36	5	11	9

for every right hand side. This requires a case by case analysis very much like in the proof of the previous theorem. We omit the details.  $\square$

Not much is known about  $R_B(e, m)$  for  $e > 3$ . The results on primitive BCH codes are summarized in Table 10.1.

### 10.3 Long BCH codes

In spite of our poor knowledge of covering radii of short BCH codes, we can show that for long enough BCH codes the lower bound in Lemma 10.2.1 is tight. We start by presenting some weaker bounds which give better estimates on the minimal length and introduce the main ideas.

**Theorem 10.3.1** *If  $q = 2^m \geq (2e - 1)^{4e+2}$ , then*

$$2e - 1 \leq R_B(e, m) \leq 2e. \quad (10.3.2)$$

**Proof.** The lower bound stems from Lemma 10.2.1. To show the upper bound, we prove that the system

$$\sum_{j=1}^{2e} x_j^{2i-1} = \beta_i, \quad i \in [1, e], \quad (10.3.3)$$

is solvable for all  $\beta_1, \dots, \beta_e \in \mathbb{F}_q$ . Instead of (10.3.3) consider the “homogenized” system

$$\sum_{j=1}^{2e} x_j^{2i-1} = \beta_i y^{2i-1}, \quad i \in [1, e]. \quad (10.3.4)$$

If (10.3.4) has a solution  $x_1, \dots, x_{2e} \in \mathbb{F}_q$ , and  $y \in \mathbb{F}_q^*$ , then, clearly,  $x_1/y, \dots, x_{2e}/y$  is a solution of (10.3.3). Let  $N_0$  be the number of solutions of (10.3.4). Then,

$$\begin{aligned} N_0 q^e &= \sum_{x_1, \dots, x_{2e} \in \mathbb{F}_q} \sum_{y \in \mathbb{F}_q^*} \left( \sum_{\alpha_1 \in \mathbb{F}_q} \psi(\alpha_1(x_1 + \dots + x_{2e} + \beta_1 y)) \right) \cdot \\ &\quad \left( \sum_{\alpha_2 \in \mathbb{F}_q} \psi(\alpha_2(x_1^3 + \dots + x_{2e}^3 + \beta_2 y^3)) \right) \cdot \\ &\quad \cdots \cdot \\ &\quad \left( \sum_{\alpha_e \in \mathbb{F}_q} \psi(\alpha_e(x_1^{2e-1} + \dots + x_{2e}^{2e-1} + \beta_e y^{2e-1})) \right) \\ &= \sum_{\alpha_1 \in \mathbb{F}_q} \cdots \sum_{\alpha_e \in \mathbb{F}_q} \left( \sum_{y \in \mathbb{F}_q^*} \psi(\alpha_1 \beta_1 y + \dots + \alpha_e \beta_e y^{2e-1}) \right) \cdot \\ &\quad \left( \sum_{x_1 \in \mathbb{F}_q} \psi(\alpha_1 x_1 + \dots + \alpha_e x_1^{2e-1}) \right) \cdot \\ &\quad \cdots \cdot \\ &\quad \left( \sum_{x_{2e} \in \mathbb{F}_q} \psi(\alpha_1 x_{2e} + \dots + \alpha_e x_{2e}^{2e-1}) \right) \\ &= \sum_{\alpha_1 \in \mathbb{F}_q} \cdots \sum_{\alpha_e \in \mathbb{F}_q} \left( \sum_{y \in \mathbb{F}_q^*} \psi(\alpha_1 \beta_1 y + \dots + \alpha_e \beta_e y^{2e-1}) \right) \cdot \\ &\quad \left( \sum_{x \in \mathbb{F}_q} \psi(\alpha_1 x + \dots + \alpha_e x^{2e-1}) \right)^{2e}. \end{aligned}$$

Now, from Theorem 10.1.7 and (10.1.5) we have

$$\left| \sum_{x \in \mathbb{F}_q} \psi(\alpha_1 x + \dots + \alpha_e x^{2e-1}) \right| \begin{cases} = q & \text{for } \alpha_1 = \dots = \alpha_e = 0, \\ \leq 2(e-1)\sqrt{q} & \text{otherwise,} \end{cases}$$

$$\sum_{y \in \mathbb{F}_q^*} \psi(\alpha_1 \beta_1 y + \dots + \alpha_e \beta_e y^{2e-1}) \begin{cases} = q-1 & \text{for } \alpha_1 \beta_1 = \dots = \alpha_e \beta_e = 0, \\ \geq -2(e-1)\sqrt{q} - 1 & \text{otherwise.} \end{cases}$$

Thus we have

$$\begin{aligned} q^e N_0 &\geq q^{2e}(q-1) - (q^e - 1)(2e-2)^{2e} q^e ((2e-2)\sqrt{q} + 1) \\ &> q^{2e+1} - (2e-2)^{2e} (2e-1) q^{2e+1/2} - q^{2e} \\ &> q^{2e+1/2} (\sqrt{q} - (2e-1)^{2e+1}) \geq 0. \end{aligned}$$

Hence (10.3.3) is solvable.  $\square$

It is easy to see that in the process of calculating  $N_0$  we took into account many redundant solutions. For example, solutions with  $x_i = x_j$  are irrelevant, since they involve a smaller number of variables. A more thorough analysis now allows us to decrease the minimal length.

**Theorem 10.3.5**  $R_B(e, m) \leq 2e$  if

$$2^m \geq 4(e-1)^2(e!)^2.$$

**Proof.** Instead of counting all solutions of (10.3.4), we count the number  $N'_s$  of solutions with  $0 < x_1 < \dots < x_s$ ,  $y \neq 0$ , where we have ordered the elements of  $\mathbb{F}_q$ . We get

$$\begin{aligned} q^e N'_s &= \sum_{\alpha_1, \dots, \alpha_e \in \mathbb{F}_q} \sum_{y \neq 0} \psi(\alpha_1 \beta_1 y + \dots + \alpha_e \beta_e y^{2e-1}) \\ &\quad \sum_{0 < x_1 < \dots < x_s} \psi(\alpha_1 x_1 + \dots + \alpha_e x_1^{2e-1}) \dots \psi(\alpha_1 x_s + \dots + \alpha_e x_s^{2e-1}). \end{aligned} \quad (10.3.6)$$

In the sum (10.3.6) every choice  $(x_1, \dots, x_s)$  corresponds to choosing  $s$  coordinates of the word  $\mathbf{c} = Tr(\mathbf{aH})$ , where  $\mathbf{a} = (\alpha_1, \dots, \alpha_e)$  and  $\mathbf{H}$  is as in (10.1.1). Hence

$$\begin{aligned} q^e N'_s &= \sum_{\mathbf{a} \in \mathbb{F}_q^e} \sum_{y \neq 0} \psi(\alpha_1 \beta_1 y + \dots + \alpha_e \beta_e y^{2e-1}) \sum_{\mathbf{u} \in \mathbb{F}^n, w(\mathbf{u})=s} (-1)^{(\mathbf{c}, \mathbf{u})} \\ &= \sum_{\mathbf{a} \in \mathbb{F}_q^e} \sum_{y \neq 0} \psi(\alpha_1 \beta_1 y + \dots + \alpha_e \beta_e y^{2e-1}) P_s(w(\mathbf{c})), \end{aligned}$$

where  $P_i(x)$  denotes the Krawtchouk polynomial of degree  $i$  (cf. Sections 2.2 and 2.3). Choose now  $m_0, m_1, \dots, m_{2e}$  such that

$$g_{2e}(x) := \left( \sum_{i=0}^e P_i(x) \right)^2 = \sum_{i=0}^{2e} m_i P_i(x).$$

By (2.3.12),

$$g_{2e}(0) = \left( \sum_{i=0}^e \binom{n}{i} \right)^2.$$

Using (2.3.23) and (2.3.19) we have

$$m_0 = 2^{-n} \sum_{x=0}^n \binom{n}{x} \left( \sum_{i=0}^e P_i(x) \right)^2$$

$$\begin{aligned}
&= 2^{-n} \sum_{x=0}^n \binom{n}{x} \sum_{i=0}^e \sum_{j=0}^e P_i(x) P_j(x) = 2^{-n} \sum_{i=0}^e \sum_{j=0}^e \sum_{x=0}^n \binom{n}{x} P_i(x) P_j(x) \\
&= 2^{-n} \sum_{i=0}^e \binom{n}{i} 2^n = \sum_{i=0}^e \binom{n}{i}.
\end{aligned}$$

So,

$$\frac{g_{2e}(0)}{m_0} = \sum_{i=0}^e \binom{n}{i}. \quad (10.3.7)$$

Because  $g_{2e}(x)$  is always nonnegative we get

$$\begin{aligned}
q^e \sum_{i=0}^{2e} m_i N'_i &= \sum_{\mathbf{a} \in \mathbb{F}_q^e, y \neq 0} \psi(\alpha_1 \beta_1 y + \dots + \alpha_e \beta_e y^{2e-1}) \sum_{i=0}^{2e} m_i P_i(w(\mathbf{c})) \\
&\geq (q-1)g_{2e}(0) - (2(e-1)\sqrt{q} + 1) \sum_{\mathbf{a} \in (\mathbb{F}_q^e)^*} g_{2e}(w(\mathbf{c})),
\end{aligned}$$

using the Weil-Carlitz-Uchiyama bound. Assume that the BCH code  $C$  has dimension  $n - em$ ; then  $\mathbf{c}$  runs through  $C^\perp$  when  $\mathbf{a}$  runs through  $\mathbb{F}_q^e$ . Furthermore, since the degree of  $g_{2e}(x)$  is less than the minimum distance of the code, we obtain

$$\sum_{\mathbf{a} \in \mathbb{F}_q^e} g_{2e}(w(\mathbf{c})) = \sum_{i=0}^{2e} m_i \sum_{\mathbf{c} \in C^\perp} P_i(w(\mathbf{c})) = q^e \sum_{i=0}^{2e} m_i \mathcal{B}_i = q^e m_0.$$

This gives

$$q^e \sum_{i=0}^{2e} m_i N'_i \geq (q-1)g_{2e}(0) - (2(e-1)\sqrt{q} + 1)(q^e m_0 - g_{2e}(0)).$$

To prove that  $R_B(e, m) \leq 2e$  it is enough to show that  $\sum_{i=0}^{2e} m_i N'_i > 0$ . The result follows now from (10.3.7) and estimates for binomial coefficients.  $\square$

To proceed we need the following generalization of the Weil-Carlitz-Uchiyama theorem for polynomials in several variables due to Deligne, presented here in a particular version.

**Theorem 10.3.8** *If  $f(x_1, \dots, x_s)$  is a polynomial of degree  $2e-1$  over  $\mathbb{F}_q$ ,  $q = 2^m$ , and  $\hat{f}$ , the maximal degree homogeneous part of  $f$ , is such that the only solution of the system*

$$\frac{\partial \hat{f}}{\partial x_j} = 0, \quad j \in [1, s],$$

in the algebraic closure of  $\mathbb{F}_q$  is the trivial one:  $x_1 = \dots = x_s = 0$ , then

$$\left| \sum_{x_1, \dots, x_s \in \mathbb{F}_q} \psi(f(x_1, \dots, x_s)) \right| \leq (2e - 2)^s q^{s/2}.$$

□

Now we are ready to prove the following

**Theorem 10.3.9** *If  $q = 2^m \geq (2e)^{4e-2}$  and  $e$  is of the form  $2^u + 1$ , then*

$$R_B(e, m) = 2e - 1.$$

**Proof.** We may assume  $e \geq 4$ . We show that for each  $(\gamma_1, \dots, \gamma_e) \in \mathbb{F}_q^e$  the system of  $2e - 1$  equations

$$\sum_{j=1}^{2e-1} z_j^{2i-1} = \gamma_i, \quad i \in [1, e], \quad (10.3.10)$$

has a solution  $(z_1, \dots, z_{2e-1}) \in \mathbb{F}_q^{2e-1}$ . Substituting  $x_j = z_j + \gamma_1$ ,  $j \in [1, 2e-1]$ , transforms the system into

$$\sum_{j=1}^{2e-1} x_j^{2i-1} = \beta_i, \quad i \in [1, e],$$

where  $\beta_1 = 0$  and  $\beta_i$  depends on  $\gamma_1$  and  $\gamma_i$ . Any solution of this system yields a solution to the original one. As in the proof of Theorem 10.3.1, it suffices to show that the system

$$\sum_{j=1}^{2e-1} x_j^{2i-1} = \beta_i y^{2i-1}, \quad i \in [1, e],$$

has a solution  $x_1, \dots, x_{2e-1}, y$  with  $y \in \mathbb{F}_q^*$ .

Furthermore, solving for  $x_{2e-1}$  in the first equation and substituting transforms the system into

$$f_i(\mathbf{x}) = \beta_i y^{2i-1}, \quad i \in [2, e],$$

where  $\mathbf{x} = (x_1, \dots, x_{2e-2})$  and

$$f_i(\mathbf{x}) = \sum_{j=1}^{2e-2} x_j^{2i-1} + \left( \sum_{j=1}^{2e-2} x_j \right)^{2i-1}.$$

The number  $N_{total}$  of solutions  $(x_1, \dots, x_{2e-2}, y)$  with  $y \neq 0$  can be written as

$$N_{total} = q^{-e+1} \sum_{\mathbf{x} \in \mathbb{F}_q^{2e-2}} \sum_{y \in \mathbb{F}_q^*} \sum_{\mathbf{a} \in \mathbb{F}_q^{e-1}} \psi(\langle \mathbf{a}, \mathbf{f}(\mathbf{x}) + \mathbf{b}(y) \rangle)$$

where  $\mathbf{a} = (\alpha_2, \dots, \alpha_e)$ ,  $\mathbf{f}(\mathbf{x}) = (f_2(\mathbf{x}), \dots, f_e(\mathbf{x}))$  and

$$\mathbf{b}(y) = (\beta_2 y^3, \dots, \beta_e y^{2e-1}).$$

If all the  $\beta_i$ 's are zero, then the system has a trivial solution. Thus assume that at least one of them, say  $\beta_v$ , is nonzero.

We may write

$$q^{e-1} N_{total} = U_0 + U_1,$$

where

$$U_i = \sum_{\mathbf{a} \in A_i} \sum_{\mathbf{x} \in \mathbb{F}_q^{2e-2}} \psi(\langle \mathbf{a}, \mathbf{f}(\mathbf{x}) \rangle) \sum_{y \in \mathbb{F}_q^*} \psi(\langle \mathbf{a}, \mathbf{b}(y) \rangle)$$

and

$$A_0 = \{\mathbf{a} \in \mathbb{F}_q^{e-1} : \alpha_e = 0\}, \quad A_1 = \{\mathbf{a} \in \mathbb{F}_q^{e-1} : \alpha_e \neq 0\}.$$

Here  $U_0$  equals  $q^{e-2}$  times the number  $N_0$  of solutions  $(\mathbf{x}, y)$ ,  $y \in \mathbb{F}_q^*$ , of the system

$$f_i(\mathbf{x}) = \beta_i y^{2i-1}, \quad i \in [2, e-1].$$

However, this is equivalent to the system

$$\sum_{j=1}^{2e-1} x_j^{2i-1} = \beta_i y^{2i-1}, \quad i \in [1, e-1],$$

and exactly the same argument as in the proof of Theorem 10.3.1 gives (using the simple estimate, for any polynomial  $g$ ,  $|\sum_{y \in \mathbb{F}_q^*} \psi(g(y))| \leq q-1$ ):

$$q^{e-1} N_0 \geq q^{2e-1} (q-1) - q^{e-1} (q-1) ((2e-4)\sqrt{q})^{2e-1}$$

and therefore

$$U_0 = q^{e-2} N_0 \geq (q-1) q^{2e-\frac{5}{2}} (\sqrt{q} - (2e-4)^{2e-1}).$$

Consider now

$$U_1 = \sum_{\mathbf{a} \in A_1} F(\mathbf{a}) G(\mathbf{a})$$

where

$$F(\mathbf{a}) = \sum_{\mathbf{x} \in \mathbb{F}_q^{2e-2}} \psi(\langle \mathbf{a}, \mathbf{f}(\mathbf{x}) \rangle),$$

$$G(\mathbf{a}) = \sum_{y \in \mathbb{F}_q^*} \psi(\langle \mathbf{a}, \mathbf{b}(y) \rangle).$$

Since  $\alpha_e \neq 0$ , the maximal degree homogenous part of  $\langle \mathbf{a}, \mathbf{f}(\mathbf{x}) \rangle$  is  $\alpha_e f_e(\mathbf{x})$ . Moreover, the equations

$$\frac{\partial f_e(\mathbf{x})}{\partial x_j} = 0, \quad j \in [1, 2e-2] \quad (10.3.11)$$

imply

$$x_j^{2e-2} = (x_1 + \dots + x_{2e-2})^{2e-2}, \quad j \in [1, 2e-2].$$

Since  $e = 2^u + 1$ , we have

$$x_j^{2^{u+1}} = (x_1 + \dots + x_{2e-2})^{2^{u+1}}, \quad j \in [1, 2e-2].$$

Therefore the only solution of (10.3.11) in the algebraic closure of  $\mathbb{F}_q$  is  $x_1 = x_2 = \dots = x_{2e-2} = 0$ . Hence by Theorem 10.3.8,

$$|F(\mathbf{a})| \leq (2e-2)^{2e-2} q^{e-1}.$$

Furthermore, using Theorem 10.1.7,

$$|G(\mathbf{a})| \leq \begin{cases} q-1 & \text{if } \alpha_v = 0 \\ (2e-2)\sqrt{q} + 1 & \text{otherwise.} \end{cases}$$

There are at most  $q^{e-3}(q-1)$  terms with  $\alpha_v = 0$  in the sum  $U_1$  and we obtain

$$\begin{aligned} |U_1| &< (2e-2)^{2e-2} q^{e-1} (q^{e-3}(q-1)^2 + q^{e-2}(q-1)(2e-1)\sqrt{q}) \\ &< (q-1)q^{2e-5/2} 2e(2e-2)^{2e-2}. \end{aligned}$$

All in all we get

$$q^{e-1} N_{\text{total}} > (q-1)q^{2e-5/2} ((\sqrt{q} - (2e-4)^{2e-1}) - 2e(2e-2)^{2e-2}) > 0$$

when  $q \geq (2e)^{4e-2}$ . Therefore  $R_B(e, m) \leq 2e-1$  and equality again follows from Lemma 10.2.1.  $\square$

In fact, the upper bound  $R_B(e, m) \leq 2e-1$  holds for all long enough primitive BCH codes. We omit the quite involved proof.

**Theorem 10.3.12** *If  $q = 2^m \geq (2e-3)((2e-1)!)^2$ , then*

$$R_B(e, m) = 2e-1.$$

$\square$

Now we consider the nonprimitive case; first an upper bound.

**Theorem 10.3.13** *If  $h > 1$  and*

$$q = 2^m \geq ((2e - 1)h - 1)^2 (e!)^2,$$

*then  $R_{B,h}(e, m) \leq 2e$ .*

**Proof.** To upperbound  $R_{B,h}(e, m)$ , an approach analogous to the proof of Theorem 10.3.5 applied to the system

$$\sum_{j=1}^s x_j^{h(2i-1)} = \beta_i, \quad i \in [1, e], \quad (10.3.14)$$

can be used. We again omit the details.  $\square$

**Theorem 10.3.15** *If  $h > 1$  and*

$$q = 2^m \geq ((2e - 1)h - 1)^2 (e!)^2,$$

*then  $R_{B,h}(e, m) = 2e$ .*

**Proof.** In particular, the technique used in the previous proof shows that the dimension of the code is  $n - em$ , and therefore  $R_{B,h}(e, m)$  is the smallest integer  $s$  such that the system (10.3.14) has a solution for all  $\beta_1, \dots, \beta_e \in \mathbb{F}_q^*$ . Choose  $\beta \in \mathbb{F}_q^*$  not an  $h$ -th power of any field element,  $\beta_i = \beta^{2i-1}$  for all  $i \in [1, e]$ , and let  $a$  be the smallest  $s$  such that the system (10.3.14) has a solution. By the choice of  $\beta$ , trivially  $a \geq 2$ . If  $(x_1, \dots, x_a)$  is a solution, then  $(x_1^h, \dots, x_a^h)$  is a solution of the system

$$\sum_{j=1}^a y_j^{2i-1} = \beta^{2i-1}, \quad i \in [1, e]. \quad (10.3.16)$$

Interpret now (10.3.16) in terms of the primitive  $e$ -error-correcting BCH code  $C'$  of length  $nh = 2^m - 1$ : every vector  $\mathbf{z} \in \mathbb{F}^{nh}$  of syndrome  $(\beta, \beta^3, \dots, \beta^{2e-1})$  has distance  $a$  to a codeword of  $C'$  (by the minimality of  $a$ , the elements  $x_i^h$  are all different). However,  $(\beta, \beta^3, \dots, \beta^{2e-1})$  is a column in the parity check matrix of the primitive BCH code  $C'$ , and hence  $d(\mathbf{z}, C') = 1$ . But  $a \geq 2$ , and the minimum distance of  $C'$  is at least  $2e + 1$ , implying  $a \geq 2e$  by the triangle inequality.  $\square$

## 10.4 Normality of BCH codes

Using techniques similar to the ones in the previous section, one can also study the normality of long binary BCH codes.

**Theorem 10.4.1** *There is a constant  $m_0$  depending only on  $e$  such that for all  $m \geq m_0$ ,  $\mathcal{BCH}(e, m)$  is normal.*

**Proof.** If  $e = 1$ , the code  $\mathcal{BCH}(1, m)$  is the Hamming code. It has covering radius one and is normal. So assume  $e > 1$ . We show that  $C = \mathcal{BCH}(e, m)$  has norm  $4e - 1$  with respect to the first coordinate, when  $m$  is large enough. Let  $\mathbf{v}$  be an arbitrary vector of length  $n$  and  $\mathbf{b} = \mathbf{H}\mathbf{v}^T$  its syndrome. Assume first that  $\mathbf{v} \in C$ , i.e.,  $\mathbf{b} = \mathbf{0}$ . If  $m$  is large enough,  $C$  has minimum distance  $2e + 1$ . The code  $C$  is cyclic and hence contains a codeword  $\mathbf{c}$  of weight  $2e + 1$  beginning with 1. Therefore,

$$\begin{aligned} d(\mathbf{v}, C_0^{(1)}) + d(\mathbf{v}, C_1^{(1)}) &\leq d(\mathbf{v}, \mathbf{v}) + d(\mathbf{v}, \mathbf{v} + \mathbf{c}) \\ &= 0 + 2e + 1 \leq 4e - 1. \end{aligned}$$

Denote by  $\mathbf{v}'$  the result of complementing the first coordinate of  $\mathbf{v}$ . Since

$$d(\mathbf{v}, C_0^{(1)}) + d(\mathbf{v}, C_1^{(1)}) = d(\mathbf{v}', C_0^{(1)}) + d(\mathbf{v}', C_1^{(1)}),$$

we can now assume that  $\mathbf{v}$  is such that  $\mathbf{b} \neq \mathbf{0}, \mathbf{1}$ . It is sufficient to show that for all  $\mathbf{b} = (\beta_1, \dots, \beta_e) \in \mathbb{F}_q^e \setminus \{\mathbf{0}, \mathbf{1}\}$ , the system

$$\sum_{j=1}^{2e-1} x_j^{2i-1} = \beta_i, \quad i \in [1, e], \quad (10.4.2)$$

has a solution  $x_1, \dots, x_{2e-1}$  such that  $x_j \neq 1$  for all  $j$ .

If  $\beta_i = \beta_1^{2i-1}$  for all  $i \in [1, e]$ , then we simply choose  $x_1 = \beta_1, x_2 = \dots = x_{2e-1} = 0$ .

We can therefore assume that  $\beta_i \neq \beta_1^{2i-1}$  for some  $i$ . We need the following particular case of the Lang-Weil theorem.

**Theorem 10.4.3** *If  $e > 1$  and  $\beta_1, \dots, \beta_e$  are such that  $\beta_i \neq \beta_1^{2i-1}$  for some  $i \geq 2$ , then there is a constant  $A$  depending only on  $e$  such that the number  $N$  of solutions of the system (10.4.2) satisfies  $|N - q^{e-1}| \leq Aq^{e-3/2}$ .  $\square$*

Hence, the number of solutions of (10.4.2) is at least  $q^{e-1} - Aq^{e-3/2}$  for some constant  $A$ . In the same way as in the previous section, we see that the system

$$\sum_{j=1}^{2e-2} x_j^{2i-1} = \gamma_i y^{2i-1}, \quad i \in [1, e],$$

for  $\mathbf{g} = (\gamma_1, \dots, \gamma_e) \neq \mathbf{0}$ , has at most

$$S = \frac{q^{2e-2}(q-1) + ((q^e - q^{e-1})(\sqrt{q}(2e-2) + 1) + q^e - q)(2e-2)^{2e-2}q^{e-1}}{q^e}$$

solutions with  $y \neq 0$ ; therefore the number of solutions of (10.4.2) such that  $x_j = 1$  for some  $j$  is at most  $S(2e-1)/(q-1)$ . Hence, for a fixed  $e$  and  $q$  large enough, the number of solutions of (10.4.2) such that  $x_j \neq 1$  for all  $j$ , is positive.  $\square$

If we consider subnormality of BCH codes, then Theorem 4.2.18 implies that  $\mathcal{BCH}(e, m)$  is subnormal for fairly small values of  $m$ , and that  $C_1$  can be chosen a linear subcode of  $C$  of codimension one. This result however does not give any explicit description of  $C_1$ . In what follows we prove that if  $m$  is large enough, then we can choose  $C_1$  to be the even weight subcode  $C_e$  and  $C_2$  to be the odd weight subcode  $C_o$ . We need the following auxiliary lemma.

**Lemma 10.4.4** *If  $q = 2^m \geq (2e)^{4e+2}$ , then for every  $\mathbf{v} \in \mathbb{F}^n$  there exists a codeword  $\mathbf{c} \in \mathcal{BCH}(e, m)$  such that  $d(\mathbf{v}, \mathbf{c})$  is even and at most  $2e$ .*

**Proof.** We consider the system (10.3.3). We claim that it has a solution with  $x_j \neq 0$  for  $j \in [1, 2e]$ . The  $x_j$ 's may not be distinct, but if some of them are equal, they cancel pairwise, yielding a solution with still an even number of nonzero variables. To prove this, consider the system (10.3.4), proceed like in the proof of Theorem 10.3.1 but extend the sums to  $x_j$  over  $\mathbb{F}_q^*$  instead of  $\mathbb{F}_q$ .  $\square$

**Theorem 10.4.5** *If  $q = 2^m \geq (2e)^{4e+2}$ , then the code  $C = \mathcal{BCH}(e, m)$  is subnormal and the partition  $C = C_e \cup C_o$  is acceptable.*

**Proof.** Let  $\mathbf{v} \in \mathbb{F}^n$  be arbitrary and again  $\mathbf{v}' = \mathbf{v} + \mathbf{e}_1$ . For these lengths  $R = R(C)$  can be  $2e-1$  or  $2e$ .

Assume first that  $R = 2e$ . By the previous lemma there is a codeword  $\mathbf{c}$  such that  $d(\mathbf{v}, \mathbf{c})$  is even and at most  $2e$ ; similarly, there is a codeword  $\mathbf{c}'$  such that  $d(\mathbf{v}', \mathbf{c}')$  is even and at most  $2e$ . Now  $\mathbf{v}$  and  $\mathbf{c}$  have the same parity and so do  $\mathbf{v}'$  and  $\mathbf{c}'$ . As  $\mathbf{v}$  and  $\mathbf{v}'$  differ in exactly one coordinate they, and consequently  $\mathbf{c}$  and  $\mathbf{c}'$ , have different parities. Hence

$$d(\mathbf{v}, C_e) + d(\mathbf{v}, C_o) \leq d(\mathbf{v}, \mathbf{c}) + d(\mathbf{v}, \mathbf{c}') \leq 2e + 2e + 1 = 2R + 1.$$

Assume now that  $R = 2e-1$ . Choose  $\mathbf{c} \in C$  such that  $d(\mathbf{v}, \mathbf{c}) = d(\mathbf{v}, C)$ . Suppose first that  $d(\mathbf{v}, \mathbf{c})$  is odd. By the previous lemma there exists a codeword  $\mathbf{c}' \in C$  such that  $d(\mathbf{v}, \mathbf{c}')$  is even and at most  $2e$ . Again,  $\mathbf{c}$  and  $\mathbf{c}'$  have different parities and therefore

$$d(\mathbf{v}, C_e) + d(\mathbf{v}, C_o) \leq d(\mathbf{v}, \mathbf{c}) + d(\mathbf{v}, \mathbf{c}') \leq 2e - 1 + 2e = 2R + 1.$$

Suppose now that  $d(\mathbf{v}, \mathbf{c})$  is even and hence at most  $2e - 2$ . By the previous lemma there is a codeword  $\mathbf{c}'$  such that  $d(\mathbf{v}', \mathbf{c}')$  is even and at most  $2e$ . Again,  $\mathbf{c}$  and  $\mathbf{c}'$  have different parities and

$$d(\mathbf{v}, C_e) + d(\mathbf{v}, C_o) \leq d(\mathbf{v}, \mathbf{c}) + d(\mathbf{v}, \mathbf{c}') \leq 2e - 2 + 2e + 1 = 2R + 1.$$

□

## 10.5 Other algebraic codes

In this section we survey some known results about covering radii of particular classes of algebraic codes.

### Cyclic codes

Let  $C$  be a cyclic code of length  $(2^m - 1)/h$  with roots  $\alpha^{hi_1}, \dots, \alpha^{hi_e}$ . An approach analogous to the proof of Theorem 10.3.1 gives the following result.

**Theorem 10.5.1** *If  $m \geq (4e + 2) \log_2(h \max_{s \in [1, e]} i_s - 1)$ , then the covering radius does not exceed  $2e$ .* □

### Duals of BCH codes

We have seen in Section 10.1 that upper bounds on exponential sums give lower bounds on the minimum distance of duals of BCH codes. Determining the covering radius of duals of BCH codes is related to lower bounds on exponential sums.

Theorem 8.3.11, along with knowledge of the minimum distance of BCH codes (duals of the aforementioned) and the bound (2.3.32) on the minimal root of Krawtchouk polynomials give

#### Theorem 10.5.2

$$R_B^\perp(e, m) \leq 2^{m-1} - 1 - (\sqrt{e} - \sqrt[6]{e})\sqrt{2^m - e - 2}.$$

□

## Goppa codes

Consider a Goppa code  $\mathcal{GOP}(L, g)$ , where  $g(x)$  is a polynomial of degree  $e$  over  $\mathbb{F}_q$ ,  $q = 2^m$ . Moreover, assume that  $g(x)$  has no roots in  $\mathbb{F}_q$  (i.e.,  $L = \mathbb{F}_q$ ). To estimate the covering radius, we study the solvability of the system

$$\begin{array}{lllll} 1/g(x_1) + & \dots & +1/g(x_r) & = \beta_1 \\ x_1/g(x_1) + & \dots & +x_r/g(x_r) & = \beta_2 \\ \dots & \dots & \dots & \dots \\ x_1^{e-1}/g(x_1) + & \dots & +x_r^{e-1}/g(x_r) & = \beta_e. \end{array}$$

The approach is the same as in the proof of Theorem 10.3.1, but uses the following result of Bombieri instead of Theorem 10.1.7:

**Theorem 10.5.3** *Let  $q = 2^m$  and  $g(x)$  be a polynomial over  $\mathbb{F}_q$  of degree at most  $d_1$  with distinct roots over the algebraic closure of  $\mathbb{F}_q$ ,  $L = \mathbb{F}_q \setminus Z$ , where  $Z$  is the set of zeros of  $g(x)$  in  $\mathbb{F}_q$ , and  $f(x)$  be a polynomial of degree  $d_2$ . If the equation  $y^2 + y = f(x)/g(x)$  has no solution in  $\mathbb{F}_q$ , then*

$$\left| \sum_{x \in L} \psi(f(x)/g(x)) \right| \leq (d_1 + d_2 - 1)2^{m/2}.$$

□

Combining this theorem with additional considerations similar to those of Section 8.3 gives

**Theorem 10.5.4** *Provided  $2^m \geq (1 + \varepsilon(e))(e - 1)^{4e+2}$ ,*

$$R_{\mathcal{GOP}}(L, g) \leq 2e + 1,$$

where  $\varepsilon(2) = 1023$ ,  $\varepsilon(3) = 8.610^{-5}$ ,  $\varepsilon(e) \leq 1.0510^{-7}$  for  $e \geq 4$ . □

## Extremal doubly-even self-dual codes

Bounds on  $R_S(m)$ , the covering radius of extremal doubly-even self-dual codes of length  $n = 8m$ , are given in Table 10.2.

**Theorem 10.5.5**

$$R_S(m) \leq 2m - 2\lfloor m/3 \rfloor$$

and asymptotically

$$0.88m \approx 8mH^{-1}(1/2) \leq R_S(m).$$

**Proof.** The upper bound is simply Delsarte's, whereas the lower bound is the asymptotic sphere-covering bound. □

Table 10.2: Bounds on the covering radius of extremal doubly-even self-dual codes.

$n$	8	16	24	32	40	48	56	64
$k$	4	8	12	16	20	24	28	32
$d$	4	4	8	8	8	12	12	12
$R_S$	2	2	4	6	6–8	8	8–10	8–12

## Reed-Solomon codes

Reed-Solomon  $[n \leq q-1, n-d+1, d]_q$  or singly and doubly extended Reed-Solomon  $[q, q-d+1, d]_q, [q+1, q-d+2, d]_q$  codes meet the Singleton bound. To upperbound the covering radius of these codes, one may use the redundancy bound (Theorem 8.1.3), thus getting

**Lemma 10.5.6** *For  $n \leq q+1$ ,*

$$R_{RS}(q, d, n) \leq d-1.$$

□

To derive lower bounds we use the supercode lemma along with the fact that Reed-Solomon and singly extended Reed-Solomon codes constitute a nested family. This and Lemma 10.5.6 give

**Theorem 10.5.7**

$$R_{RS}(q, d, n \leq q) = d-1.$$

□

## 10.6 Notes

§10.1 For more information on true designed distance and dimension of BCH codes, see, e.g., MacWilliams and Sloane [464] and references therein. Some BCH codes are nested in Reed-Muller codes, see Zinoviev and Litsyn [714] for details. Theorem 10.1.7 is by A. Weil [684] and Carlitz and Uchiyama [126]. The relation between the duals of BCH codes and characters was found by D. Anderson [21]. The estimate (10.1.8) may be tightened in some cases, for such results see Cáceres and O. Moreno [109], Litsyn, C. J. Moreno and

O. Moreno [443], O. Moreno and C. J. Moreno [500] and Rodier [556], [557], [558]. For the dual spectra of BCH codes, see Kasami [366].

§10.2 Theorem 10.2.3 is by Gorenstein, Peterson and Zierler [264]. The study of  $R_B(3, m)$  was started by van der Horst and Berger [330] who proved the result for  $m \equiv 0 \pmod{4}$ . Later Assmus and Mattson [25] used the result of Kasami [366] on the number of weights in the duals of two-error-correcting BCH codes, to derive the result using the Delsarte bound. The last case,  $m \equiv 2 \pmod{4}$ , was solved by Helleseth [295]. It would be very desirable to have a more direct proof of Theorem 10.2.6.

§10.3 The exponential sum approach was suggested by Helleseth [297], who proved Theorem 10.3.1 in a weaker version, namely with the upper bound  $2e + 1$ . For an earlier result see Helleseth [296]. Theorem 10.3.1 is due to Tietäväinen [643]. Theorem 10.3.5 is due to Levy-dit-Vehel and Litsyn [421], where the choice of the polynomial  $g_{2e}(x)$  minimizing the ratio  $g_{2e}(0)/m_0$  is proved to be optimal under some not very restrictive conditions. The theorem is stated here in the form suggested by Hirvensalo. For Deligne's theorem see [191]. Theorem 10.3.9 is by Tietäväinen [644], [645]. The first proof of Theorem 10.3.12, without explicit minimal length, was given by Vlăduț and Skorobogatov [673] (see also [589]). They used tools from algebraic geometry and the theorem of Lang and Weil (see Theorem 10.4.3). O. Moreno and C. J. Moreno [499] and Kaipainen [356] present explicit lower bounds on the minimal length. The theorem in its present form is proved by S. D. Cohen [173].

Theorem 10.3.13 is by Levy-dit-Vehel and Litsyn [421]. The fact that  $2e$  is a lower bound was proved earlier by Vlăduț and Skorobogatov [673]. We present here the proof of [421]. By mistake, (10.1.2) is used also in the nonprimitive case in Theorems 1 and 5 in Honkala, Litsyn and Tietäväinen [327] and in Theorem 3 in [421], leading to a smaller lower bound on  $q$  in Theorem 10.3.15. For earlier results see Helleseth [297], Tietäväinen [643] and Vlăduț and Skorobogatov [673].

Kaipainen [357] studied the covering radius of nonbinary long BCH codes. His upper bounds are quite close to the lower bounds given by the supercode lemma. For instance, in the ternary primitive case, for  $m$  large enough,

$$e \leq R_B(e, m) \leq \begin{cases} e + 1 & \text{if } e \equiv 1 \pmod{3}, \\ e + 2 & \text{otherwise.} \end{cases}$$

§10.4 We follow Honkala, Kaipainen and Tietäväinen [324]. The theorem of Lang and Weil is from [409]. An analogous technique was used in [324] to derive similar results about normality and subnormality of nonprimitive BCH codes.

§10.5 Theorem 10.5.1 is due to Helleseth [297] and Tietäväinen [643]. In Downie and Sloane [210] one may find computer calculations of the covering radius for cyclic codes of lengths up to 31. The most extensive table can be found in Dougherty and Janwa [209], collecting the results for all cyclic codes of lengths up to 63 with redundancy up to 28. Many of these codes are optimal in the sense of having the smallest possible covering radius of any linear code with the same length and dimension. The covering radius of some classes of cyclic double-error-correcting codes, among them Melas and Zetterberg codes, is studied by O. Moreno [498] and Dodunekov [202], [203]. For other results see Velikova [667], [668] and Velikova and K. N. Manev [671]. Baicheva [37], [39] studies covering radii of ternary cyclic codes.

Theorem 10.5.2 is by Tietäväinen [646], [648]. Recalling the definition of the duals of BCH codes via values of additive characters of polynomials, we have the following expression for  $C = \mathcal{BCH}^\perp(e, m)$ :

$$\begin{aligned} R_B^\perp(e, m) &= \max_{\mathbf{a} \in \mathbb{F}^n} \min_{\mathbf{c} \in C} w(\mathbf{a} + \mathbf{c}) \\ &= \frac{1}{2} \left( q - \min_g \max_f \sum_{\beta \in \mathbb{F}_q} \psi(g(\beta) + f(\beta)) \right), \end{aligned}$$

where the minimum is taken over all polynomials  $g$  over  $\mathbb{F}_q$ , and the maximum extends over the polynomials  $f = \alpha_1 x + \alpha_2 x^3 + \dots + \alpha_e x^{2e-1}$  over  $\mathbb{F}_q$ . Thus, by Theorem 10.5.2, we have

$$\min_g \max_f \sum_{\beta \in \mathbb{F}_q} \psi(g(\beta) + f(\beta)) \geq 2 + 2(\sqrt{e} - \sqrt[3]{e})\sqrt{q - e - 2}. \quad (10.6.1)$$

On the other hand, taking  $g = 0$  we get

$$\max_f \sum_{\beta \in \mathbb{F}_q} \psi(f(\beta)) \geq \min_g \max_f \sum_{\beta \in \mathbb{F}_q} \psi(g(\beta) + f(\beta)).$$

Lower bounds for the left hand side of the last expression have been extensively studied, see Levenshtein [416], [417] and Tarnanen [633]. The best known bounds (see, e.g., [416]) have order  $2\sqrt{eq}$ . Thus, any essential improvement of Theorem 10.5.2 would lead to improving on the lower bounds for exponential sums.

For the Bombieri theorem see [91]. Theorem 10.5.4 is by Levy-dit-Vehel and Litsyn [420]. For other results see C. J. Moreno and O. Moreno [496], [497] and Levy-dit-Vehel and Litsyn [422]. Table 10.2 and Theorem 10.5.5 are by Assmus and Pless [27]. Dür [213] considers the covering radius of extended Reed-Solomon codes.

The covering radius of algebraic-geometric codes is studied by Janwa [345], [347], [348]. For estimates of the covering radius of binary subcodes of algebraic-geometric codes, see Skorobogatov [590].

This Page Intentionally Left Blank

# Chapter 11

## Perfect codes

Perfect codes are fascinating objects which have been thoroughly studied; almost everything is known about them. We remind the reader that an  $e$ -error-correcting code with length  $n$  and covering radius  $R$  is perfect if the following three equivalent properties are satisfied:

- equality holds for the sphere-packing, or Hamming, bound, i.e., the spheres of radius  $e$ , centred at the codewords, not only do not intersect but also fill the whole space of length  $n$ ;
- equality holds for the sphere-covering bound, i.e., the spheres of radius  $R$ , centred at the codewords, not only fill the whole space but also do not intersect;
- the covering radius  $R$  of the code is equal to its error-correcting capacity  $e$ .

In Section 11.1, we list some perfect codes which, as we shall see in the following section, are the only perfect linear codes over  $\mathbb{F}_q$  (up to equivalence); we construct the  $q$ -ary Hamming codes (of length  $n = (q^m - 1)/(q - 1)$ , dimension  $n - m$ , covering radius one and minimum distance three), the binary Golay code (of length 23, dimension 12, covering radius three and minimum distance seven) and the ternary Golay code (of length 11, dimension 6, covering radius two and minimum distance five). Section 11.2 states a famous nonexistence result. In Sections 11.3 and 11.4, families of perfect nonlinear single-error-correcting codes over  $\mathbb{F}_q$  are described, Section 11.3 being exclusively devoted to the binary case; these codes have the same parameters as the Hamming codes. Section 11.5 deals briefly with perfect mixed codes. The figure at the end of Section 11.5 illustrates the relationships between the different constructions described in Sections 11.3, 11.4 and 11.5. Section 11.6 studies some generalizations of perfect codes. Notes at the end of the chapter provide further comments and references, for instance on some other generalizations of perfect codes, on the case of composite alphabet size, or on mixed codes.

## 11.1 Perfect linear codes over $\mathbb{F}_q$

Perfect codes can be characterized via two simple bounds. The first one, the sphere-packing bound, also known as the Hamming bound, gives a necessary condition for a  $q$ -ary  $(n, K)$  code  $C$  to be  $e$ -error-correcting; since the  $K$  spheres of radius  $e$  centred at the codewords must not intersect, we get the inequality

$$K \cdot V_q(n, e) \leq q^n. \quad (11.1.1)$$

On the other hand, the sphere-covering bound gives a necessary condition for  $C$  to have covering radius  $R$ ; since the  $K$  spheres of radius  $R$  centred at the codewords must cover the whole space  $\mathbb{F}_q^n$ , the following inequality is satisfied

$$K \cdot V_q(n, R) \geq q^n. \quad (11.1.2)$$

If equality holds in (11.1.1), then  $R = e$  and equality holds in (11.1.2). If equality holds in (11.1.2), then  $e = R$  and equality holds in (11.1.1). If  $R = e$ , then equality holds in (11.1.1) and in (11.1.2). In all cases,  $C$  is said to be perfect (of course this can be generalized to composite  $q$  or to mixed codes).

We now describe the perfect linear codes over  $\mathbb{F}_q$ , with their parameters  $[n, k, d]_R$ .

**Trivial perfect codes.** For all  $n \geq 1$  and all  $q \geq 2$ ,  $\{0^n\}$  is a  $q$ -ary perfect  $[n, 0]_n$  code (any singleton is a perfect  $(n, 1)_n$  code) and  $\mathbb{F}_q^n$  is a  $q$ -ary perfect  $[n, n, 1]_0$  code.

**Repetition codes.** For all  $n \geq 0$ , the binary repetition codes  $\{0^{2n+1}, 1^{2n+1}\}$  with odd length are perfect  $[2n+1, 1, 2n+1]_n$  codes (and any pair of complementary vectors is a perfect  $(2n+1, 2, 2n+1)_n$  code).

**Hamming codes.** These are linear codes over  $\mathbb{F}_q$  with the following parameters:  $n = (q^m - 1)/(q - 1)$ ,  $k = n - m$ . They have  $m \times (q^m - 1)/(q - 1)$  parity check matrices, whose columns are all the nonzero  $m$ -tuples from  $\mathbb{F}_q$  with the first nonzero coordinate equal to 1. Their covering radius is one. Since  $q^{n-m}(1 + (q - 1)n) = q^n$ , the sphere-covering bound is satisfied with equality and these codes are perfect. Their minimum distance is three.

**The binary Golay code.** Consider the binary square matrices

$$\mathbf{G}_{11} = \left( \begin{array}{cccccccccc} 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \end{array} \right)$$

and

$$\mathbf{G}_{12} = \left( \begin{array}{c|cccc} 0 & 1 & 1 & \dots & 1 \\ \hline 1 & & & & \\ \vdots & & & & \\ 1 & & & & \mathbf{G}_{11} \end{array} \right).$$

Let  $C_{23}$  and  $C_{24}$  be the two codes of dimension 12 spanned by the rows of the matrices

$$\mathbf{G}_{23} = \left( \begin{array}{c|cccc} \mathbf{I}_{12} & \begin{array}{cccc} 1 & 1 & \dots & 1 \end{array} \\ \hline & \mathbf{G}_{11} \end{array} \right)$$

and

$$\mathbf{G}_{24} = (\mathbf{I}_{12} | \mathbf{G}_{12}) = \left( \begin{array}{c|cccc} \mathbf{I}_{12} & \begin{array}{cccc} 0 & 1 & 1 & \dots & 1 \end{array} \\ \hline \mathbf{I}_{12} & \begin{array}{c|cccc} 1 & & & & \\ \vdots & & & & \\ 1 & & & & \mathbf{G}_{11} \end{array} \end{array} \right).$$

The code  $C_{24}$  is called the *extended binary Golay code* and  $C_{23}$  the *binary Golay code*. We first show by combinatorial arguments that  $C_{24}$  has minimum distance 8. Then it is immediate to prove that the binary Golay code  $C_{23}$  has minimum distance 7, covering radius 3 and is perfect.

Consider any two distinct rows,  $\mathbf{g}_1$  and  $\mathbf{g}_2$ , in  $\mathbf{G}_{11}$ . It is easy to verify that the weight of their componentwise product  $\mathbf{g}_1 * \mathbf{g}_2$  is equal to 3; indeed because all the rows of  $\mathbf{G}_{11}$  are cyclic shifts of the first row, it suffices to compare the first row with the other ones. Denoting by  $\mathbf{c}_1, \mathbf{c}_2, \dots, \mathbf{c}_{12}$  the rows of  $\mathbf{G}_{24}$ , we get immediately:

- for any  $i, j$  such that  $i \neq 1, j \neq 1$  and  $i \neq j$ ,  $w(\mathbf{c}_i * \mathbf{c}_j) = 4$ ;
- $w(\mathbf{c}_1 * \mathbf{c}_1) = 12$ ;
- for any  $i \neq 1$ ,  $w(\mathbf{c}_i * \mathbf{c}_i) = 8$ ;
- for any  $i \neq 1$ ,  $w(\mathbf{c}_1 * \mathbf{c}_i) = 6$ .

This implies that for all  $i, j$ , the scalar product of  $\mathbf{c}_i$  and  $\mathbf{c}_j$  is equal to 0, i.e., the extended binary Golay code is self-dual.

**Theorem 11.1.3**  $C_{24} = C_{24}^\perp$ . □

**Corollary 11.1.4** *The matrix  $(\mathbf{G}_{12} \mid \mathbf{I}_{12})$  is a generator matrix of the code  $C_{24}$ .*

**Proof.** Follows directly from Section 2.1. □

**Theorem 11.1.5** *The weight of any codeword in  $C_{24}$  is a multiple of 4.*

**Proof.** Let  $\mathbf{c} \in C_{24}$  be the sum of some  $\lambda$  rows of  $\mathbf{G}_{24}$ . The proof is by induction on  $\lambda$ . The claim is clear for  $\lambda = 1$ . Assume that it is true whenever  $\mathbf{c}$  is a sum of at most  $\lambda$  rows of  $\mathbf{G}_{24}$ .

Assume that  $\mathbf{c}' = \mathbf{c}_i + \mathbf{c}''$ , where  $\mathbf{c}_i$  is a row of  $\mathbf{G}_{24}$  and  $\mathbf{c}''$  is a sum of  $\lambda$  rows of  $\mathbf{G}_{24}$ . Then by (2.1.7),  $w(\mathbf{c}')$  is equal to  $w(\mathbf{c}_i) + w(\mathbf{c}'') - 2w(\mathbf{c}_i * \mathbf{c}'')$  which is divisible by four, because the first two terms are divisible by four by the induction hypothesis and the last one by Theorem 11.1.3. □

**Theorem 11.1.6** *No codeword in  $C_{24}$  has weight 4.*

**Proof.** Assume that  $\mathbf{x} = (\mathbf{y}|\mathbf{z})$  is a codeword of weight 4, where  $\mathbf{y}$  and  $\mathbf{z}$  have length 12.

- If  $w(\mathbf{y}) \leq 1$ , then either  $\mathbf{x} = \mathbf{0}^{24}$  or  $\mathbf{x}$  is a row of  $\mathbf{G}_{24}$ , a contradiction.
- If  $w(\mathbf{y}) = 2$ , then  $\mathbf{x}$  is the sum of two distinct rows of  $\mathbf{G}_{24}$ ,  $\mathbf{c}_i$  and  $\mathbf{c}_j$ . Clearly  $w(\mathbf{c}_1 + \mathbf{c}_\lambda) = 8$  for every  $\lambda > 1$ , and therefore  $i, j > 1$ . But then  $w(\mathbf{c}_i + \mathbf{c}_j) = w(\mathbf{c}_i) + w(\mathbf{c}_j) - 2w(\mathbf{c}_i * \mathbf{c}_j) = 8 + 8 - 2 \cdot 4 = 8$ , a contradiction.
- If  $w(\mathbf{y}) \geq 3$ , then  $w(\mathbf{z}) \leq 1$ . By Corollary 11.1.4 however,  $\mathbf{x}$  is a linear combination of rows of  $(\mathbf{G}_{12} \mid \mathbf{I}_{12})$ ; the number of these rows,  $w(\mathbf{z})$ , is at most one, which is impossible. □

**Theorem 11.1.7** *The code  $C_{24}$  has minimum distance 8 and its codewords have weights in  $W = \{0, 8, 12, 16, 24\}$ .*

**Proof.** We have to consider only multiples of 4. The all-one row vector belongs to  $C_{24}$  ( $1^{24}$  is the sum of all the rows of  $\mathbf{G}_{24}$ ), hence if  $w \in W$ , so does  $24 - w$ . Consequently, there is no codeword with weight 20. The first row of  $\mathbf{G}_{24}$  has weight 12 and there are rows with weight 8, so  $\{8, 12, 16\} \subset W$ .  $\square$

**Corollary 11.1.8** *The binary Golay code  $C_{23}$  has minimum distance 7.*

**Proof.** By construction,  $\mathbf{G}_{23}$  is obtained from  $\mathbf{G}_{24}$  by deleting its thirteenth column. So  $C_{23}$  has minimum distance 7 or 8. But the second row of  $\mathbf{G}_{23}$  has weight 7.  $\square$

**Corollary 11.1.9** *The binary Golay code is a  $[23, 12, 7]_3$  perfect code.*

**Proof.** The sphere-covering bound is satisfied with equality.  $\square$

**The ternary Golay code.** Consider the ternary square matrices

$$\mathbf{G}_5^{(3)} = \begin{pmatrix} 0 & 1 & 2 & 2 & 1 \\ 1 & 0 & 1 & 2 & 2 \\ 2 & 1 & 0 & 1 & 2 \\ 2 & 2 & 1 & 0 & 1 \\ 1 & 2 & 2 & 1 & 0 \end{pmatrix}$$

and

$$\mathbf{G}_6^{(3)} = \left( \begin{array}{c|ccccc} 0 & 1 & 1 & \dots & 1 \\ \hline 1 & & & & & \\ \vdots & & & & & \\ 1 & & & & \mathbf{G}_5^{(3)} & \end{array} \right).$$

Let  $C_{11}^{(3)}$  and  $C_{12}^{(3)}$  be the two codes of dimension 6 spanned by the rows of the matrices

$$\mathbf{G}_{11}^{(3)} = \left( \begin{array}{c|ccccc} & 1 & 1 & \dots & 1 \\ \hline \mathbf{I}_6 & & & & & \\ & & & & & \mathbf{G}_5^{(3)} \end{array} \right)$$

and

$$\mathbf{G}_{12}^{(3)} = \left( \begin{array}{c|c} \mathbf{I}_6 & \mathbf{G}_6^{(3)} \end{array} \right) = \left( \begin{array}{c|c} \mathbf{I}_6 & \begin{array}{c|cccc} 0 & 1 & 1 & \dots & 1 \\ \hline 1 & & & & \\ \vdots & & & & \\ 1 & & & & \mathbf{G}_5^{(3)} \end{array} \end{array} \right).$$

The code  $C_{12}^{(3)}$  is called the *extended ternary Golay code* and  $C_{11}^{(3)}$  the *ternary Golay code*. As for the binary and binary extended Golay codes, it is easy to prove that  $C_{12}^{(3)}$  is self-dual and has minimum distance 6, and that  $C_{11}^{(3)}$  therefore has minimum distance 5.

**Corollary 11.1.10** *The ternary Golay code is a  $[11, 6, 5]_2$  perfect code.*

**Proof.** The sphere-covering bound is satisfied with equality.  $\square$

## 11.2 A nonexistence result

Since many people failed to discover parameters of perfect codes over  $\mathbb{F}_q$  other than those mentioned in the previous section, a considerable amount of work was devoted to nonexistence results (e.g., by van Lint, Zinoviev and Leontiev, and Tietäväinen) and led to a remarkable conclusion (see Theorem 11.2.2 below).

To that end, we need the following result, known as *Lloyd's theorem*, which gives a necessary condition for the existence of perfect codes.

**Theorem 11.2.1** *If a perfect code of length  $n$  and covering radius  $R$  over  $\mathbb{F}_q$  exists, then the Lloyd polynomial  $L_R(x) = \sum_{i=0}^R (-1)^i (q-1)^{R-i} \binom{x-1}{i} \binom{n-x}{R-i}$  has  $R$  integer zeros  $x_1, \dots, x_R$  such that  $0 < x_1 < \dots < x_R \leq n$ .*  $\square$

For a proof of this result, see Section 13.2, where the Lloyd theorem is given in the more general case of perfect weighted coverings (Theorem 13.2.5).

The following theorem was finally obtained in the early seventies.

**Theorem 11.2.2** *A nontrivial perfect code over  $\mathbb{F}_q$  necessarily has the same parameters as one of the binary repetition codes with odd length, or  $q$ -ary Hamming codes, or binary or ternary Golay codes.*

The first proof was long, complicated and used a computer search. Later the proof could be shortened and the computer search avoided.

**Proof.** Let  $L_R(x) = \sum_{i=0}^R \ell_i x^i$ . A perfect code  $C$  of length  $n$  and covering radius  $R$  over  $\mathbb{F}_q$  must satisfy the sphere-covering bound (11.1.2) with equality:

$$|C| \cdot \sum_{i=0}^R (q-1)^i \binom{n}{i} = q^n.$$

Since  $q$  is a prime power, say  $q = p^r$ , necessarily  $\sum_{i=0}^R (q-1)^i \binom{n}{i}$  is also a power of  $p$ , say  $p^j$ . Hence  $\sum_{i=1}^R (q-1)^i \binom{n}{i} = p^j - 1$ ,  $q-1 = p^r - 1$  divides  $p^j - 1$  and  $r$  divides  $j$ . This proves that there is an integer  $m = j/r$  such that

$$\sum_{i=0}^R (q-1)^i \binom{n}{i} = q^m. \quad (11.2.3)$$

This equation was the starting point for the first nonexistence results, sometimes with the help of a computer (for instance, the case  $R \leq 1000$ ,  $q \leq 100$  and  $n \leq 1000$  was settled this way). Then van Lint [430] observed in 1969 that combining Lloyd's theorem with (11.2.3) gives

$$\ell_0 = L_R(0) = \sum_{i=0}^R (q-1)^i \binom{n}{i} = q^m. \quad (11.2.4)$$

Therefore computing the coefficient  $\ell_R$  of  $x^R$  in  $L_R(x)$  shows that the product of the zeros  $x_1, x_2, \dots, x_R$  of  $L_R(x)$  has a simple form:

$$x_1 x_2 \dots x_R = \frac{(-1)^R \ell_0}{\ell_R} = \frac{R!}{q^R} \sum_{i=0}^R (q-1)^i \binom{n}{i} = R! q^{m-R}. \quad (11.2.5)$$

Now (11.2.5) combined with:

$$x_1 + x_2 + \dots + x_R = \frac{-\ell_{R-1}}{\ell_R} = \frac{R(n-R)(q-1)}{q} + \frac{R(R+1)}{2} \quad (11.2.6)$$

gave new nonexistence results for  $R \leq 7$  and arbitrary  $q = p^r$ , as well as for  $R \geq 3$  and  $q = p^r$  with  $p > R$ .

Then it was observed that, because of the divisibility properties implied by (11.2.5), all the  $x_i$ 's cannot be very close to each other. But (11.2.5) and (11.2.6) also imply that the arithmetic mean and the geometric mean of the  $x_i$ 's must be very close to each other. This combined with the Bassalygo-Elias lemma (see Lemma 12.6.6) and earlier nonexistence results finally gave the first proof of Theorem 11.2.2 in Tietäväinen [640], Tietäväinen and Perko [649] and independently Zinoviev and Leontiev [712], [713].

Shortening the proof was possible using the formula

$$\prod_{i=1}^R (x_i - 1) = \frac{(-1)^R L_R(1)}{\ell_R} = (q-1)^R \frac{(n-1)(n-2)\dots(n-R)}{q^R}. \quad (11.2.7)$$

Let  $A$  be defined by

$$x_1 x_2 \dots x_R = A \left( \frac{x_1 + \dots + x_R}{R} \right)^R. \quad (11.2.8)$$

By the arithmetic/geometric-mean inequality,  $A \leq 1$ , and if the  $x_i$ 's are not close to each other,  $A$  can be much smaller than 1. Now (11.2.4), (11.2.5), (11.2.6) and (11.2.8) show that

$$\frac{R!}{q^R} \sum_{i=0}^R (q-1)^i \binom{n}{i} = A \left( \frac{(n-R)(q-1)}{q} + \frac{R+1}{2} \right)^R, \quad (11.2.9)$$

and when  $q(R-1) \geq 2R$ :

$$\frac{R!}{q^R} \sum_{i=0}^R (q-1)^i \binom{n}{i} \leq A \left( \frac{n(q-1)}{q} \right)^R. \quad (11.2.10)$$

We are now ready to give a shortened proof of Theorem 11.2.2. We assume that  $C$  is a nontrivial perfect code of length  $n$  and covering radius  $R$  over  $\text{IF}_q$ , with  $n > 2R+1$  (thus the repetition codes are excluded).

- Case  $R = 1$ . Using (11.2.5) and (11.2.6), we obtain  $q^m = qx_1 = n(q-1)+1$ ,  $n = (q^m-1)/(q-1)$  and  $|C| = q^{n-m}$ ; we are in the case of Hamming codes.
- Case  $R = 2$ . By (11.2.5) we have  $x_1 x_2 = 2q^{m-2} = 2p^{j-2r}$ , which means that
  - either  $x_1 = p^i$ ,  $x_2 = 2p^{i'}$  for some  $i' \geq i$ , in which case  $x_2/x_1 \geq 2$ ;
  - or  $x_1 = 2p^i$  and  $x_2 = p^{i'}$ , in which case  $x_2/x_1 \geq 3/2$  if  $p = 3$ , and  $x_2/x_1 \geq 2$  if  $p \neq 3$ .

Therefore  $A \leq 8/9$  if  $p \neq 3$ , and  $A \leq 24/25$  if  $p = 3$ . Using (11.2.10) for  $q \geq 4$ , or (11.2.9) for  $q = 2, 3$ , we obtain, if  $q \geq 4$ :

$$n(n-1) \frac{(q-1)^2}{q^2} < A \left( \frac{n(q-1)}{q} \right)^2,$$

i.e.,

$$n - 1 < An;$$

if  $q = 3$ :

$$\frac{2}{9} (2n^2 + 1) \leq \frac{24}{25} \left( \frac{4n+1}{6} \right)^2;$$

if  $q = 2$ :

$$\frac{n^2 + n + 2}{4} \leq \frac{8}{9} \left( \frac{n+1}{2} \right)^2.$$

The case  $q = 2$  leads to  $(n-5)(n-2) \leq 0$ , which cannot be satisfied for  $n > 5 = 2R+1$ . If  $q = 3$ , then  $n \leq 11$ . Using (11.2.6) shows that 3 must divide  $n-2$ , so 3 cannot divide  $n-1$ . Combined with (11.2.7), this shows that 9 divides  $n-2$ . Hence  $n = 11$  and we are in the case of the ternary Golay code. When  $q \geq 4$ , then  $n < 9$  when  $p \neq 3$ , and  $n < 25$  when  $p = 3$ . This contradicts (11.2.7), because (11.2.7) implies that  $q^2$  divides  $(n-1)(n-2)$  and therefore  $n \geq 1 + q^2$ , i.e.,  $n \geq 17$  for  $p \neq 3$ , and  $n \geq 82$  for  $p = 3$ .

– Case  $R = 3$  and  $q = 2$ . Using (11.2.5) gives  $x_1 x_2 x_3 = 3 \cdot 2^{m-2}$ , which implies that two of the three integers  $x_1, x_2, x_3$  are powers of 2 and the third is of the form  $3 \cdot 2^i$ . This eventually leads to  $A = 8/9$  or  $A \leq 96/125$ . If  $A = 8/9$ , then, by (11.2.9), we have  $(n+1)(n-2)(n-23) = 0$ . Since  $n > 2R+1 = 7$ , we find the parameters of the binary Golay code. If  $A \leq 96/125$ , then (11.2.9) yields  $(n+1)(29n^2 - 317n + 654) \leq 0$ , which implies  $n \leq 8$ , i.e.,  $n = 8$ . But 2 must divide  $n-3$  by (11.2.6), a contradiction.

– Case  $R \geq 3$  and  $q > 2$ . By (11.2.5),  $x_1 x_2 \dots x_R = R! q^{m-R} = R! p^{r(m-R)}$ . Write the  $x_i$ 's in the form  $x_i = a_i p^{\alpha_i}$ , where  $a_i$  and  $p$  are coprime. Now  $a_1 a_2 \dots a_R \leq R!$ . So either two of the  $a_i$ 's are equal, or all the  $a_i$ 's are distinct and equal to  $1, 2, \dots, R$  in some order and  $p > R \geq 3$ . In the first case,  $p$  divides  $x_{i'}/x_i$  for some  $i \neq i'$ . In both cases,  $x_R/x_1 \geq 2$ . Using the arithmetic/geometric-mean inequality, we get

$$x_1 x_2 \dots x_R \leq \frac{8}{9} \left( \frac{x_1 + x_R}{2} \right)^2 \left( \frac{x_2 + \dots + x_{R-1}}{R-2} \right)^{R-2} \leq \frac{8}{9} \left( \frac{x_1 + \dots + x_R}{R} \right)^R,$$

so  $A \leq 8/9$ . Combined with (11.2.10), this yields:

$$n(n-1) \dots (n-R+1) < \frac{8}{9} n^R.$$

The repeated application of the trivial inequality  $(n-a)(n-b) \geq n(n-a-b)$  (for nonnegative  $a$  and  $b$ ) leads to  $n(n-1) \dots (n-R+1) \geq n^{R-1} (n - \frac{R(R-1)}{2})$  and finally

$$n < \frac{9R(R-1)}{2}. \quad (11.2.11)$$

But  $p^{rR}$  must divide  $\mathcal{P} := (n-1)(n-2)\dots(n-R)$ , by (11.2.7). Let  $\lambda$  and  $\Lambda$  be the largest integers such that  $p^\lambda$  divides  $\mathcal{P}$  and  $p^\Lambda$  divides any of the factors  $n-i$ . Then

$$\lambda \leq \sum_{i=1}^{\Lambda} \left\lceil \frac{R}{p^i} \right\rceil \leq \Lambda + \sum_{i=1}^{\Lambda} \frac{R}{p^i} \leq \Lambda + \frac{R}{p-1}. \quad (11.2.12)$$

Because  $\lambda \geq rR$ , we get

$$n > p^\Lambda \geq p^{R(r-\frac{1}{p-1})} \geq p^{Rr/2} = q^{R/2}. \quad (11.2.13)$$

By (11.2.11) and (11.2.13), we obtain  $3^{R/2} \leq q^{R/2} < n < \frac{9R(R-1)}{2}$ , which implies that  $R \leq 11$ ,  $q \leq 8$  and  $n \leq 494$ . We already mentioned that nonexistence results had been obtained in this range. This settles the case  $R \geq 3$ ,  $q > 2$ .

– Case  $R \geq 4$  and  $q = 2$ . In this last case, we make use of the formula

$$\prod_{i=1}^R (x_i - 2) = \frac{(-1)^R L_R(2)}{\ell_R} = \frac{(n-2)(n-3)\dots(n-R)(n-2R-1)}{2^R}. \quad (11.2.14)$$

The combination of (11.2.7), (11.2.14) and the fact that  $(x_i - 1)(x_i - 2)$  is even, yields

$$\mathcal{Q} := (n-1)(n-2)^2(n-3)^2\dots(n-R)^2(n-2R-1) \equiv 0 \pmod{2^{3R}}.$$

Let  $\beta$  and  $\alpha$  be the largest integers such that  $2^\beta$  divides  $\mathcal{Q}$  and  $2^\alpha$  divides any of the factors  $n-i$ , say  $n-s$ . The difference between any two distinct factors is at most  $2R$ . If  $s \neq 2R+1$ , this implies, together with (11.2.12), that  $2^\beta \leq 2R \cdot 2^{2R+2\alpha}$ . When  $s = 2R+1$  the same result holds since

$$\beta \leq \alpha + 2 + \sum_{i=1}^{\min\{\alpha, \lfloor \log_2(2R) \rfloor\}} \left\lceil \frac{R}{2^i} \right\rceil \leq \alpha + (\log_2(2R) + R) + (\alpha + R).$$

This implies that  $3R \leq \beta \leq 2R + 2\alpha + \log_2(2R)$  and

$$n > 2^\alpha \geq \frac{2^{R/2}}{\sqrt{2R}}.$$

The rest of the proof for the case  $R \geq 4$  and  $q = 2$  is very similar to that of the case  $R \geq 3$  and  $q > 2$ . It finally leads to  $R \leq 29$  and  $n \leq 3652$ . Now a

computer search showed that there are no unknown perfect codes in the range  $R \leq 100$  and  $n \leq 10000$ .  $\square$

We now give results on the uniqueness of the Golay codes (equivalent codes are defined in Section 2.1 and at the beginning of next section).

**Theorem 11.2.15** *Let  $C$  be any  $(24, K, 8)$  binary code; then  $K \leq 2^{12}$  and if  $K = 2^{12}$ ,  $C$  is equivalent to the extended binary Golay code.*  $\square$

**Corollary 11.2.16** *Any  $(23, 2^{12})3$  binary code is equivalent to the binary Golay code.*  $\square$

**Theorem 11.2.17** *Let  $C$  be any  $(12, K, 6)$  ternary code; then  $K \leq 3^6$  and if  $K = 3^6$ ,  $C$  is equivalent to the extended ternary Golay code.*  $\square$

**Corollary 11.2.18** *Any  $(11, 3^6)2$  ternary code is equivalent to the ternary Golay code.*  $\square$

These results were first proved in their linear version by Pless [541] in 1968. Snover [598] proved Theorem 11.2.15 in 1973. Delsarte and Goethals [195] gave a new proof of it and proved Theorem 11.2.17 in 1975.

Theorem 11.2.2 does not exhaust the topic. Although the case of the binary and ternary Golay codes is completely settled by the above results, the situation of the Hamming codes is quite different: it is easy to see that any *linear* code with the Hamming parameters is necessarily equivalent to a Hamming code. But families of nonlinear codes with the same parameters as the Hamming codes exist and are described in the next two sections. Finding all perfect nonlinear codes with covering radius one over  $\mathbb{F}_q$  is still an open problem and, even in the binary case, a very difficult one!

It is necessary here to go back over the meanings of linear and nonlinear that we use through the following sections. Strictly speaking, if  $C$  is a perfect linear code, a coset  $C_1$  of  $C$  which does not contain the all-zero vector is a nonlinear perfect code. However, the codes  $C$  and  $C_1$  are equivalent. In the following, we use, rather informally, the word *linear* for codes which are *equivalent to a linear code* and the word *nonlinear* for codes which are *not equivalent to any linear code*.

### 11.3 Enumeration of perfect binary codes

This section deals with perfect codes with covering radius one (or equivalently perfect single-error-correcting codes) over  $\mathbb{F}_2$ , that are not equivalent to any linear code, and gives a comprehensive discussion of all the constructions, known to us, presented in various contexts. For some of these families of codes, it is possible to give a lower bound on the number of nonequivalent codes which they contain or to prove that they are nonequivalent or nonisomorphic to other previously known families.

**Definition 11.3.1** *Two  $(n, K)$  codes  $C_1$  and  $C_2$  over  $\mathbb{F}_q$  are said to be equivalent if there are  $n$  permutations  $\tau_1, \dots, \tau_n$  of the  $q$  elements in  $\mathbb{F}_q$  and a permutation  $\sigma$  of the  $n$  components such that if  $(c_1, \dots, c_n) \in C_1$ , then  $\sigma(\tau_1(c_1), \dots, \tau_n(c_n)) \in C_2$ . In the binary case, this is equivalent to the existence of a permutation  $\sigma \in S_n$  and a vector  $\mathbf{a} \in \mathbb{F}^n$  such that  $C_2 = \{\sigma(\mathbf{c}) + \mathbf{a} : \mathbf{c} \in C_1\}$ .*

**Definition 11.3.2** *Two  $(n, K)$  codes  $C_1$  and  $C_2$  over  $\mathbb{F}_q$  are said to be isomorphic if there is a permutation  $\sigma \in S_n$  such that  $C_2 = \{\sigma(\mathbf{c}) : \mathbf{c} \in C_1\}$ .*

Note that in all the following constructions, the lengths and cardinalities have the right form and to prove that a code is perfect, it suffices to show that it has covering radius one or minimum distance three, which is usually straightforward. This is why we give such a proof only for the first construction (Construction A). Proofs about nonequivalent or nonisomorphic codes are beyond our goals and are not provided here.

Note also that several of these constructions use perfect codes as “starting” codes and yield new perfect codes of greater lengths. This means that the starting and the resulting codes have covering radius one and satisfy the sphere-covering bound with equality. For other applications, it can be useful to use “good” covering codes (not necessarily perfect) as starting codes. In exactly the same way, if the starting code has covering radius one, so does the resulting code.

The first construction of perfect nonlinear codes is due to Vasiliev [664], in the binary case (cf. the  $(\pi(\mathbf{u})|\mathbf{u}|\mathbf{u} + \mathbf{v})$  construction in Section 3.4).

– **Construction A** (1962). Consider a perfect  $(n = 2^m - 1, K = 2^{n-m})$  code  $C$ , linear or not. Let  $\varphi$  be any mapping from  $C$  to  $\mathbb{F}$  such that  $\varphi(0^n) = 0$  and  $\varphi(\mathbf{v}_1 + \mathbf{v}_2) \neq \varphi(\mathbf{v}_1) + \varphi(\mathbf{v}_2)$  for some  $\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_1 + \mathbf{v}_2 \in C$ . For any vector  $\mathbf{u}$ , let  $\pi(\mathbf{u})$  be the parity function of  $\mathbf{u}$ :  $\pi(\mathbf{u}) = 0$  if  $w(\mathbf{u})$  is even,  $\pi(\mathbf{u}) = 1$  otherwise. Let  $D$  be the code

$$D = \{(\mathbf{u}|\mathbf{u} + \mathbf{v}|\pi(\mathbf{u}) + \varphi(\mathbf{v})) : \mathbf{u} \in \mathbb{F}^n, \mathbf{v} \in C\}.$$

**Theorem 11.3.3** For all  $m \geq 3$ , the code  $D$  is a perfect

$$(2n+1 = 2^{m+1} - 1, 2^n \cdot K = 2^{2n-m})$$

code which is not equivalent to any linear code.

**Proof.** (cf. proof of Theorem 3.4.3) Nonlinearity stems from the nonlinearity of  $\varphi$ . We now prove that  $D$  has covering radius one. Take an arbitrary vector  $\mathbf{z} = (\mathbf{z}_0|\mathbf{z}_1|\mathbf{z}_2)$  in  $\mathbb{F}^{2n+1}$ , where  $\mathbf{z}_0$  and  $\mathbf{z}_1$  belong to  $\mathbb{F}^n$  and  $\mathbf{z}_2$  belongs to  $\mathbb{F}$ . Since  $C$  is perfect, there is a vector  $\mathbf{v} \in C$  such that  $d(\mathbf{v}, \mathbf{z}_0 + \mathbf{z}_1) \leq 1$ .

If  $d(\mathbf{v}, \mathbf{z}_0 + \mathbf{z}_1) = 0$  or if  $\pi(\mathbf{z}_0) = \mathbf{z}_2 + \varphi(\mathbf{v})$ , then

$$\mathbf{c} = (\mathbf{z}_0|\mathbf{z}_0 + \mathbf{v}|\pi(\mathbf{z}_0) + \varphi(\mathbf{v})) \in D \text{ and } d(\mathbf{c}, \mathbf{z}) \leq 1.$$

Otherwise, change one coordinate in  $\mathbf{z}_0$  to obtain a vector  $\mathbf{z}'_0$  such that  $\mathbf{z}'_0 + \mathbf{z}_1 = \mathbf{v}$ . Then  $\pi(\mathbf{z}'_0) = \mathbf{z}_2 + \varphi(\mathbf{v})$ ,

$$\mathbf{c}' = (\mathbf{z}'_0|\mathbf{z}'_0 + \mathbf{v}|\pi(\mathbf{z}'_0) + \varphi(\mathbf{v})) \in D \text{ and } d(\mathbf{c}', \mathbf{z}) \leq 1,$$

which ends the proof.  $\square$

Vasiliiev notes that all  $(7, 2^4)1$  codes are necessarily equivalent and linear, and proves the following

**Theorem 11.3.4** The number of nonequivalent codes of length  $n$  obtained through Construction A is at least  $2^{2^n(1-\epsilon_n)}$ , where  $\epsilon_n$  tends to 0 as  $n$  goes to infinity.  $\square$

Later, it was proved that for any  $q \geq 3$  and  $m \geq 3$ , there exist  $q$ -ary nonlinear  $(n = (q^m - 1)/(q - 1), K = q^{n-m})1$  codes, that is, codes which have the same parameters as the  $q$ -ary Hamming codes and are not equivalent to any linear code; see Section 11.4.

But in this section we focus on the binary case. The next construction is a generalization of Construction A.

– **Construction B** (1983). For

$$\mathbf{u} = (u_{1,1}, u_{1,2}, \dots, u_{1,n_2}, u_{2,1}, u_{2,2}, \dots, u_{n_1,n_2}) \in \mathbb{F}^{n_1 n_2},$$

if  $s_i = \sum_{j=1}^{n_2} u_{i,j}$  and  $s'_j = \sum_{i=1}^{n_1} u_{i,j}$ , we define the following two generalized parity functions,  $\pi_1(\mathbf{u}) \in \mathbb{F}^{n_1}$  and  $\pi_2(\mathbf{u}) \in \mathbb{F}^{n_2}$ , by

$$\pi_1(\mathbf{u}) = (s_1, s_2, \dots, s_{n_1}),$$

$$\pi_2(\mathbf{u}) = (s'_1, s'_2, \dots, s'_{n_2}).$$

In other words, if vector  $\mathbf{u}$  is represented by an  $n_1 \times n_2$  array, the calculation of the parity functions can be illustrated by the figure

$$\left[ \begin{array}{cccc|c} u_{1,1} & u_{1,2} & \dots & u_{1,n_2} & \rightarrow & s_1 \\ u_{2,1} & u_{2,2} & \dots & u_{2,n_2} & \rightarrow & s_2 \\ \dots & \dots & \dots & \dots & & \dots \\ u_{n_1,1} & u_{n_1,2} & \dots & u_{n_1,n_2} & \rightarrow & s_{n_1} \\ \hline \downarrow & \downarrow & & \downarrow & & \uparrow \pi_1(\mathbf{u}) \\ s'_1 & s'_2 & \dots & s'_{n_2} & \leftarrow \pi_2(\mathbf{u}) & \end{array} \right].$$

Let  $C_1$  and  $C_2$  be perfect ( $n_1 = 2^{m_1} - 1, K_1 = 2^{n_1-m_1}$ ) and ( $n_2 = 2^{m_2} - 1, K_2 = 2^{n_2-m_2}$ ) codes and  $\varphi$  any mapping from  $C_1$  to  $\mathbb{F}^{n_2}$ . Define

$$D = \{(\mathbf{u}|\mathbf{v}_1 + \pi_1(\mathbf{u})|\mathbf{v}_2 + \pi_2(\mathbf{u}) + \varphi(\mathbf{v}_1)) : \mathbf{u} \in \mathbb{F}^{n_1 n_2}, \mathbf{v}_1 \in C_1, \mathbf{v}_2 \in C_2\}.$$

**Theorem 11.3.5** *The code  $D$  is a perfect*

$$(n_1 n_2 + n_1 + n_2 = 2^{m_1+m_2} - 1, 2^{n_1 n_2} \cdot K_1 K_2 = 2^{n_1 n_2 + n_1 + n_2 - (m_1 + m_2)})$$

code. □

The case  $n_2 = 1$  shows that Construction B generalizes Construction A:  $\pi_1(\mathbf{u}) = \mathbf{u}$ ,  $\pi_2(\mathbf{u}) = \pi(\mathbf{u})$  and  $C_2 = \{0\}$ . This construction can be further generalized, using a family of  $p$  perfect codes of lengths  $n_1, \dots, n_p$  and a family of  $p$  functions  $\pi_i$ , playing the part of parity functions, from  $\mathbb{F}^m$  to  $\mathbb{F}^{n_i}$ , where  $m = \prod_{i=1}^p (n_i + 1) - \sum_{i=1}^p n_i - 1$ . The length of the perfect codes thus obtained is  $\prod_{i=1}^p (n_i + 1) - 1$ .

A more recent construction also contains Construction A.

– **Construction C** (1994). Let  $n_1 = 2^{m_1} - 1$  and  $n_2 = 2^{m_2} - 1$ . Let  $C_1$  and  $C_2$  be two perfect codes of lengths  $n_1$  and  $n_2$ , respectively. Let  $\varphi$  be a mapping from  $C_2$  to  $\mathbb{F}^{n_1}$ . Define

$$D = \{(\mathbf{v}_1 + \varphi(\mathbf{v}_2) + \mathbf{u}_1 + \dots + \mathbf{u}_{n_2}|\mathbf{u}_1| \dots |\mathbf{u}_{n_2}|(\pi(\mathbf{u}_1), \dots, \pi(\mathbf{u}_{n_2})) + \mathbf{v}_2) : \mathbf{v}_1 \in C_1, \mathbf{v}_2 \in C_2, \mathbf{u}_i \in \mathbb{F}^{n_1}, i = 1, 2, \dots, n_2\}.$$

**Theorem 11.3.6** *The code  $D$  is a perfect*

$$(n_1 n_2 + n_1 + n_2 = 2^{m_1+m_2} - 1, 2^{n_1 n_2 + n_1 + n_2 - (m_1 + m_2)})$$

code. □

If  $n_1 = 1$ ,  $C_1 = \{0\}$ , vectors  $\mathbf{u}_i$  have length one and we can set  $\mathbf{u} = (u_1, u_2, \dots, u_{n_2})$ . Now  $D = \{(\varphi(\mathbf{v}_2) + \pi(\mathbf{u})|\mathbf{u}|\mathbf{u} + \mathbf{v}_2) : \mathbf{v}_2 \in C_2, \mathbf{u} \in \mathbb{F}^{n_2}\}$ . This shows that Construction A is included in Construction C. Moreover, it can be shown that Construction C also produces codes which are nonequivalent to those of Construction A.

**Theorem 11.3.7** *The number of nonequivalent codes of length  $n$  obtained through Construction C is at least  $2^{2^{n \cdot (5 - \delta_n)}}$ , where  $\delta_n$ , as  $n$  goes to infinity, tends to 0 faster than  $\epsilon_n$  of Theorem 11.3.4.*  $\square$

A closer look shows that Construction C is identical to Construction B; indeed, if we set

$$\mathbf{u} = (\mathbf{u}_1 | \dots | \mathbf{u}_{n_2}) = (u_{1,1}, u_{2,1}, \dots, u_{n_1,1}, u_{1,2}, \dots, u_{n_1,n_2}),$$

then, using the notation of Construction B:  $\sum_{i=1}^{n_2} \mathbf{u}_i = \pi_1(\mathbf{u})$  and  $(\pi(\mathbf{u}_1), \dots, \pi(\mathbf{u}_{n_2})) = \pi_2(\mathbf{u})$ . Hence

$$D = \{(\mathbf{v}_1 + \varphi(\mathbf{v}_2) + \pi_1(\mathbf{u})|\mathbf{u}|\pi_2(\mathbf{u}) + \mathbf{v}_2) : \mathbf{u} \in \mathbb{F}^{n_1 n_2}, \mathbf{v}_1 \in C_1, \mathbf{v}_2 \in C_2\}$$

and we get exactly Construction B.

After this generalization of Vasiliev's construction, we go back in time to describe three constructions that can be seen as special cases of Zinoviev's generalized concatenated codes (cf. Section 3.6), although the first one was not originally presented in terms of concatenated codes.

– **Construction D** (1970), **Construction E** (1988) and **Construction F** (1996). Let  $A$  (respectively,  $B$ ) be a  $q(A)$ -ary  $(n(A), |A|, d(A))$  code (respectively, a  $q(B)$ -ary  $(n(B), |B|, d(B))$  code), with  $|B| = q(A)$ . We label the codewords of  $B$  from 0 to  $q(A) - 1$ :  $B = \{\mathbf{b}(0), \dots, \mathbf{b}(q(A) - 1)\}$ . For any codeword  $\mathbf{a} = (a_1, \dots, a_{n(A)}) \in A$ , we construct the vector  $\mathbf{a}(B) = (\mathbf{b}(a_1) | \dots | \mathbf{b}(a_{n(A)}))$ . Now  $C = \{\mathbf{a}(B) : \mathbf{a} \in A\}$  is a  $q(B)$ -ary code with length  $n(C) = n(A)n(B)$ , size  $|C| = |A|$  and minimum distance  $d(C) \geq d(A)d(B)$ . The codes  $A$ ,  $B$  and  $C$  are called, respectively, the *outer*, *inner* and *concatenated codes*.

Assume now that the inner code  $B$  is partitioned into  $q_1$  subcodes:

$$B = \bigcup_{i=0}^{q_1-1} B_i,$$

where, for  $i = 0, 1, \dots, q_1 - 1$ ,  $B_i$  is a  $q(B)$ -ary  $(n(B), K_1, d_1)$  code.

Assume furthermore that each subcode  $B_i$  can be partitioned into  $q_2$  subcodes: for  $i = 0, 1, \dots, q_1 - 1$ ,

$$B_i = \bigcup_{j=0}^{q_2-1} B_{i,j},$$

where, for  $j = 0, 1, \dots, q_2 - 1$ ,  $B_{i,j}$  is a  $q(B)$ -ary  $(n(B), K_2, d_2)$  code. Now any codeword  $\mathbf{b} \in B$  belongs to exactly one  $B_{i,j}$  and, if  $\mathbf{b}$  has index  $k$  in  $B_{i,j}$ , we see that

$$(i, j, k) \in \{0, \dots, q_1 - 1\} \times \{0, \dots, q_2 - 1\} \times \{0, \dots, K_2 - 1\}$$

completely identifies the vector  $\mathbf{b}$ . We note  $\mathbf{b} = \mathbf{b}(i, j, k)$ .

Let  $q_3 = K_2$ . Consider, for  $\ell = 1, 2, 3$ , a  $q_\ell$ -ary  $(n(A), |A_\ell|, d(A_\ell))$  code  $A_\ell$  and a codeword  $\mathbf{a}_{i_\ell} = (a_{i_\ell,1}, \dots, a_{i_\ell,n(A)}) \in A_\ell$ . For any  $s$  between 1 and  $n(A)$ , the triple  $(a_{i_1,s}, a_{i_2,s}, a_{i_3,s})$  designates a codeword  $\mathbf{b} = \mathbf{b}(a_{i_1,s}, a_{i_2,s}, a_{i_3,s})$  belonging to  $B$ .

Let  $C = \{(\mathbf{b}(a_{i_1,1}, a_{i_2,1}, a_{i_3,1}) | \dots | \mathbf{b}(a_{i_1,n(A)}, a_{i_2,n(A)}, a_{i_3,n(A)})) : \mathbf{a}_{i_\ell} \in A_\ell, 1 \leq \ell \leq 3\}$ .

**Theorem 11.3.8** *The code  $C$  is a  $q(B)$ -ary code of length  $n(C) = n(A)n(B)$ , size  $|A_1||A_2||A_3|$  and minimum distance  $d(C) \geq \min\{d(A_1)d(B), d(A_2)d_1, d(A_3)d_2\}$ .  $\square$*

The proof is straightforward. This construction can be extended to more levels of partitioning and more codes  $A_\ell$ , leading to *Zinoviev's generalized concatenated codes*. For our purpose, partitioning  $B$  into subcodes  $B_i$  and  $B_{i,j}$  as above is sufficient.

For Construction D, it is even sufficient to consider a partition of  $B$  into subcodes  $B_i$ , together with two codes  $A_1$  and  $A_2$  only: in this case, we set  $q_2 = K_1$  and

$$C = \{(\mathbf{b}(a_{i_1,1}, a_{i_2,1}) | \dots | \mathbf{b}(a_{i_1,n(A)}, a_{i_2,n(A)})) : \mathbf{a}_{i_\ell} \in A_\ell, 1 \leq \ell \leq 2\}.$$

**Corollary 11.3.9** *The code  $C$  is a  $q(B)$ -ary code of length  $n(C) = n(A)n(B)$ , size  $|A_1||A_2|$  and minimum distance  $d(C) \geq \min\{d(A_1)d(B), d(A_2)d_1\}$ .  $\square$*

Now choose  $B$  to be a binary  $(3, 8, 1)$  code,  $\mathbb{F}^3$ . Partition  $B$  into the four cosets  $B_i$  of the set  $\{000, 111\}$ ; each  $B_i$  is a  $(3, 2, 3)$  code and  $q_1 = 4$ ,  $q_2 = 2$ . For  $A_1$ , take a perfect quaternary Hamming  $(n(A) = (4^m - 1)/3, 4^{n(A)-m}, 3)$  code and let  $A_2 = \mathbb{F}^{n(A)}$ .

**Corollary 11.3.10** *The code  $C$  is a — generally nonlinear — perfect binary code of length  $2^{2m} - 1$  and size  $2^{2^{2m}-1-2m}$ .  $\square$*

For Construction E, take  $B = \mathbb{F}^4$ . Consider the partition of  $B$  into the set of even weight vectors and the set of odd weight vectors: the two subcodes  $B_i$  are  $(4, 8, 2)$  codes and  $q_1 = 2$ . For  $i = 0, 1$ , partition  $B_i$  into four subcodes  $B_{i,j}$  with size 2 and minimum distance 4:  $q_2 = 4$  and  $q_3 = 2$ . Finally  $d(B) = 1$ ,  $d_1 = 2$  and  $d_2 = 4$ .

Consider now a perfect binary code of length  $2^m - 1$ . If we extend this code with either an even or odd parity component, we get an *extended perfect*  $(2^m, 2^{2^m-m-1}, 4)$  code (we have already seen the example of the extended perfect Golay codes in Section 11.1). Let  $A_1$  be such an extended perfect code:  $n(A) = 2^m$ ,  $|A_1| = 2^{n(A)-m-1}$ ,  $d(A_1) = 4$ . Let  $A_2$  be a quaternary  $(n(A), 4^{n(A)-1}, 2)$  code ( $A_2$  can consist for instance of all the quaternary vectors of length  $n(A)$  whose parity check is 0). Let  $A_3 = \mathbb{F}^{n(A)}$ .

**Corollary 11.3.11** *The code  $C$  is a binary code of length  $2^{m+2}$ , cardinality  $2^{2^{m+2}-(m+2)-1}$  and minimum distance four. Puncturing  $C$  in one component yields a perfect*

$$(2^{m+2} - 1, 2^{2^{m+2}-(m+2)-1})$$

*code, generally nonlinear.  $\square$*

Construction F generalizes Construction E; consider  $B = \mathbb{F}^{n(B)}$ , where  $n(B) = 2^u$ . As above, partition  $B$  into the set of even vectors, denoted by  $\mathbb{E}^{n(B)}$ , and the set of odd vectors:  $B_0 = \mathbb{E}^{n(B)}$  and  $B_1 = \mathbb{F}^{n(B)} \setminus \mathbb{E}^{n(B)}$  are  $(n(B), 2^{n(B)-1}, 2)$  codes and  $q_1 = 2$ . For  $i = 0, 1$ , partition  $B_i$  into  $2^u$  subcodes  $B_{i,j}$  with size  $2^{n(B)-u-1}$  and minimum distance four (such partitions can be induced, for instance, by a partition of  $\mathbb{F}^{n(B)-1}$  into  $n(B)$  cosets of a perfect linear code). This yields  $q_2 = 2^u$ ,  $q_3 = 2^{n(B)-u-1}$ ,  $d(B) = 1$ ,  $d_1 = 2$  and  $d_2 = 4$ .

Again,  $n(A) = 2^m$  and  $A_1$  is an extended binary perfect  $(2^m, 2^{2^m-m-1}, 4)$  code. Let  $A_2$  be an  $n(B)$ -ary  $(n(A), n(B)^{n(A)-1}, 2)$  code:  $A_2$  can consist for instance of all the  $n(B)$ -ary vectors of length  $n(A)$  whose parity check is 0. Let  $A_3 = \mathbb{F}_{q_3}^{n(A)}$ .

**Corollary 11.3.12** *The code  $C$  is a binary code of length  $2^{m+u}$ , cardinality  $2^{2^{m+u}-(m+u)-1}$  and minimum distance four. Puncturing  $C$  in one component yields a perfect*

$$(2^{m+u} - 1, 2^{2^{m+u}-(m+u)-1})$$

*code, generally nonlinear.  $\square$*

The case  $u = 2$  gives Construction E. As it stands, this corollary is only a particular case of a construction that will be described later (Construction I). However we can also generalize Corollary 11.3.12 in another direction, namely by permuting the  $n_B$  alphabet symbols of the second outer code  $A_2$ .

We present Construction G in a version which is restricted to the binary case, but this construction also produces perfect mixed codes (see Construction G' in Section 11.5 on perfect mixed codes).

– **Construction G** (1977). Let  $n = 2^m - 1$ . Let  $C_1$  be a perfect mixed single-error-correcting code included in  $\mathbb{F}_{n+1}\mathbb{F}^{n+1}$  (cf. Notes on Section 11.5) and  $C_2$  a perfect binary code of length  $n$ ; necessarily  $|C_1| = 2^n$ . Let  $\varphi$  be an injective mapping from  $\mathbb{F}_{n+1}$  to  $\mathbb{F}^n$ , such that  $\varphi(0) = 0^n$  and  $\varphi(u)$  has weight 1 for all  $u \in \mathbb{F}_{n+1} \setminus \{0\}$ . Let  $D$  be the code

$$D = \{(\mathbf{c} + \varphi(u)|\mathbf{v}) : \mathbf{c} \in C_2, (u|\mathbf{v}) \in C_1\}. \quad (11.3.13)$$

**Theorem 11.3.14** *The code  $D$  is a perfect*

$$(2n + 1 = 2^{m+1} - 1, 2^{2n-m})$$

*code. Moreover, nonlinear codes can be obtained, as well as codes which are not equivalent to those of Construction A.*  $\square$

For Construction H, which generalizes Construction G, we use extended perfect  $(2^m, 2^{n-m}, 4)$  codes obtained from a perfect code of length  $n = 2^m - 1$  (cf. Construction E).

– **Construction H** (1981). Consider partitions of  $\mathbb{E}^{n+1}$  and  $\mathbb{F}^{n+1} \setminus \mathbb{E}^{n+1}$  into  $n + 1$  extended perfect codes (cf. Construction F):

$$\mathbb{E}^{n+1} = C_0^0 \cup C_1^0 \cup \dots \cup C_n^0, \quad (11.3.15)$$

$$\mathbb{F}^{n+1} \setminus \mathbb{E}^{n+1} = C_0^1 \cup C_1^1 \cup \dots \cup C_n^1. \quad (11.3.16)$$

Let  $\sigma$  be any permutation on  $\{0, 1, \dots, n\}$ . The code

$$D = \{(\mathbf{c}_1|\mathbf{c}_2) : \mathbf{c}_1 \in C_{\sigma(i)}^0, \mathbf{c}_2 \in C_{\sigma(i)}^1, i = 0, 1, \dots, n\}$$

is an extended perfect code with length  $2(n + 1) = 2^{m+1}$  and cardinality

$$(n + 1)2^{n-m}2^{n-m} = 2^{2n-m}.$$

**Corollary 11.3.17** *Puncturing any coordinate of the code  $D$  gives a perfect*

$$(2n + 1 = 2^{m+1} - 1, 2^{2n-m})$$

*code, generally nonlinear.*  $\square$

One can see that  $D$  is the blockwise direct sum of the two families of codes  $\{C_0^0, C_1^0, \dots, C_n^0\}$  and  $\{C_{\sigma(0)}^1, C_{\sigma(1)}^1, \dots, C_{\sigma(n)}^1\}$  (see Section 4.5).

We now show that Construction H is a generalization of Construction G. Consider the code  $C_1$  in Construction G. Necessarily  $|C_1| = 2^n$ . If we puncture  $C_1$  on the first coordinate, we get a binary code  $C_1^*$  with length  $n + 1$ , cardinality  $2^n$  and minimum distance at least two. So  $C_1^*$  is equal to either  $\mathbb{E}^{n+1}$  or  $\mathbb{F}^{n+1} \setminus \mathbb{E}^{n+1}$ . Without loss of generality, we can assume that  $C_1^* = \mathbb{E}^{n+1}$ . For every  $u \in \mathbb{F}^{n+1}$ , if two vectors  $(u|\mathbf{v}_1)$  and  $(u|\mathbf{v}_2)$  belong to  $C_1$ , then  $d(\mathbf{v}_1, \mathbf{v}_2) \geq 4$ . Therefore the symbols  $u$  partition  $C_1^*$  into at most  $n+1$  subcodes of length  $n + 1$  and minimum distance at least 4. Extended perfect codes are the largest codes with these parameters, and they have  $2^n/(n + 1)$  elements. This shows that  $C_1$  is of the form  $\{(u|\mathbf{v}) : u \in \mathbb{F}^{n+1}, \mathbf{v} \in C_u^0\}$ , where the sets  $C_u^0$  are extended perfect codes partitioning  $\mathbb{E}^{n+1}$ . The code  $D$  in (11.3.13) now reads

$$\begin{aligned} D &= \{(\mathbf{c} + \varphi(u)|\mathbf{v}) : \mathbf{c} \in C_2, \mathbf{v} \in C_u^0, u \in \mathbb{F}^{n+1}\} \\ &= \{(\mathbf{c}|\mathbf{v}) : \mathbf{c} \in C_2 + \varphi(u), \mathbf{v} \in C_u^0, u \in \mathbb{F}^{n+1}\}. \end{aligned} \quad (11.3.18)$$

The  $n + 1$  sets  $C_2 + \varphi(u)$  partition  $\mathbb{F}^n$  and can be extended to  $n + 1$  sets  $C_u^1$  partitioning  $\mathbb{F}^{n+1} \setminus \mathbb{E}^{n+1}$ : from  $D$  we get an extended perfect code

$$\{(\mathbf{c}|\mathbf{v}) : \mathbf{c} \in C_u^1, \mathbf{v} \in C_u^0, u \in \mathbb{F}^{n+1}\},$$

proving that we are in a particular case of Construction H.

The next construction is a generalization of Construction H.

– **Construction I** (1984). We still consider the partitions of  $\mathbb{E}^{n+1}$  and  $\mathbb{F}^{n+1} \setminus \mathbb{E}^{n+1}$  into  $n + 1$  extended perfect codes, given by (11.3.15) and (11.3.16), respectively. Now let  $C$  be an extended perfect code of length  $2^{m_0} = n_0 + 1$ . For each vector  $\mathbf{v} \in C$ , let  $C(\mathbf{v})$  be an  $(n + 1)$ -ary  $(n_0 + 1, (n + 1)^{n_0}, 2)$  code (cf.  $A_2$  in Constructions E and F). Then

$$\begin{aligned} D &= \{(\mathbf{c}_0|\mathbf{c}_1|\dots|\mathbf{c}_{n_0}) : \mathbf{c}_i \in C_{j_i}^{v_i}, \mathbf{v} = (v_0, v_1, \dots, v_{n_0}) \in C, \\ &\quad (j_0, j_1, \dots, j_{n_0}) \in C(\mathbf{v})\} \end{aligned}$$

is an extended perfect code with length  $(n_0 + 1)(n + 1) = 2^{m+m_0}$  and cardinality

$$(2^{n-m})^{n_0+1} 2^{n_0-m_0} (n + 1)^{n_0} = 2^{(n_0+1)(n+1)-1-(m+m_0)}.$$

**Corollary 11.3.19** *Puncturing any coordinate of the code  $D$  gives a perfect*

$$((n_0 + 1)(n + 1) - 1 = 2^{m+m_0} - 1, 2^{(n_0+1)(n+1)-1-(m+m_0)})$$

*code.*  $\square$

For  $n_0 = 1$ , we consider that  $C$  is a  $(2, 1)$  code;  $C(\mathbf{v})$  is an  $(n + 1)$ -ary  $(2, n + 1, 2)$  code which corresponds to a permutation  $\sigma$  on  $n + 1$  elements — for instance, if we take

$$C(\mathbf{v}) = \{(0, 1), (1, 2), \dots, (n - 1, n), (n, 0)\},$$

then  $\sigma = (1, 2, \dots, n, 0)$ . If we choose  $C = \{(0, 1)\}$ , we see that Corollary 11.3.17 is a particular case of Corollary 11.3.19. If we let  $C(\mathbf{v})$  be the same code for all vectors  $\mathbf{v} \in C$ , then we obtain Corollary 11.3.12.

**Theorem 11.3.20** *The number of nonequivalent codes of length  $n$  given by Construction I is at least  $2^{2^{cn}}$  for some constant  $c < 1$ .*  $\square$

Another way of generalizing Construction H was more recently given by Construction J, due to Etzion and Vardy [224] (see also [662]):

— **Construction J** (1994). Let  $n = 2^m - 1$  and let  $V$  be a subset of  $\mathbb{F}^n$ ; let  $\mathcal{A} = \{A_1, A_2, \dots, A_j\}$ ,  $\mathcal{B} = \{B_1, B_2, \dots, B_j\}$  be two ordered sets of subsets of  $V$ . For all  $\mathbf{z} \in V$ , consider the sets

$$\Lambda_{\mathcal{A}}(\mathbf{z}) = \{i \in \{1, 2, \dots, j\} : \mathbf{z} \in A_i\},$$

$$\Lambda_{\mathcal{B}}(\mathbf{z}) = \{i \in \{1, 2, \dots, j\} : \mathbf{z} \in B_i\}.$$

Sets  $\mathcal{A}$  and  $\mathcal{B}$  are said to form a *perfect segmentation of order  $j$  of  $V$*  if, for all  $\mathbf{z} \in V$ , both  $\bigcup_{i \in \Lambda_{\mathcal{B}}(\mathbf{z})} A_i$  and  $\bigcup_{i \in \Lambda_{\mathcal{A}}(\mathbf{z})} B_i$  are perfect codes (of length  $n$ ). Define

$$D = \{(\mathbf{u}|\pi(\mathbf{u})|\mathbf{v}) : \mathbf{u} \in A_i, \mathbf{v} \in B_i, i = 1, 2, \dots, j\}.$$

**Theorem 11.3.21** *If  $\mathcal{A}$  and  $\mathcal{B}$  form a perfect segmentation of order  $j$  of  $V$ , then  $D$  is a perfect code of length  $2n + 1$ .*  $\square$

Two partitions into  $n+1$  perfect codes form a perfect segmentation of order  $n+1$  of  $V = \mathbb{F}^n$  and show that Theorem 11.3.21 generalizes Construction H; perfect segmentations of higher order exist.

The authors also construct a family  $\mathcal{C}$  of perfect codes of full rank (the *rank of a code* of a code is the maximum number of linearly independent

codewords; the code is of *full rank* when its rank is equal to its length) and they show that none of the perfect codes given by Constructions A, B, H, I or J is of full rank. We give here a brief description of the family  $\mathcal{C}$ .

— **Construction K.** Let  $m \geq 4$  and  $n = 2^m - 1$ . Let  $\mathbf{h}_1, \mathbf{h}_2, \dots, \mathbf{h}_n$  be the columns of a parity check matrix of a Hamming code  $\mathcal{H}_m$ . For any nonzero vector  $\mathbf{z} \in \mathbb{F}^m$ ,  $\varphi(\mathbf{z})$  is (uniquely) defined by  $\mathbf{h}_{\varphi(\mathbf{z})} = \mathbf{z}$ . Furthermore,  $\mathbf{z}$  induces a unique partition of  $\{1, 2, \dots, n\} \setminus \{\varphi(\mathbf{z})\}$  into  $2^{m-1} - 1$  pairs  $(i, j)$  such that  $i < j$  and  $\mathbf{h}_i + \mathbf{h}_j = \mathbf{z}$ . If, for each such pair  $(i, j)$ , we write  $j = \phi(\mathbf{z}, i)$  and  $i = \phi(\mathbf{z}, j)$ , then we see that  $\mathbf{z}$  defines a unique set  $I \subset \{1, 2, \dots, n\} \setminus \{\varphi(\mathbf{z})\}$  such that  $|I| = 2^{m-1} - 1$  and for all  $i \in I$ ,  $i < \phi(\mathbf{z}, i)$  and  $\mathbf{h}_i + \mathbf{h}_{\phi(\mathbf{z}, i)} = \mathbf{z}$ .

For any nonzero vector  $\mathbf{z} \in \mathbb{F}^m$ , define

$$C_1(\mathbf{z}) = \{\mathbf{x} = (x_1, \dots, x_n) \in \mathbb{F}^n : \forall i \in I, x_i = x_{\phi(\mathbf{z}, i)}; x_{\varphi(\mathbf{z})} = \sum_{i \in I} x_i\};$$

$$C_2(\mathbf{z}) = \{\mathbf{x} = (x_1, \dots, x_n) \in \mathbb{F}^n : \forall i \in I, x_i = x_{\phi(\mathbf{z}, i)}; x_{\varphi(\mathbf{z})} = 1 + \sum_{i \in I} x_i\}.$$

For all  $\mathbf{z}$ , the code  $C_1(\mathbf{z})$  is included in  $\mathcal{H}_m$  and is isomorphic to  $\{(\mathbf{x}|\mathbf{x}|\pi(\mathbf{x})) : \mathbf{x} \in \mathbb{F}^{(n-1)/2}\}$ , the code  $C_2(\mathbf{z})$  is isomorphic to  $\{(\mathbf{x}|\mathbf{x}|\pi(\mathbf{x}) + 1) : \mathbf{x} \in \mathbb{F}^{(n-1)/2}\}$ , and  $C_1(\mathbf{z})$  and  $C_2(\mathbf{z})$  perfectly 1-cover the same subset of  $\mathbb{F}^n$ . The idea of Construction K is to remove from  $\mathcal{H}_m$  some  $m$  disjoint subsets which are isomorphic to  $C_1(\mathbf{z})$  and to replace them by cosets of these subsets. For this, we need the following property, whose proof we skip.

Let  $k \leq m$  be any integer and  $\mathbf{z}_1, \dots, \mathbf{z}_k$  be  $k$  linearly independent vectors in  $\mathbb{F}^m$ . Then, for any  $\mathbf{z}_1 \neq \mathbf{z}_2$ ,  $C_2(\mathbf{z}_1) \cap C_2(\mathbf{z}_2) = \emptyset$ , whereas  $|C_1(\mathbf{z}_1) \cap C_1(\mathbf{z}_2)| = 2^{2^{m-2}}$ . But there exist  $k$  codewords  $\mathbf{c}_1, \dots, \mathbf{c}_k \in \mathcal{H}_m$  such that the sets  $C_1(\mathbf{z}_1) + \mathbf{c}_1, \dots, C_1(\mathbf{z}_k) + \mathbf{c}_k$  are disjoint.

Now let

$$D = \left( \mathcal{H}_m \setminus \bigcup_{1 \leq j \leq k} (C_1(\mathbf{z}_j) + \mathbf{c}_j) \right) \cup \bigcup_{1 \leq j \leq k} (C_2(\mathbf{z}_j) + \mathbf{c}_j).$$

**Theorem 11.3.22** *The code  $D$  is perfect and has rank  $n - m + k$ .*  $\square$

Finally, the authors give a lower bound on the number of nonequivalent perfect codes.

**Theorem 11.3.23** *The number of nonequivalent perfect codes of length  $n$  is at least  $2^{f(n)}$ , with*

$$f(n) = 2^{.5(n+1)-\log(n+1)} - (n+1) - \log^2(n+1).$$

$\square$

We now present a last binary construction, which, as we shall see, is included in Construction G.

— **Construction L (1983).** Consider a perfect ( $n = 2^m - 1, K = 2^{n-m}$ ) code  $C$ , linear or not, and a mapping  $\varphi_1$  from  $\mathbb{E}^{n+1}$  to  $\{0, 1, \dots, n\}$ , with the following property: any two vectors  $\mathbf{x}_1, \mathbf{x}_2 \in \mathbb{E}^{n+1}$  such that  $d(\mathbf{x}_1, \mathbf{x}_2) = 2$  satisfy  $\varphi_1(\mathbf{x}_1) \neq \varphi_1(\mathbf{x}_2)$ . For  $i = 1, 2, \dots, n$ , let  $\mathbf{e}_i$  be the binary vector of length  $n$  with only one nonzero coordinate in position  $i$ , and  $\mathbf{e}_0 = 0^n$ . Let  $\varphi_2$  be the mapping from  $\mathbb{E}^{n+1}$  to  $\mathbb{F}^n$  which, to each vector  $\mathbf{x}$ , associates  $\mathbf{e}_{\varphi_1(\mathbf{x})}$ . Finally, define

$$D = \{(\mathbf{x}|\mathbf{v} + \varphi_2(\mathbf{x})) : \mathbf{x} \in \mathbb{E}^{n+1}, \mathbf{v} \in C\}. \quad (11.3.24)$$

**Theorem 11.3.25** *The code  $D$  is a perfect ( $2n + 1 = 2^{m+1} - 1, 2^n \cdot K = 2^{2n-m}$ ) code. Moreover, Construction L can be used to produce codes which are nonlinear and nonisomorphic to the codes given by Construction A, for all  $m \geq 3$ .*  $\square$

Actually, we can observe that Construction L is contained in Construction G (1977). *Rien de nouveau sous le soleil.* Consider any mapping  $\varphi_1$  fulfilling the required conditions of Construction L.

**Lemma 11.3.26** *The sets  $\varphi_1^{-1}(0), \varphi_1^{-1}(1), \dots, \varphi_1^{-1}(n)$  partition  $\mathbb{E}^{n+1}$  into  $n + 1$  extended perfect codes.*

**Proof.** For all  $i = 0, 1, \dots, n$ , the code  $\varphi_1^{-1}(i)$  has minimum distance at least 4. Puncturing any coordinate gives a code with minimum distance at least 3 and by the sphere-packing bound:  $|\varphi_1^{-1}(i)| \leq 2^n/(n+1)$ , which in turn implies that  $|\varphi_1^{-1}(i)| = 2^n/(n+1)$ : each set  $\varphi_1^{-1}(i)$  is an extended perfect code.  $\square$

Without loss of generality, the code  $D$  in Construction G satisfies (11.3.18). Consider the particular case where for  $u = 0, 1, \dots, n$  the sets  $C_u^0$  are the sets  $\varphi_1^{-1}(u)$  and  $\varphi(u) = \mathbf{e}_u$ ; now

$$D = \{(\mathbf{c} + \mathbf{e}_u|\mathbf{v}) : \mathbf{c} \in C_2, \mathbf{v} \in \varphi_1^{-1}(u), u \in \mathbb{F}_{n+1}\}.$$

If  $\varphi_2$  is defined as in Construction L, then for any  $\mathbf{v} \in \varphi_1^{-1}(u)$ ,  $\varphi_2(\mathbf{v}) = \mathbf{e}_u$ . So the code  $D$  is equal to

$$\{(\mathbf{c} + \varphi_2(\mathbf{v})|\mathbf{v}) : \mathbf{c} \in C_2, \mathbf{v} \in \varphi_1^{-1}(i), i = 0, 1, \dots, n\},$$

i.e.,  $\{(c + \varphi_2(v))|v : c \in C_2, v \in \mathbb{F}^{n+1}\}$ , which is exactly (11.3.24) in Construction L.

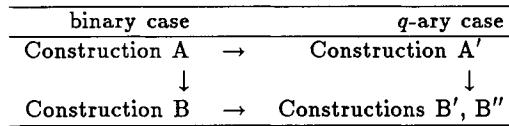
For some of the above constructions, a lower bound on the number of nonequivalent codes could be given. An upper bound on the number of nonequivalent single-error-correcting perfect binary codes of length  $n$  is

$$2^{2^{n-(3/2)\log n+\log\log n}}. \quad (11.3.27)$$

## 11.4 Enumeration of perfect codes over $\mathbb{F}_q$

For  $q \geq 3$  a prime power, the first  $q$ -ary perfect nonlinear codes can be found in Schönheim [573]. They have parameters  $n = (q^m - 1)/(q - 1)$ ,  $K = q^{n-m}$ , covering radius one (and minimum distance three) and exist for all  $m \geq 3$ . Since then, other families of codes with the same parameters have been constructed. We describe some of them below. Since the  $q$ -ary case is not our priority, we give no proofs in this section.

This first construction [573] (1968), which we call Construction A', is a generalization of Construction A to the  $q$ -ary case. We do not describe it here, but rather immediately give Constructions B' and B'', which are generalizations of Construction A' as well as generalizations to the  $q$ -ary case of Construction B, which was itself a generalization of Construction A, so that we have the following scheme (where arrows represent generalizations):



– **Construction B'** (1983). Consider the lexicographical order on the coordinates of any vector  $u \in \mathbb{F}_q^{(q-1)n_1n_2}$ :  $u = (u_{1,1,1}, u_{1,1,2}, \dots, u_{q-1,n_1,n_2})$ . If  $s_i = \sum_{h=1}^{q-1} \sum_{j=1}^{n_2} u_{h,i,j}$  and  $s'_j = \sum_{h=1}^{q-1} h \sum_{i=1}^{n_1} u_{h,i,j}$ , we define  $\pi_1(u) \in \mathbb{F}_q^{n_1}$  and  $\pi_2(u) \in \mathbb{F}_q^{n_2}$  in the following way:

$$\pi_1(u) = (s_1, s_2, \dots, s_{n_1}),$$

$$\pi_2(u) = (s'_1, s'_2, \dots, s'_{n_2}).$$

Let  $C_1$  and  $C_2$  be two perfect ( $n_1 = (q^{m_1} - 1)/(q - 1)$ ,  $K_1 = q^{n_1-m_1}$ ) and ( $n_2 = (q^{m_2} - 1)/(q - 1)$ ,  $K_2 = q^{n_2-m_2}$ ) codes over  $\mathbb{F}_q$  and let  $\varphi$  be any mapping from  $C_1$  to  $\mathbb{F}_q^{n_2}$ ; define

$$D = \{(u|v_1 + \pi_1(u)|v_2 + \pi_2(u) + \varphi(v_1)) : u \in \mathbb{F}_q^{(q-1)n_1n_2}, v_1 \in C_1, v_2 \in C_2\}.$$

**Theorem 11.4.1** *The code  $D$  is a perfect*

$$(n = (q^{m_1+m_2} - 1)/(q - 1), q^{(q-1)n_1n_2} \cdot K_1 K_2 = q^{n-(m_1+m_2)})$$

*code. Nonlinear codes can be obtained for  $m_1 \geq 3$  (and  $m_1 \geq 2$  if  $q \neq 2$ ).  $\square$*

If  $q = 2$ , or  $n_2 = 1$ , or  $q = 2$  and  $n_2 = 1$ , we have Constructions B, or A', or A, respectively.

Construction B'' is a less straightforward generalization of Construction A'.

— **Construction B'' (1984).** Let  $C_1$  and  $C_2$  be, as above, two perfect  $(n_1, K_1)$  and  $(n_2, K_2)$  codes over  $\mathbb{F}_q$ . Let  $C_3$  be a perfect  $q$ -ary code of length  $q + 1$  and cardinality  $q^{q-1}$ . Let  $C_4$  and  $C_5$  be two  $q$ -ary  $(n_1 + 2, q^{n_1+1}, 2)$  and  $(n_2 + 2, q^{n_2+1}, 2)$  codes, respectively (cf.  $A_2$  in Construction F). Because they have minimum distances 3, 2 and 2, respectively, the codes  $C_3$ ,  $C_4$  and  $C_5$  can be expressed as

$$C_3 = \{(\mathbf{x}|f_1(\mathbf{x})|f_2(\mathbf{x})) : \mathbf{x} \in \mathbb{F}_q^{q-1}\},$$

$$C_4 = \{(\mathbf{x}|f_3(\mathbf{x})) : \mathbf{x} \in \mathbb{F}_q^{n_1+1}\},$$

$$C_5 = \{(\mathbf{x}|f_4(\mathbf{x})) : \mathbf{x} \in \mathbb{F}_q^{n_2+1}\},$$

where  $f_i(\mathbf{x}) \in \mathbb{F}_q$  for  $i = 1, 2, 3, 4$  and can be interpreted as a parity function.

For  $\mathbf{c} = (c_1, \dots, c_{n_1}) \in C_1$ ,  $\mathbf{d} = (d_1, \dots, d_{n_2}) \in C_2$ ,  $\mathbf{u}_{i,j} \in \mathbb{F}_q^{q-1}$ , for  $i = 1, 2, \dots, n_1$  and  $j = 1, 2, \dots, n_2$ , let  $a_i = f_4(f_1(\mathbf{u}_{i,1}), \dots, f_1(\mathbf{u}_{i,n_2}), c_i)$  and  $b_j = f_3(f_2(\mathbf{u}_{1,j}), \dots, f_2(\mathbf{u}_{n_1,j}), d_j)$ . Now define

$$D = \{(\mathbf{u}_{1,1}|\dots|\mathbf{u}_{i,j}|\dots|\mathbf{u}_{n_1,n_2}|(a_1, a_2, \dots, a_{n_1}, b_1, \dots, b_{n_2})) :$$

$$\mathbf{u}_{i,j} \in \mathbb{F}_q^{q-1}, \mathbf{c} \in C_1, \mathbf{d} \in C_2\}.$$

**Theorem 11.4.2** *The code  $D$  is a perfect*

$$(n = (q^{m_1+m_2} - 1)/(q - 1), q^{n-(m_1+m_2)})$$

*code.  $\square$*

When  $q = 2$ , if we take  $C_3 = \{0^3, 1^3\}$ , then for  $i = 1, 2$  and for  $x = 0, 1$ ,  $f_i(x) = x$ ; the functions  $f_3$  and  $f_4$  can be either the usual binary parity function  $\pi$  or  $1 + \pi$ . Now for  $u_{i,j} \in \mathbb{F}$ ,  $a_i = \pi(u_{i,1}, \dots, u_{i,n_2}, c_i) = \pi(u_{i,1}, \dots, u_{i,n_2}) + c_i$  and  $b_j = \pi(u_{1,j}, \dots, u_{n_1,j}) + d_j$ . So, using the generalized

parity functions  $\pi_1$  and  $\pi_2$  of Construction B and letting  $\mathbf{u} = (\mathbf{u}_{1,1} | \dots | \mathbf{u}_{i,j} | \dots | \mathbf{u}_{n_1, n_2})$ , we have

$$D = \{(\mathbf{u}|\mathbf{c} + \pi_1(\mathbf{u})|\mathbf{d} + \pi_2(\mathbf{u})) : \mathbf{u} \in \mathbb{F}_q^{n_1 n_2}, \mathbf{c} \in C_1, \mathbf{d} \in C_2\},$$

which is slightly less general than Construction B.

When  $n_2 = 1$ , one gets Construction A'; when  $n_2 = 1$  and  $q = 2$ , one gets Construction A (without the mapping  $\varphi$ ). So using a mapping from  $C_1$  to  $\mathbb{F}_q^{n_2}$  in Construction B'' gives a construction which is truly a generalization of Constructions A, A' and B.

Let us mention here that, for Construction A', it is possible to give a lower bound on the number of nonequivalent codes:

**Theorem 11.4.3** *The number of nonequivalent codes of length  $n$  obtained through Construction A' is at least  $q^{q^{n(1/q - \epsilon_n)}}$ , where  $\epsilon_n$  tends to 0 as  $n$  goes to infinity.*  $\square$

Zinoviev's generalized concatenated codes (cf. Constructions D, E and F) can be used to construct  $q$ -ary perfect codes.

— **Construction D'** (1996). With the same notation as in Construction D, take  $B = \mathbb{F}_q^n$ , where  $q = q(B)$  is a prime power and  $n = n(B) = (q^s - 1)/(q - 1)$ . Partition  $B$  into  $q^s$  cosets  $B_i$  of a  $q$ -ary Hamming code of length  $n$ : each  $B_i$  is an  $(n, q^{n-s}, 3)$  code and  $q_1 = q^s$ ,  $q_2 = q^{n-s}$ .

For  $A_1$ , take a  $q_1$ -ary Hamming  $(n(A) = (q_1^m - 1)/(q_1 - 1), q_1^{n(A)-m}, 3)$  code and let  $A_2 = \mathbb{F}_{q_2}^{n(A)}$ .

With this choice of parameters, we have the following result.

**Theorem 11.4.4** *The code  $C$  is a  $q$ -ary perfect code with length*

$$n(C) = n(A)n(B) = (q^{sm} - 1)/(q - 1)$$

and size

$$|A_1||A_2| = (q^s)^{n(A)-m}(q^{n-s})^{n(A)} = q^{n(C)-sm}.$$

$\square$

Considering the case  $q = 2, n = 3$  shows that Construction D' generalizes Construction D.

The next construction is a generalization of Construction H to the  $q$ -ary case.

– **Construction H'** (1984). For any vector  $\mathbf{v} = (v_1, \dots, v_n) \in \mathbb{F}_q^n$ , let  $\pi(\mathbf{v}) = \sum_{i=1}^n v_i$  and for any  $q-1$  vectors  $\mathbf{v}_1, \dots, \mathbf{v}_{q-1}$  in  $\mathbb{F}_q^n$ , let  $\pi(\mathbf{v}_1, \dots, \mathbf{v}_{q-1}) = \sum_{i=1}^{q-1} i \cdot \pi(\mathbf{v}_i)$ . Let  $n = (q^m - 1)/(q - 1)$ , and let  $C_0^0 \cup C_1^0 \cup \dots \cup C_{n(q-1)}^0$  and  $C_0^1 \cup C_1^1 \cup \dots \cup C_{n(q-1)}^1$  be two partitions of  $\mathbb{F}_q^n$  into  $n(q-1) + 1 = q^m$  perfect  $(n, q^{n-m})$  codes. Define

$$D = \{(\mathbf{v}_1 | \dots | \mathbf{v}_{q-1} | \pi(\mathbf{v}_1, \dots, \mathbf{v}_{q-1}) | \mathbf{v}_q) : \mathbf{v}_i \in \mathbb{F}_q^n, i = 1, \dots, q-1,$$

$$\sum_{i=1}^{q-1} \mathbf{v}_i \in C_j^0 \Rightarrow \mathbf{v}_q \in C_j^1\}.$$

**Theorem 11.4.5** *The code  $D$  is a perfect*

$$(n' = (q^{m+1} - 1)/(q - 1), (q^n)^{q-1} q^{n-m} = q^{n'-(m+1)})$$

code. □

The case  $q = 2$  yields

$$D = \{(\mathbf{v}_1 | \pi(\mathbf{v}_1) | \mathbf{v}_2) : \mathbf{v}_1 \in \mathbb{F}_2^n, \mathbf{v}_1 \in C_j^0 \Rightarrow \mathbf{v}_2 \in C_j^1\},$$

which is, up to permutation  $\sigma$ , Construction H.

## 11.5 Mixed codes

The first perfect mixed codes date back to 1970. Before 1993, all of them had covering radius one. In [222], Etzion and Greenberg present an infinite family of perfect mixed codes with covering radius two.

Since we do not want to focus on mixed codes, we give here only the mixed version of Construction G of Section 11.3 (Construction G') and a brief description of the Etzion-Greenberg codes. Further results and references can be found in the notes at the end of the chapter.

– **Construction G'** (1977). Let  $n, n_1$  and  $n_2$  be three integers satisfying  $n \geq n_2 + 1 \geq 2$  and  $n = n_1 + n_2 - 1$ . Let  $q_1, q_2, \dots, q_{n+1}$  be  $n+1$  integers, which are not necessarily prime powers.

We assume that  $C_1$  is a perfect code of length  $n_1$  and covering radius one in

$$\mathbf{V}_1 = \mathbb{Z}_{q_1} \mathbb{Z}_{q_{n_2+2}} \mathbb{Z}_{q_{n_2+3}} \dots \mathbb{Z}_{q_{n+1}}$$

and that  $C_2$  is a perfect code of length  $n_2$  and covering radius one in

$$\mathbf{V}_2 = \mathbb{Z}_{q_2} \dots \mathbb{Z}_{q_{n_2+1}}.$$

Consider the mixed space

$$\mathbf{V} = \mathbb{Z}_{q_2} \dots \mathbb{Z}_{q_{n_2+1}} \mathbb{Z}_{q_{n_2+2}} \dots \mathbb{Z}_{q_{n+1}}$$

of length  $n$ . Denote by  $\mathcal{V}_1$ ,  $\mathcal{V}_2$  and  $\mathcal{V}$  the cardinality of the sphere of radius one in  $\mathbf{V}_1$ ,  $\mathbf{V}_2$  and  $\mathbf{V}$ , respectively:  $|C_1| = |\mathbf{V}_1|/\mathcal{V}_1$  and  $|C_2| = |\mathbf{V}_2|/\mathcal{V}_2$ .

Assume that  $\mathcal{V}_2 = q_1$  (hence  $q_1 - 1 = \sum_{i=2}^{n_2+1} (q_i - 1)$  and  $\mathcal{V}_1 = 1 + (q_1 - 1) + \sum_{i=n_2+2}^{n+1} (q_i - 1) = \mathcal{V}$ ). Let  $\varphi$  be an injective mapping from  $\mathbb{Z}_{q_1}$  to  $\mathbf{V}_2$  such that  $\varphi(0) = 0^{n_2}$  and  $\varphi(u)$  has weight 1 for all  $u \in \mathbb{Z}_{q_1} \setminus \{0\}$ . Let  $D$  be the following code in  $\mathbf{V}$ :

$$D = \{(\mathbf{c} + \varphi(u)|\mathbf{v}) : \mathbf{c} \in C_2, (u|\mathbf{v}) \in C_1\}.$$

The code  $D$  has length  $n$  and cardinality  $|C_1||C_2| = |\mathbf{V}_1||\mathbf{V}_2|/\mathcal{V}_1\mathcal{V}_2 = |\mathbf{V}|/\mathcal{V}$ .

**Theorem 11.5.1** *The code  $D$  has covering radius one and is therefore perfect.*  $\square$

The particular case  $q_1 = n_2 + 1 = n_1 - 1 = 2^m$ ,  $q_2 = \dots = q_{n+1} = 2$  gives Construction G.

– **Construction M** (1993). Etzion and Greenberg [222] described the first perfect mixed codes with covering radius greater than one. Their construction is simple and efficient: these codes  $C$  have length  $2^m + 1$ , size  $2^{2^m - m - 1}$  and are subsets of  $\mathbb{F}_2^{2^m} \mathbb{F}_{2^{m-1}}^1$ , for all even  $m > 3$ ; they consist of all vectors  $\mathbf{c} = (\mathbf{x}|i)$ , where  $\mathbf{x}$  is a codeword of the extended Hamming code of length  $2^m$  and  $i$  is the number of the coset of the Preparata code of the corresponding length which contains  $\mathbf{x}$  (cf. Theorem 2.6.5).

**Theorem 11.5.2** *The codes  $C$  have covering radius two and therefore are perfect.*  $\square$

In the same article, the authors use, among others, these perfect mixed codes for the construction of good binary covering codes (cf. Example 3.6.2).

To summarize Sections 11.3, 11.4 and 11.5, the following scheme represents the relationships between the different constructions described in these sections. Vertical arrows stand for generalizations, right arrows for generalizations to the  $q$ -ary case and left arrows for a restriction to the binary case.

binary	$q$ -ary	mixed
A	$\rightarrow$	$A'$
$\downarrow$		$\downarrow$
B	$\rightarrow$	$B', B''$
C ( $= B$ )		
D	$\rightarrow$	$D'$
E		
$\downarrow$		
F		
G	$\leftarrow$	$\leftarrow$
$\downarrow$		$G'$
H	$\rightarrow$	$H'$
$\downarrow$		
I, J		$M$
K		
$L ( \subset G )$		

## 11.6 Generalizations of perfect codes

Active study of perfect codes led to an interest in codes which are very close to being perfect. Among these classes we will mention nearly perfect and uniformly packed codes.

Consider a binary  $e$ -error-correcting code  $C$  of length  $n$ , i.e.,  $d(C) = 2e + 1$  or  $2e + 2$ . Let, moreover,  $R(C) \leq e + 1$ . Consider the set  $Z$  of vectors being at distance  $e$  or  $e + 1$  from  $C$ . Clearly,

$$|Z| = 2^n - |C|V(n, e - 1).$$

For every  $\mathbf{z} \in Z$ , let  $\mathcal{A}_i(\mathbf{z})$  stand for the number of codewords being at distance  $i$  from  $\mathbf{z}$ , and let  $m(\mathbf{z}) = \mathcal{A}_e(\mathbf{z}) + \mathcal{A}_{e+1}(\mathbf{z})$ . By a suitable translation of the code, we may assume that  $\mathbf{z} = \mathbf{0}$ . Now,  $m(\mathbf{0})$  is equal to the number of codewords of weight  $e$  or  $e + 1$ . Since the distance between these vectors is at least  $2e + 1$ , we have  $m(\mathbf{0}) \leq \lfloor (n + 1)/(e + 1) \rfloor$ , and so for all  $\mathbf{z} \in Z$ ,

$$m(\mathbf{z}) \leq \left\lfloor \frac{n + 1}{e + 1} \right\rfloor.$$

Since

$$\sum_{\mathbf{z} \in Z} m(\mathbf{z}) = \sum_{\mathbf{c} \in C} |S_e(\mathbf{c}) \cup S_{e+1}(\mathbf{c})| = |C| \left( \binom{n}{e} + \binom{n}{e+1} \right),$$

the average value  $m$  of  $m(\mathbf{z})$  is

$$m = \frac{|C| \left( \binom{n}{e} + \binom{n}{e+1} \right)}{2^n - |C|V(n, e - 1)}. \quad (11.6.1)$$

If we have  $m(\mathbf{z}) = m$  for all  $\mathbf{z} \in Z$ , the code is called *strongly uniformly packed*. If  $C$  is strongly uniformly packed and  $m(\mathbf{z})$  achieves its maximum value,  $\lfloor (n+1)/(e+1) \rfloor$ , then  $C$  is called *nearly perfect*. From (11.6.1) we have for nearly perfect codes

$$|C| \left( V(n, e-1) + \frac{1}{\lfloor (n+1)/(e+1) \rfloor} \left( \binom{n}{e} + \binom{n}{e+1} \right) \right) = 2^n. \quad (11.6.2)$$

If  $e+1$  divides  $n+1$ , (11.6.2) becomes

$$|C|V(n, e) = 2^n,$$

and in this case nearly perfect codes are just perfect codes.

Actually, the strongly uniformly packed codes must have minimum distance  $2e+1$ . Indeed, assume  $d(C) = 2e+2$ . Without loss of generality,  $\mathbf{0} \in C$ . Let  $\mathbf{c}$  be a codeword of weight  $2e+2$ . Then, for every vector  $\mathbf{z}$  of weight  $e+1$  with  $\text{supp}(\mathbf{z}) \subset \text{supp}(\mathbf{c})$ , we have  $m(\mathbf{z}) \geq 2$  and  $\mathbf{z} \in Z$ . However, any vector  $\mathbf{z}'$  of weight  $e$  belongs to  $Z$ , but is at distance at most  $e+1$  only from the zero codeword. Hence,  $m(\mathbf{z}') = 1$ , a contradiction.

The following nearly perfect codes are known.

- (i) The shortened perfect single-error-correcting  $(n = 2^r - 2, 2^{n-r}, 3)2$  codes.
  - (ii) The punctured Preparata  $(n = 2^{2r} - 1, 2^{n-4r+1}, 5)3$  codes.
- This list is complete.

**Theorem 11.6.3** *There are no binary nearly perfect codes which are not perfect and have parameters other than the ones listed above.*  $\square$

The following codes are strongly uniformly packed but are neither nearly perfect nor perfect.

- (i) The punctured Hadamard  $(11, 24, 5)3$  code,  $m = 3$ .
  - (ii) The two-error-correcting BCH  $[n = 2^{2r+1} - 1, n - 4r - 2, 5]3$  codes,  $m = (n-1)/6$ .
  - (iii) The  $[n = 2^{2r-1} - 2^{r-1} - 1, n - 2r, 3]2$  codes derived by puncturing Reed-Muller codes,  $m = \binom{2^{r-1}}{2}$ .
  - (iv) The  $[n = 2^{2r-1} + 2^{r-1} - 1, n - 2r, 3]2$  codes derived by puncturing Reed-Muller codes,  $m = \binom{2^{r-1}+1}{2}$ .
- This list is also complete.

**Theorem 11.6.4** *There are no binary strongly uniformly packed codes which are neither nearly perfect nor perfect and have parameters other than the ones listed above.*  $\square$

The next step towards generalizing the concept of uniformly packed codes is to introduce, instead of  $m$ , two numbers depending on the distance of a vector from the code. Namely, a code  $C$  of length  $n$  is a *uniformly packed code of the first order* if  $R(C) = e + 1$ , and

for every  $\mathbf{z} \in \mathbb{F}^n$ ,  $d(\mathbf{z}, C) = e$ , we have  $\mathcal{A}_{e+1}(\mathbf{z}) = t_1$ ;

for every  $\mathbf{z} \in \mathbb{F}^n$ ,  $d(\mathbf{z}, C) = e + 1$ , we have  $\mathcal{A}_{e+1}(\mathbf{z}) = t_2$ .

If  $t_1 = 0$  it is clear that  $d(C) = 2e + 2$ . There are many single-error-correcting uniformly packed codes of the first order. For  $e > 1$  only the following codes do not fall under previous definitions.

(i) The twice punctured Golay  $[21, 12, 5]3$  code,  $t_1 = 1, t_2 = 4$ .

(ii) The punctured Golay  $[22, 12, 6]3$  code,  $t_1 = 0, t_2 = 2$ .

(iii) The extended Golay  $[24, 12, 8]4$  code,  $t_1 = 0, t_2 = 6$ .

The complete classification of the parameters of such codes is not known.

A code  $C$  is called *uniformly packed of the  $j$ -th order* if  $R(C) = e + j$ , and

for every  $\mathbf{z} \in \mathbb{F}^n$  such that there exists  $\mathbf{c} \in C$ ,  $d(C) - e - j \leq d(\mathbf{z}, \mathbf{c}) \leq e$ , we have  $\mathcal{A}_{e+1}(\mathbf{z}) + \dots + \mathcal{A}_{e+j} = t_1$ ;

for every  $\mathbf{z} \in \mathbb{F}^n$ ,  $d(\mathbf{z}, C) \geq e + 1$ , we have  $\mathcal{A}_{e+1}(\mathbf{z}) + \dots + \mathcal{A}_{e+j} = t_2$ .

We conclude this section with some examples of uniformly packed codes of the second order ( $j = 2$ ).

(i) The BCH  $[n = 2^{2r+1} - 1, n - 6r - 3, 7]5$  codes,  $t_1 = t_2 + 1$ ,  $t_2 = 2(2^{2r} - 1)(2^{2r-2} - 1)/15$ .

(ii) The punctured Goethals  $(n = 2^{2r} - 1, 2^{n-6r+2}, 7)5$  codes,  $t_1 = (2^{2r+1} - 17)(2^{2r-2} - 1)/15$ ,  $t_2 = 2(2^{2r} - 1)(2^{2r-2} - 1)/15$ .

(iii) The quadratic residue  $[17, 9, 5]4$  ( $t_1 = 10, t_2 = 15$ ), and  $[47, 24, 11]7$  ( $t_1 = 8, t_2 = 9$ ) codes.

## 11.7 Notes

About normality and perfect codes, see Theorems 4.2.4 and 4.5.11.

See Section 14.2 on perfect multiple coverings and Section 16.6 on tilings and perfect binary codes. See also Sections 19.1 and 19.2 for perfect coverings by  $L$ -spheres and perfect coverings by spheres with two different radii.

For perfect codes in the Lee metric, see, e.g., Golomb and Posner [257], Golomb and Welch [258], [259], Bassalygo [54], Racsmány [548], Astola [28], [29], Post [544], Solé [600].

For perfect arithmetic codes, see for instance Rao [549, Ch. 4], Astola [30], D. M. Gordon [260], Solé [600], or Lobstein and Solé [454].

For perfect codes in graphs, see, e.g., Biggs [81], [82], Heden [287], Hammond and D. H. Smith [283], Hammond [280], [282], Cameron, Thas and Payne [116], Thas [637], D. H. Smith [597], Kratochvíl [389], [390], [391], [392], [393], Etienne [219], Dvoráková-Rulíková [214].

For perfect codes correcting asymmetric errors and for some generalizations, see Fang [228], Fang, van Tilborg and Sun [229], [230], Fang, van Tilborg, Sun and Honkala [231].

**§11.1** Hamming and Golay codes are well-known codes and can be found in any book on coding theory (see [464], for instance). Binary Hamming codes are attributed to ... Hamming [279] (1950). Their generalization over  $\mathbb{F}_q$  can be found in Shapiro and Slotnick [581] (1959). The Golay codes are attributed to ... Golay [256] (1949). However, see Section 15.3, for the history of the ternary Golay code. See also Thompson [638] for more historical information.

**§11.2** The proof of Theorem 11.2.2 follows Honkala and Tietäväinen [329]. It slightly differs from that given by MacWilliams and Sloane [464].

Equality (11.2.3) was used by van Lint [430] (with the help of a computer) to settle the case when  $R \leq 1000$ ,  $q \leq 100$  and  $n \leq 1000$ .

A computer search by Tietäväinen and Perko [649] showed that there are no unknown binary perfect codes for  $R \leq 100$  and  $n \leq 10000$ .

Equalities (11.2.5) and (11.2.6) led to nonexistence results for  $R \leq 7$  and arbitrary  $q = p^r$  (see van Lint [431], [432], [434], Tietäväinen [639]) and for  $R \geq 3$ ,  $q = p^r$ , where  $p > R$  (see, e.g., van Lint [433]).

The shortening of the proof of Theorem 11.2.2 is due to Tietäväinen [641] in the case  $q > 2$  and van Lint [436] for  $q = 2$ .

H. W. Lenstra and Odlyzko (unpublished) showed that the computer search in the proof of Theorem 11.2.2 (in the last two cases) can be avoided by tightening the inequalities.

On the existence and nonexistence of perfect codes, see van Lint [437], for a ... perfect survey article.

Results of equivalence for shortened binary Golay codes can be found in Dodunekov and Encheva [205].

**§11.3** Zaremba [698] was the first to establish the uniqueness of the  $(7, 16)1$  code. Construction B is due to Mollard [492], [494], as well as its generalization using  $p$  perfect codes and  $p$  functions  $\pi_i$ . Construction C is by Solovjova [612]. Constructions D and E were presented by Zinoviev in [707] and [710], respectively. Construction E was described independently by Solovjova [610]. Construction F is by Lobstein and Zinoviev, see [456] where a possible way of permuting the symbols of  $A_2$  is described. Concatenated codes were introduced by Forney [239] and Zinoviev's generalized concatenated codes can be found in [708], [709]. Construction G has been given, in its mixed version, by Heden [289] (see Section 11.5, Construction G'). Construction H can be found in Solovjova [608] (1981, in Russian) and in Phelps [535] (1983, in English). Construction I is by Phelps [536]. Construction L is described, in terms of  $n$ -cubes, by Laborde [403].

Very recently, Rifá and Pujol [552] described a family of binary nonlinear perfect additive propelinear codes with the parameters of the Hamming codes.

See also Theorem 16.6.2 for a construction of perfect codes using tilings.

Bauer, Ganter and Hergert [61] constructed three mutually nonequivalent  $(15, 2^{11})1$  codes which are nonlinear and are not equivalent to any of the codes given by Construction A. Phelps [535] also studied the case of  $(15, 2^{11})1$  codes. Linked to the rank of a code, the kernels of binary nonlinear perfect single-error-correcting codes (the kernel is defined to be the set of all vectors that leave the code invariant under translation) are studied by Heden [290], who constructs a  $(15, 2^{11})1$  code of full rank, and by Phelps and Levan [539]. Nonsystematic perfect binary codes have been constructed for all lengths  $2^m - 1$ ,  $m \geq 8$ , by Avgustinovich and Solovjova [34], [35], and for  $m \geq 4$  by Phelps and Levan [540]. For other properties of perfect codes, see, e.g., Solovjova [609], [611], Etzion and Vardy [224], Avgustinovich and Solovjova [32], Vasiliev and Solovjova [665], [666].

The upper bound (11.3.27) on the number of nonequivalent perfect binary codes is in Avgustinovich [31]. The best known lower bound has been recently established by Avgustinovich and Solovjova [33]: the number of perfect binary codes is at least

$$2^{2^{(n+1)/2-\log(n+1)}} \cdot 6^{2^{(n+5)/4-\log(n+1)}} \cdot (1 - o(1)).$$

§11.4 The first  $q$ -ary perfect nonlinear codes were described by Schönheim [573]. These codes are also described by the same author in [574] and by B. Lindström [425] who proved Theorem 11.4.3. Construction B' is by Mollard [492], [494]. Construction B'' is due to Phelps [537]. Construction D', by Dumer, will appear in [212]. Construction H' can be found in Mollard [493].

Very recently, Etzion [221] constructed a family of  $q^{q^cn}$  nonequivalent  $q$ -ary perfect single-error-correcting codes of length  $n$ , where  $q$  is a prime power,  $n$  is sufficiently large and  $c$  is a constant less than  $1/q$ .

For  $q$  not a prime power, see, e.g., Golomb and Posner [257], B. Lindström [425], H. W. Lenstra [414], Bassalygo [53], Bassalygo, Zinoviev and Leontiev [59], Bassalygo, Zinoviev, Leontiev and Feldman [60], Bannai [44], Reuvers [551], Tietäväinen [642], Best [72], [73], [74], Laakso [400], Hong [306], [307], Phelps [537]. This case is not completely settled. One knows no example of a nontrivial perfect code. What is known is, for instance, that possible nontrivial perfect codes exist only for covering radius one or two; that, when  $q$  is of the form  $2^a 3^b$  ( $a, b \geq 1$ ), possible nontrivial perfect codes exist only for covering radius one; that no 6-ary perfect  $(7, 6^5)1$  code exists (whether  $q$ -ary  $(q + 1, q^{q-1})1$  codes exist for  $q > 6$  is an open problem); that for fixed  $q$  and covering radius two, the number of possible perfect codes is finite...

§11.5 The first example of a perfect mixed code was given by Schönheim [575], in the case of covering radius one and alphabets of sizes all equal to

powers of the same prime. This work was deepened by Herzog and Schönheim in [302] and [303] (the latter being a more detailed version of the former). For instance, they showed that if, for some  $m$  and  $\alpha \geq 2$ ,  $n-1 = (q^m - q^\alpha)/(q-1)$ , where  $q$  is a prime power, then  $\mathbf{V} = \mathbb{F}_{q^\alpha} \mathbb{F}_q^{n-1}$  contains perfect codes. In particular, if  $q = 2$  and  $m = \alpha + 1$ , then  $\mathbf{V} = \mathbb{F}_{2^\alpha} \mathbb{F}^{2^\alpha}$  contains perfect codes (cf. Construction G). Further investigation was done by B. Lindström [426] when all alphabet sizes but one are equal.

A generalized Lloyd theorem (cf. Section 11.2) was established by Heden [288] for mixed spaces  $\mathbf{V} = \mathbb{Z}_{q_1} \mathbb{Z}_{q_2} \dots \mathbb{Z}_{q_n}$  (with no assumption on the  $q_i$ 's). Reuvers [551] proved nonexistence results for certain perfect mixed codes with covering radius two or three. Very simple necessary conditions were stated by Heden and by van Wee.

Heden [288] proved that if a perfect code with covering radius  $R$  exists in  $\mathbf{V}$  and if a prime  $p$  divides at least one number  $q_i$ , then  $p$  divides the cardinality of the sphere of radius  $R$  and  $p$  divides at least  $n - R + 1$  numbers  $q_i$ .

van Wee [678] showed that if a perfect code with covering radius  $R$  exists in  $\mathbf{V}$ , then for  $i = 1, 2, \dots, R+1$  and for all  $A \subseteq \{1, \dots, n\}$  of size  $n - R + i - 1$ , the following congruences hold

$$\sum_{B \subseteq A, |B|=i} \prod_{j \in B} (q_j - 1) \equiv 0 \pmod{\binom{R+i}{i}}.$$

As a consequence, if a perfect code with covering radius  $R$  exists in  $\mathbf{V}$ , then  $R+1$  divides any difference  $q_i - q_j$ . Thus, no nontrivial perfect codes exist for football pool systems (for which the  $q_i$ 's are equal to 2 or 3; see Chapter 15).

A result by Etzion and Greenberg [222] shows that their aforementioned perfect mixed codes with covering radius two have optimal length in some sense: if a perfect mixed code has length  $n = \sum_{i=1}^t n_i$  and covering radius  $R$  in  $\mathbf{V} = \mathbb{Z}_{q_1}^{n_1} \mathbb{Z}_{q_2}^{n_2} \dots \mathbb{Z}_{q_t}^{n_t}$ , where the  $q_i$ 's are distinct and  $q_i > 2$ , then  $n \geq Rq_t + 1$ . Indeed, the Etzion-Greenberg codes have length  $n = Rq_t + 1 = 2^m + 1$ .

We already mentioned that Construction G' is by Heden [289]. As a conclusion, the case of perfect mixed codes is far from being settled, unlike perfect codes over  $\mathbb{F}_q$ .

**§11.6** The study of nearly perfect codes was started by Goethals and Snover [254]. The idea of these codes was suggested by the Johnson amendment of the Hamming bound [353]. Theorem 11.6.3 is due to K. Lindström [427] (for earlier results see van Lint [436] and Semakov, Zinoviev and Zaïtsev [576]). It has been shown in K. Lindström and Aaltonen [429] (the case  $1 \leq e \leq 10$ ) and K. Lindström [428] (the general case) that if the alphabet size  $q > 2$  is a prime power, there are no nearly perfect codes which are not perfect.

Strongly uniformly packed codes were introduced by Semakov, Zinoviev and Zaitsev [576]. Theorem 11.6.4 is by van Tilborg [650], [651]. Its proof can be found in [438, §7.5]. Nonbinary strongly uniformly packed codes were studied by van Tilborg [651], who showed that there are no strongly uniformly packed codes with  $e \geq 4$ , and all parameters for such codes with  $e \leq 3$  are known.

Uniformly packed codes of the first order were studied by Goethals and van Tilborg [255], and van Tilborg [651]. They give a big list of single-error-correcting such codes. In [651] it is proved that in the nonbinary case there are no uniformly packed codes of the first order with  $e \geq 4$ . The extended ternary Golay [12, 6, 6]3 code is a uniformly packed code of the first order with parameters  $t_1 = 0, t_2 = 4$ .

Uniformly packed codes of the  $j$ -th order were introduced by Goethals and van Tilborg [255].

The most general definition of uniform packing was introduced by Bas-salygo, Zaitsev and Zinoviev [57]. According to their definition, a code  $C$  of length  $n$  is *generalized uniformly packed* if there exist  $R(C) + 1$  numbers  $m_0, \dots, m_{R(C)}$  such that for every  $\mathbf{z} \in \mathbb{F}^n$ ,

$$\sum_{i=0}^{R(C)} m_i \mathcal{A}_i(\mathbf{z}) = 1$$

(cf. weighted coverings in Section 13.1). Every code is generalized uniformly packed if and only if it satisfies the Delsarte upper bound on covering radius (Theorem 8.3.7) with equality [58] (see the discussion following the proof of Theorem 13.2.5).

Actually, all the mentioned generalizations of perfect codes can be seen as particular cases of weighted coverings, see Section 13.1.

# Chapter 12

## Asymptotic bounds

In this chapter we discuss problems related to the asymptotic behaviour of codes when their length tends to infinity. It is convenient to study normalized parameters with respect to the length of the  $(n, K, d)R$  code  $C$  with dual distance  $d^\perp$ , viz., the *normalized covering radius*  $\rho(C) = R/n$ , *normalized minimum distance*  $\delta(C) = d/n$ , *normalized dual distance*  $\delta^\perp(C) = d^\perp/n$  and *rate*  $\kappa(C) = (\log_2 K)/n$ . Many problems may be considered in this setting. To name but a few:

- For a given rate, what is the minimum possible normalized covering radius?
- Is it possible to achieve the minimal value of normalized covering radius constructively?
- What is the proportion of codes with a given rate achieving the minimal value of normalized covering radius?
- What is the minimum rate of covering codes for fixed values of covering radius?
- What is the minimum covering radius of codes having polynomial (in  $n$ ) size?
- Given normalized minimum — or dual — distance, what are possible values for normalized covering radius?

These are the questions we attempt to answer in this chapter, organized as follows. In Section 12.1, we first prove that there exist (not necessarily linear) covering codes with normalized covering radius asymptotically meeting the sphere-covering bound; moreover, virtually all codes do. Another proof of existence is given using a greedy algorithm in Section 12.2. Then we proceed to linear codes in Section 12.3, first proving that they asymptotically achieve the sphere-covering bound; then again, like in the unrestricted case, we strengthen this statement by demonstrating that virtually all linear codes have normalized covering radius on the asymptotic sphere-covering bound.

Then, in Section 12.4, we pass to covering radius one, and show that for lengths sufficiently large, there are coverings of density arbitrarily close to 1. Next, we discuss lower and upper bounds for the covering radius of codes of small size, in Section 12.5. Here we employ a relation between covering radius and discrepancy of sets, to improve on the sphere-covering bound when  $K/n = o(n)$ . Further, in Section 12.6, we survey known asymptotic bounds on the minimum distance as a function of the rate. These results are used in Section 12.7 to derive asymptotic upper bounds on the normalized covering radius as a function of the normalized dual distance. In the last section, we characterize achievable pairs of normalized covering radius *vs* minimum distance, apart from a small undecided region which seems difficult to settle.

## 12.1 Covering radius of unrestricted codes

In the following, we assume that  $R < n/2$ . By the sphere-covering bound, for any  $(n, K)R$  code  $C$  the covering radius is lowerbounded by

$$K \geq 2^n / V(n, R).$$

Taking logarithms on both sides,

$$\log_2 K \geq n - \log_2 V(n, R),$$

and for growing  $n$ , using (2.4.5):

$$\kappa(C) = (\log_2 K)/n \geq 1 - H(\rho(C)). \quad (12.1.1)$$

Below we prove that virtually all codes have covering radius asymptotically achieving (12.1.1).

**Theorem 12.1.2** *For any  $n$  and  $R \leq n$ , there exist  $(n, K)R$  codes with*

$$K \leq \lceil n2^n \ln 2/V(n, R) \rceil.$$

**Proof.** Given a radius  $R$  and a code  $C$ , denote by  $Q_R(C)$  the set of vectors in  $\mathbb{F}^n$  that are not covered, i.e., have distance more than  $R$  from every codeword. Consider the normalized cardinality

$$q_R(C) = 2^{-n} |Q_R(C)|.$$

Let  $\mathcal{C}_K$  denote the set of all codes of size  $K$ . Clearly

$$|\mathcal{C}_K| = \binom{2^n}{K}.$$

Let us estimate  $\sum q_R(C)$ , where the sum is taken over all  $C \in \mathcal{C}_K$ .

$$\begin{aligned}
 \sum_{C \in \mathcal{C}_K} q_R(C) &= 2^{-n} \sum_{C \in \mathcal{C}_K} |Q_R(C)| \\
 &= 2^{-n} \sum_{C \in \mathcal{C}_K} \sum_{\mathbf{x} \in \mathbb{F}^n : d(\mathbf{x}, C) > R} 1 \\
 &= 2^{-n} \sum_{\mathbf{x} \in \mathbb{F}^n} \sum_{C \in \mathcal{C}_K : d(\mathbf{x}, C) > R} 1 \\
 &= 2^{-n} \sum_{\mathbf{x} \in \mathbb{F}^n} \binom{2^n - V(n, R)}{K} = \binom{2^n - V(n, R)}{K}.
 \end{aligned}$$

The last expression just counts the number of codes of size  $K$  not  $R$ -covering a particular vector of  $\mathbb{F}^n$ . Now, in the set  $\mathcal{C}_K$  there exists at least one code, say  $C'$ , with

$$\begin{aligned}
 q_R(C') &\leq \frac{\sum_{C \in \mathcal{C}_K} q_R(C)}{|\mathcal{C}_K|} = \binom{2^n - V(n, R)}{K} / \binom{2^n}{K} \\
 &\leq \frac{(2^n - V(n, R))(2^n - V(n, R) - 1) \dots (2^n - V(n, R) - K + 1)}{2^n(2^n - 1) \dots (2^n - K + 1)} \\
 &\leq \frac{(2^n - V(n, R))^K}{(2^n)^K} = (1 - 2^{-n}V(n, R))^K.
 \end{aligned}$$

Let us choose  $K = \lceil n2^n \ln 2/V(n, R) \rceil$ , which, by

$$(1 - 1/x)^x \leq e^{-1} \quad \text{for } x \geq 1,$$

implies

$$q_R(C') < 2^{-n},$$

and thus

$$|Q_R(C')| < 1.$$

But  $|Q_R(C')|$  is an integer, so  $|Q_R(C')| = 0$ , and  $C'$  is an  $R$ -covering.  $\square$

In terms of normalized parameters we have the following.

**Theorem 12.1.3** *Let  $0 \leq \rho < 1/2$ . Then there exists an infinite sequence of codes  $C_n$  of growing length  $n$  with  $\rho(C_n) \rightarrow \rho$  such that*

$$1 - H(\rho) \leq \kappa(C_n) \leq 1 - H(\rho) + O(n^{-1} \log_2 n).$$

**Proof.** Use (2.4.5).  $\square$

A simple refinement of the argument shows that the previous upper bound holds for almost all codes.

**Theorem 12.1.4** *For any positive real number  $\varepsilon$ , the fraction  $\alpha$  of  $(n, K)R$  codes with*

$$K \leq \lceil (1 + \varepsilon) n 2^n \ln 2 / V(n, R) \rceil,$$

*satisfies*

$$\alpha \geq 1 - 2^{-\varepsilon n}.$$

**Proof.** Notice that if  $C$  is not an  $R$ -covering, then  $q_R(C) \geq 2^{-n}$ . Since the proportion of “noncoverings” in  $\mathcal{C}_K$  is  $1 - \alpha$ ,

$$\sum_{C \in \mathcal{C}_K} q_R(C) \geq 2^{-n}(1 - \alpha)|\mathcal{C}_K|.$$

On the other hand, choosing  $K$  like in the theorem yields

$$\sum_{C \in \mathcal{C}_K} q_R(C) \leq 2^{-n(1+\varepsilon)}|\mathcal{C}_K|.$$

Comparing the last two inequalities gives the lower bound on  $\alpha$ .  $\square$

## 12.2 Greedy algorithm and good coverings

The following theorem shows the existence of good coverings through a semi-constructive greedy algorithm (see Section 20.3 for semi-constructive issues).

**Theorem 12.2.1 (Johnson-Stein-Lovász theorem)** *Let  $\mathbf{A}$  be a 0-1 matrix with  $N$  rows and  $M$  columns. Assume that each row contains at least  $v$  ones, and each column at most  $a$  ones. Then there exists an  $N \times K$  submatrix  $\mathbf{C}$  of  $\mathbf{A}$  with*

$$K \leq (N/a) + (M/v) \ln a \leq (M/v)(1 + \ln a) \quad (12.2.2)$$

*such that  $\mathbf{C}$  contains no all-zero row.*

**Proof.** Actually, an algorithm outputting  $\mathbf{C}$  is presented. Set  $\mathbf{A}_a = \mathbf{A}$ . Pick a maximal set of  $K_a$  columns of weight  $a$  from  $\mathbf{A}_a$  having pairwise disjoint supports ( $K_a$  may be zero). Discarding these columns and all the  $aK_a$  rows incident to one of them, we are left with a  $k_a \times (M - K_a)$  matrix  $\mathbf{A}_{a-1}$ . Clearly,

the columns of  $\mathbf{A}_{a-1}$  have weight at most  $a-1$  (otherwise such a column could be added to the previously discarded set, contradicting its maximality). Next, remove from  $\mathbf{A}_{a-1}$  a maximal set of  $K_{a-1}$  pairwise disjoint columns of weight  $a-1$  and  $(a-1)K_{a-1}$  incident rows, thus getting a  $k_{a-1} \times (M - K_a - K_{a-1})$  matrix  $\mathbf{A}_{a-2}$ . The process terminates after  $a$  steps. The union of the columns of the discarded sets is a required  $\mathbf{C}$  with

$$K = \sum_{i=1}^a K_i. \quad (12.2.3)$$

We have seen that

$$k_a = N - aK_a,$$

which we rewrite, setting  $k_{a+1} = N$ , as

$$K_a = \frac{k_{a+1} - k_a}{a}.$$

Analogously,

$$K_i = \frac{k_{i+1} - k_i}{i}, \quad i \in [1, a].$$

Now we derive an upper bound for  $k_i$  by counting the number of ones in  $\mathbf{A}_{i-1}$  in two ways: every row of  $\mathbf{A}_{i-1}$  contains at least  $v$  ones, and every column at most  $i-1$  ones, thus

$$vk_i \leq (i-1)(M - K_a - \dots - K_i) \leq (i-1)M.$$

From (12.2.3)

$$\begin{aligned} K &= \sum_{i=1}^a K_i = \sum_{i=1}^a \frac{k_{i+1} - k_i}{i} \\ &= \frac{k_{a+1}}{a} + \frac{k_a}{a(a-1)} + \frac{k_{a-1}}{(a-1)(a-2)} + \dots + \frac{k_2}{2 \cdot 1} \\ &\leq N/a + (1/a + 1/(a-1) + \dots + 1/2)M/v, \end{aligned}$$

thus giving the result. The second inequality follows from the evident  $Nv \leq Ma$ .  $\square$

Let us show the relevance of the previous theorem to coverings. Choose for  $\mathbf{A}$  the incidence matrix points/spheres. That is, the  $2^n$  columns of  $\mathbf{A}$  represent points, the  $2^n$  rows represent the centres of spheres of radius  $R$ , with a 1 at intersection of row  $i$  and column  $j$  if sphere  $i$  contains point  $j$ . Every row therefore contains a number of 1's equal to the number of points in the sphere, viz.,  $V(n, R)$ . There are exactly  $V(n, R)$  1's in every column since

every point belongs to exactly  $V(n, R)$  spheres. In this setting, the theorem yields a semi-construction of a code  $C$  of size  $K$  intersecting all spheres, i.e., an  $R$ -covering (consisting here of column vectors). By (12.2.2) we have

$$K \leq \frac{2^n}{V(n, R)} (1 + \ln V(n, R)) < \frac{n2^n \ln 2}{V(n, R)},$$

cf. Theorem 12.1.2.

### 12.3 Covering radius of linear codes

In the case of linear codes we prove the existence of coverings achieving the sphere-covering bound by a simple counting argument. The extension of this result to virtually all linear codes requires a more complicated reasoning.

**Lemma 12.3.1** *For any  $U \subseteq \mathbb{F}^n$ , there exists  $\mathbf{x} \in \mathbb{F}^n$  such that*

$$|U \cap (U + \mathbf{x})| \leq |U|^2/2^n.$$

**Proof.** The multiset  $V = \bigcup_{\mathbf{x} \in \mathbb{F}^n} (U + \mathbf{x})$  is just the  $|U|$ -time repetition of  $\mathbb{F}^n$ . Hence every element of  $U$  appears in  $V$  exactly  $|U|$  times, and there are all in all  $|U|^2$  elements from  $U$  in  $V$ . Since  $V$  consists of  $2^n$  cosets of  $U$ , there is at least one coset containing at most  $|U|^2/2^n$  elements from  $U$ .  $\square$

**Theorem 12.3.2** *For any  $n$  and  $R \leq n$ , there exist  $[n, k]R$  codes with*

$$k \leq \lceil n - \log_2 V(n, R) + \log_2 n + \log_2(\ln 2) \rceil.$$

**Proof.** Construct the desired code in a recursive manner. Start from the code  $C^{(0)}$  consisting of one word  $0^n$ . At the  $i$ -th step, add a coset  $C^{(i)} + \mathbf{x}_i$  to  $C^{(i)}$ , thus constructing  $C^{(i+1)}$ . The  $\mathbf{x}_i$  is chosen to minimize  $|Q_R(C^{(i+1)})|$ , the number of vectors not  $R$ -covered by  $C^{(i+1)}$ . Notice that

$$Q_R(C^{(i)} + \mathbf{x}) = \mathbf{x} + Q_R(C^{(i)}),$$

and

$$Q_R(C^{(i+1)}) = Q_R(C^{(i)}) \cap Q_R(C^{(i)} + \mathbf{x}) = Q_R(C^{(i)}) \cap (\mathbf{x} + Q_R(C^{(i)})).$$

From Lemma 12.3.1 we deduce

$$|Q_R(C^{(i+1)})| \leq |Q_R(C^{(i)})|^2/2^n,$$

or, in normalized form,

$$q_R(C^{(i+1)}) \leq (q_R(C^{(i)}))^2. \quad (12.3.3)$$

Since  $q_R(C^{(0)}) = (1 - 2^{-n}V(n, R))$ ,

$$q_R(C^{(k)}) \leq (1 - 2^{-n}V(n, R))^{2^k},$$

and the proof ends exactly like with unrestricted codes (see Theorem 12.1.2).  $\square$

In terms of normalized parameters, we proved the following result.

**Theorem 12.3.4** *Let  $0 \leq \rho < 1/2$ . Then there exists an infinite sequence of linear codes  $C_n$  of growing length  $n$  with  $\rho(C_n) \rightarrow \rho$  and*

$$1 - H(\rho) \leq \kappa(C_n) \leq 1 - H(\rho) + O(n^{-1} \log_2 n).$$

$\square$

Now we prove in two stages that the proportion of linear codes achieving the claimed bound is quite large. First we prove that if the size of the codes is chosen so that every point is on the average  $R$ -covered by  $n^\alpha$ ,  $\alpha > 1$ , codewords, then almost all codes are almost  $R$ -coverings, i.e.,  $R$ -cover the whole space but possibly a small number of points. Successive appendings of  $\lceil \log_2 n \rceil$  cosets to these almost  $R$ -coverings convert them into complete  $R$ -coverings without essentially decreasing their proportion.

**Theorem 12.3.5** *Let  $0 \leq \rho < 1/2$ . Let  $\mathcal{C}_{k,n}$  be the ensemble of  $2^{kn}$  linear codes generated by all possible binary  $k \times n$  matrices. Let  $R_n = \lfloor \rho n \rfloor$ . Then there exists a sequence  $k_n$  with*

$$k_n/n \leq 1 - H(\rho) + O(n^{-1} \log_2 n)$$

such that the fraction of codes  $C_n \in \mathcal{C}_{k_n,n}$  that are  $R_n$ -coverings tends to 1.

**Proof.** Denote  $K = 2^k$ ,  $k^* = k - \lceil \log_2 n \rceil$ ,  $K^* = 2^{k^*}$ . Consider  $\mathcal{C}_{k^*,n}$  the ensemble of linear codes defined by  $k^* \times n$  generator matrices with binary elements chosen randomly and independently with probability  $1/2$ . Any nonvoid linear combination of rows of the generator matrix gives all possible  $2^n$  vectors with the same probability, the zero codeword corresponds to the void linear combination of the rows and is present in all codes. Assume some consistent enumeration of the codewords in these codes, i.e., the words with the same index are given by the same linear combination of vectors from the generator matrix. By convention, the first codeword in all codes is the zero word. Let  $\mathbf{c}_i$  be the  $i$ -th codeword of a code in  $\mathcal{C}_{k^*,n}$ . Then, given an  $\mathbf{x} \in \mathbb{F}^n$ ,

$$P(\mathbf{c}_i = \mathbf{x}) = \begin{cases} 1 & \text{if } i = 1 \text{ and } \mathbf{x} = \mathbf{0}; \\ 0 & \text{if } i = 1 \text{ and } \mathbf{x} \neq \mathbf{0}; \\ 2^{-n} & \text{if } i \in [2, K^*]. \end{cases}$$

For  $i \neq j$ , the codewords  $\mathbf{c}_i$  and  $\mathbf{c}_j$  are independent.

For every  $\mathbf{x} \in \mathbb{F}^n$  define the random variable  $\eta_i$  by  $\eta_i = 1$  if the  $i$ -th codeword  $R$ -covers  $\mathbf{x}$  and  $\eta_i = 0$  otherwise. Let

$$\chi = \sum_{i=1}^{K^*} \eta_i.$$

Then  $\chi$  is equal to the number of codewords  $R$ -covering  $\mathbf{x}$ . Now, averaging over  $C$  in  $\mathcal{C}_{k^*,n}$ :

$$E(\chi) = \begin{cases} (K^* - 1)V(n, R)2^{-n} + 1 & \text{for } w(\mathbf{x}) \leq R \\ (K^* - 1)V(n, R)2^{-n} & \text{otherwise.} \end{cases}$$

Using the pairwise independence of the  $\eta_i$ 's, we see that the variance  $\text{Var}(\chi)$  satisfies

$$\begin{aligned} \text{Var}(\chi) &= \sum_{i=1}^{K^*} \text{Var}(\eta_i) = \sum_{i=1}^{K^*} (E(\eta_i^2) - E(\eta_i)^2) \\ &\leq \sum_{i=1}^{K^*} E(\eta_i^2) = \sum_{i=1}^{K^*} E(\eta_i) = E(\chi). \end{aligned}$$

By Chebyshev's inequality,

$$P(|\chi - E(\chi)| > 2^\epsilon \sqrt{E(\chi)}) < \frac{\text{Var}(\chi)}{2^{2\epsilon} E(\chi)} \leq 2^{-2\epsilon}.$$

Let  $\beta = K^*V(n, R)2^{-n}$  be the average number of codewords in a sphere. Then, since  $E(\chi) \leq \beta + 1 \leq E(\chi) + 2$ , we have

$$P(\chi < \beta(\epsilon) := \beta - 2^\epsilon \sqrt{\beta + 1}) < 2^{-2\epsilon}.$$

We call a point *remote* whenever it is  $R$ -covered by fewer than  $\beta(\epsilon)$  codewords. Let  $Q_0$  stand for the set of remote points,  $q_0 = |Q_0|2^{-n}$ . So far we have derived an upper bound on the normalized average number  $E(q_0)$  of remote points for codes in  $\mathcal{C}_{k^*,n}$ :

$$E(q_0) < 2^{-2\epsilon}.$$

Using Markov's inequality, we estimate the deviation of the normalized number of remote points from the mean,

$$P(q_0 > 2^\epsilon E(q_0)) < 2^{-\epsilon}.$$

Thus the inequality

$$q_0 < 2^{-\epsilon} \tag{12.3.6}$$

holds for a proportion greater than  $1 - 2^{-\varepsilon}$  of all codes.

Now we apply the procedure of successive appending cosets to an initial code  $C' \in \mathcal{C}_{k^*,n}$  satisfying (12.3.6). An argument similar to the derivation of (12.3.3) shows that the average normalized number  $q_1$  over  $\mathbf{x} \in \mathbb{F}^n$ , of remote points for  $C' \cup (C' + \mathbf{x})$  satisfies the inequality

$$E(q_1) \leq q_0^2.$$

From Markov's inequality, we get

$$P(q_1 > 2^\lambda E(q_1)) < 2^{-\lambda},$$

thus the proportion of codes which satisfy

$$q_1 < 2^{\lambda-2\varepsilon},$$

is at least  $1 - 2^{-\lambda}$ . Applying the same procedure to all the codes satisfying (12.3.6), we conclude that  $q_1 < 2^{\lambda-2\varepsilon}$  for a proportion at least  $(1 - 2^{-\varepsilon})(1 - 2^{-\lambda})$  of codes in  $\mathcal{C}_{k^*+1,n}$ .

Continuing the procedure we get

$$q_i < 2^{2^i(\lambda-\varepsilon)-\lambda} \quad (12.3.7)$$

for a proportion at least  $(1 - 2^{-\varepsilon})(1 - 2^{-\lambda})^i$  of the codes in  $\mathcal{C}_{k^*+i,n}$ . We stop at step  $m$  such that

$$q_m < 2^{-n}. \quad (12.3.8)$$

Choose  $m = \lceil \log_2 n \rceil$ . To satisfy (12.3.8) it is sufficient to choose  $\lambda = \varepsilon - 1$ .

Thus, for a proportion of codes from  $\mathcal{C}_{k,n}$  at least equal to

$$(1 - 2^{-\varepsilon})(1 - 2^{-\varepsilon+1})^{\lceil \log_2 n \rceil}, \quad (12.3.9)$$

we have  $q_m < 2^{-n}$ , i.e., every  $\mathbf{x} \in \mathbb{F}^n$  is  $R$ -covered by at least  $\beta(\varepsilon)$  codewords. Choose  $\varepsilon = 2 \log_2 \log_2 n$ . Plugging the values in (12.3.9), assuming  $\beta \geq n^\alpha$ ,  $\alpha > 1$ , and noticing that  $\beta(\varepsilon) > 0$  guarantees an  $R$ -covering, we get the claim.  $\square$

A more complicated reasoning gives a stronger statement in terms of the fraction of codes involved; it is presented here without proof.

**Theorem 12.3.10** *Under the assumptions of the previous theorem, the bound*

$$k_n/n \leq 1 - H(\rho) + O(n^{-1/3} \log_2 n)$$

*holds for a fraction of linear codes greater than  $1 - 2^{-n \log_2 n}$ .*  $\square$

The fact that almost every linear code achieves asymptotically the sphere-covering bound allows the following construction of infinite length coverings. Recall that the direct sum of two codes with parameters  $[n, k]R_1$  and  $[n, k]R_2$  gives a  $[2n, 2k]R_1 + R_2$  code. Given  $\kappa$ , let us take a sequence of numbers  $k_n$  such that  $k_n/n \rightarrow \kappa$  when  $n$  tends to infinity. Given  $k_n$  we construct  $C = \sum \oplus C^{(i)}$ , the direct sum of *all* linear codes  $C^{(i)} \in \mathcal{C}_{k_n, n}$ . Notice that this procedure is constructive: we set all possible 0-1 matrices of size  $k_n \times n$  on the diagonal of a block-diagonal  $k_n 2^{k_n n} \times n 2^{k_n n}$  (generator) matrix, and put zeros elsewhere. The parameters of the resulting code are

$$[N = n 2^{k_n n}, k_n 2^{k_n n}] \sum R_i,$$

where  $R_i$  is the covering radius of  $C^{(i)}$ . By the previous theorem,

$$\begin{aligned} \rho(C) &= \frac{1}{N} \sum R_i \\ &\leq (1 - 2^{-n \log_2 n}) H^{-1} \left( 1 - \frac{k_n}{n} + O \left( n^{-1/3} \log_2 n \right) \right) + 2^{-n \log_2 n}. \end{aligned}$$

Hence,

$$\kappa(C) \rightarrow 1 - H(\rho(C)),$$

as well as

$$\kappa(C) = k_n/n \rightarrow \kappa.$$

So, in contrast to error-correcting codes, for coverings the best asymptotic bound is achieved *constructively*.

## 12.4 Density of coverings

In this section we address the asymptotic behaviour of the code parameters when the covering radius is fixed while the length grows. Recall from (2.1.4) that the density of an  $(n, K)R$  code is

$$\mu(C) = K V(n, R) 2^{-n},$$

i.e., the ratio between the total size of spheres in the covering and the size of the space. Given  $n$  and  $R$ , we define the minimal density

$$\mu(n, R) = K(n, R) V(n, R) 2^{-n}.$$

Analogously, we define for linear codes

$$\mu[n, R] = 2^{k[n, R]} V(n, R) 2^{-n}.$$

By the sphere-covering bound, the density is at least 1, and equals 1 only for perfect codes. So, for Hamming codes

$$\mu(\mathcal{H}_m) = \mu(2^m - 1, 1) = \mu[2^m - 1, 1] = 1, \quad m = 1, 2, \dots$$

The sphere-covering bound together with lengthened Hamming codes (direct sums of Hamming codes and the whole space) yields

$$k[n, 1] = n - \ell, \text{ if } 2^\ell \leq n + 1 < 2^{\ell+1}, \quad (12.4.1)$$

and

$$\mu[n, 1] = 2^{-\ell}(n + 1), \text{ if } 2^\ell \leq n + 1 < 2^{\ell+1}, \quad (12.4.2)$$

giving

$$1 \leq \mu[n, 1] < 2.$$

Define

$$\mu^*(R) = \lim_{n \rightarrow \infty} \sup \mu(n, R),$$

and

$$\mu^*[R] = \lim_{n \rightarrow \infty} \sup \mu[n, R],$$

the asymptotically (worst) densities for coverings of given radius. Clearly,  $\mu^*(R) \leq \mu^*[R]$ .

The above results on the density of linear coverings of radius 1 provide

$$\mu^*[1] = 2.$$

**Theorem 12.4.3** For fixed  $R$ ,

$$1 \leq \mu^*(R) \leq \mu^*[R] < \text{const.}$$

**Proof.** From (12.4.1),

$$K(n, 1) \leq 2^{k[n, 1]} < \frac{2^{n+1}}{n + 1},$$

so, iterating the direct sum of the code with itself yields

$$K(Rn, R) \leq 2^{k[Rn, R]} < \frac{2^{nR+R}}{(n + 1)^R}.$$

Therefore,

$$\mu(Rn, R) \leq \mu[Rn, R] < \frac{2^R V(Rn, R)}{(n + 1)^R} < \frac{2^R (R + 1) \binom{Rn}{R}}{(n + 1)^R}$$

$$< \frac{2^R(R+1)(Rn)^R}{R!(n+1)^R} < \frac{2^R R^R (R+1)}{R!},$$

which depends only on  $R$ . Clearly, we did not try to obtain the best constant.  $\square$

We now prove that  $\mu^*(1) = 1$ . First we need some recursive relations for the densities of coverings.

**Lemma 12.4.4** *If there exists a 1-covering  $C$  of  $\mathbb{F}^n$ , then there exists a 1-covering  $C'$  of  $\mathbb{F}^{n+\ell}$ ,  $\ell = 0, 1, 2, \dots$ , with density*

$$\mu(C') = \mu(C) \frac{1+n+\ell}{1+n}.$$

**Proof.** Consider  $C' = C \oplus \mathbb{F}^\ell$ .  $\square$

Thus, for growing  $n$ , having constructed a family of codes of some constant density, we keep asymptotically the same density for the intervals  $[n, n+o(n)]$ .

**Lemma 12.4.5** *If there exists a 1-covering  $C$  of  $\mathbb{F}^n$ , then there exist 1-coverings of  $\mathbb{F}^N$ ,  $N = 2^j n + 2^j - 1$ ,  $j = 0, 1, 2, \dots$ , with the same density as  $C$ .*

**Proof.** Use  $j$  times the  $(\mathbf{u}, \mathbf{u} + \mathbf{v})$  construction (see Theorem 3.4.3).  $\square$

We now use the cascading construction of Section 3.6. For the sake of completeness, we repeat it here in the particular case of inner Hamming codes. Recall from (2.1.4) that the density of an  $(n, K)_q$  1 code is

$$\mu(C) = KV_q(n, 1)/q^n = K(1 + (q-1)n)q^{-n}.$$

**Lemma 12.4.6** *If there exists a  $2^\ell$ -ary  $(N, K)$  1 covering  $V$ , then there exists a binary  $(N(2^\ell - 1), 2^{N(2^\ell - \ell - 1)}K)$  1 covering  $C$ . Consequently,  $\mu(C) = \mu(V)$ .*

**Proof.** Let  $\mathcal{H}_\ell$  be the Hamming code of length  $n = 2^\ell - 1$ . Partition the space  $\mathbb{F}^n$  into the cosets of  $\mathcal{H}_\ell$ , namely,

$$\mathbb{F}^n = (C_0 = \mathcal{H}_\ell) \cup C_1 \cup \dots \cup C_n.$$

Every vector in  $\mathbb{F}^n$  belongs to exactly one coset  $C_i$  and is at distance one from all other cosets  $C_j$ ,  $j \neq i$ . The size of every coset is  $2^{2^\ell - 1 - \ell}$ .

We construct a covering of  $\mathbb{F}^{nN}$  as the union of all

$$C_{v_1} \oplus C_{v_2} \oplus \dots \oplus C_{v_N}, \tag{12.4.7}$$

where  $(v_1, \dots, v_N)$  runs through all codewords of  $V$ . To prove that the resulting code is a 1-covering, notice that for an arbitrary vector  $\mathbf{x} = (x_1, \dots, x_N) \in (\mathbb{F}^n)^N$  one finds the  $2^\ell$ -ary vector  $\mathbf{w} = (w_1, \dots, w_N)$  where  $x_i \in C_{w_i}$ . Since  $V$  is a 1-covering, we can find a vector  $\mathbf{v} \in V$ , such that  $d(\mathbf{v}, \mathbf{w}) \leq 1$ . The set of vectors produced by  $\mathbf{v}$  contains the necessary word covering  $\mathbf{x}$ .  $\square$

To construct nonbinary covering codes we use the following “supercode” construction, formulated for the particular case we need.

**Lemma 12.4.8** *Let  $C$  be a linear  $q$ -ary  $[n, k]_1$  covering, with  $q \leq 2^\ell$  a prime power. Then there exists a (nonlinear)  $2^\ell$ -ary  $(n, K)_1$  covering  $V$  with*

$$K \leq q^{k-n} 2^{\ell n}.$$

Consequently,

$$\mu(V) \leq \mu(C) \frac{1 + (2^\ell - 1)n}{1 + (q - 1)n}.$$

**Proof.** Take some partition of  $\mathbb{F}_{2^\ell}$  into  $q$  nonempty subsets or parts, and establish a (surjective) mapping  $\sigma : \mathbb{F}_{2^\ell} \rightarrow \mathbb{F}_q$ . For the supercode  $V$  we take all vectors  $\mathbf{v} = (v_1, \dots, v_n) \in (\mathbb{F}_{2^\ell})^n$  such that

$$\sigma(\mathbf{v}) := (\sigma(v_1), \dots, \sigma(v_n)) \in C.$$

Clearly,  $V$  is a 1-covering. Indeed, for every  $\mathbf{x} \in (\mathbb{F}_{2^\ell})^n$  there is a vector generated by a  $\sigma(\mathbf{v}) \in C$ , where  $d(\sigma(\mathbf{v}), \sigma(\mathbf{x})) \leq 1$ , which 1-covers  $\mathbf{x}$ . Now we have to estimate the size of the code. This is difficult to do for a particular code, but it is easy to compute its average over cosets of the code. Partition  $\mathbb{F}_q^n$  into the  $q^{n-k}$  cosets of  $C$ , and then apply  $\sigma$  to all vectors in  $(\mathbb{F}_{2^\ell})^n$ . This gives rise to  $(2^\ell)^n$   $q$ -ary vectors, partitioned into  $q^{n-k}$  cosets. Having in mind that every coset of  $C$  is also a 1-covering, and that there exists a part having at most the average number of words, we get the claim.  $\square$

Applying Lemma 12.4.8 to the  $q$ -ary Hamming codes with parameters  $[N = (q^i - 1)/(q - 1), k = N - i]_1$ , and using the evident inequality:

$$(1 + (2^\ell - 1)n)/(1 + (q - 1)n) \leq (2^\ell - 1)/(q - 1)$$

for  $q \leq 2^\ell$ , we get the following corollary.

**Corollary 12.4.9** *For  $q$  a prime power,  $q \leq 2^\ell$ , there exist 1-coverings  $V$  of  $(\mathbb{F}_{2^\ell})^N$ ,  $N = (q^i - 1)/(q - 1)$ ,  $i = 1, 2, \dots$ , of density*

$$\mu(V) \leq \frac{2^\ell - 1}{q - 1}.$$

$\square$

Now Lemma 12.4.6, combined with coverings from the previous corollary and Lemma 12.4.5, gives

**Theorem 12.4.10** *For  $q$  a prime power,  $q \leq 2^\ell$ , and  $i = 1, 2, \dots, j = 0, 1, \dots$ , there exist binary 1-coverings  $C(\ell, i, j)$  of length*

$$2^j(2^\ell - 1) \frac{q^i - 1}{q - 1} + 2^j - 1$$

with density

$$\mu(C(\ell, i, j)) \leq \frac{2^\ell - 1}{q - 1}.$$

□

Choosing for  $q$  the maximal prime power less than  $2^\ell$ , we get a sequence of coverings of density approaching 1 when  $n$  grows and  $q/2^\ell \rightarrow 1$ .

**Theorem 12.4.11**  $\mu^*(1) = 1$ .

**Proof.** Let  $q = 2^\ell(1-\varepsilon)$ , with  $\ell$  growing. From results on the density of prime numbers it follows that  $\varepsilon = O(2^{\beta\ell})$ ,  $\beta < 0$ . Set  $z = \lfloor -2/\log_2(1-\varepsilon) \rfloor$ . Noticing that for  $\ell$  large enough we get by Theorem 12.4.10 the sequence of lengths  $2^{j+\ell}q^{i-1}(1+o(1))$ , assume that  $j$  is always chosen such that  $j = \ell(z-i) + a$ , with  $i \leq z$ ,  $a = 0, 1, \dots$ . Then the sequence of lengths becomes

$$2^{\ell z+a}(1-\varepsilon)^{i-1}(1+o(1)).$$

When  $i$  runs from 1 to  $z$  the length changes from  $2^{\ell z+a}(1+o(1))$  to  $2^{\ell z+a}(1-\varepsilon)^{z-1} = 2^{\ell z+a-2}(1+o(1))$ . Checking that the distance between two consecutive lengths corresponding to  $i$  and  $i+1$  is  $o(2^{\ell z+a})$ , we conclude that the lengths constitute a dense subsequence in the interval  $[2^{\ell z+a-1}, 2^{\ell z+a}]$ , where the density of  $C(\ell, i, j)$  is at most  $(2^\ell - 1)/(q - 1) \rightarrow 1$ . Application of Lemma 12.4.4 fully covers the interval. When  $a$  runs from 0 to infinity, we obtain the sequence of intervals completely covering all the lengths greater than  $2^{\ell z}$ . □

## 12.5 Coverings of small size

Previously, we have considered situations when the size of the coverings is exponential in  $n$ . Now we switch to the case when the size is subexponential, or even polynomial, in  $n$ .

**Theorem 12.5.1** For every  $(n, K)R$  code  $C$ ,

$$R \geq n/2 - \sqrt{n \log_2 K \ln 2/2}.$$

**Proof.** This is a variation on the sphere-covering bound. Notice that the latter gives the following tight bound, valid for all  $R$  and  $K$ :

$$H(\rho(C)) \geq 1 - \kappa(C).$$

Using the easily checked inequality

$$H(1/2 - \sqrt{x}) \leq 1 - 2x/\ln 2,$$

we infer

$$1 - 2 \frac{(1/2 - \rho(C))^2}{\ln 2} \geq 1 - \kappa(C),$$

giving the claim.  $\square$

The sphere-covering bound cannot be improved asymptotically if we assume that  $K = n^\alpha$ ,  $\alpha > 1$ . To see this, we rephrase Theorem 12.1.2:

**Theorem 12.5.2** There exists an infinite sequence of  $(n, K)R$  codes with

$$R \leq n/2 - \sqrt{n(\log_2 K - \log_2 n + O(1)) \ln 2/2}.$$

$\square$

Let us introduce now the discrepancy of a code. This combinatorial concept is strongly related to covering radius: let  $\mathbf{x}^\pm$  be a  $\pm 1$ -vector, and  $C = \{\mathbf{c}_1, \dots, \mathbf{c}_K\}$  be a binary  $(n, K)$  code. We set

$$\chi_{\mathbf{x}^\pm}(\mathbf{c}_i) = \langle \mathbf{c}_i, \mathbf{x}^\pm \rangle.$$

Define the *discrepancy* of  $C$  with respect to  $\mathbf{x}^\pm$  by

$$\text{disc}(C, \mathbf{x}^\pm) = \max_{i=1, \dots, K} |\chi_{\mathbf{x}^\pm}(\mathbf{c}_i)|,$$

and the discrepancy of  $C$  by

$$\text{disc}(C) = \min_{\mathbf{x}^\pm \in \{\pm 1\}^n} \text{disc}(C, \mathbf{x}^\pm).$$

To see the relation with covering radius, consider the vector  $\mathbf{x}$  obtained from  $\mathbf{x}^\pm$  by changing 1's to 0's and -1's to 1's. Let  $\mathbf{x} \cap \mathbf{c}_i$  stand for the vector

having 1's in the coordinates where both  $\mathbf{x}$  and  $\mathbf{c}_i$  have 1's and having 0's elsewhere. As easily checked:

$$|\chi_{\mathbf{x}^\pm}(\mathbf{c}_i)| = |w(\mathbf{x} \cap \mathbf{c}_i) - w(\bar{\mathbf{x}} \cap \mathbf{c}_i)| = |w(\mathbf{x}) - w(\mathbf{x} + \mathbf{c}_i)|.$$

Since  $\text{disc}(C, \mathbf{x}^\pm) = \text{disc}(C, \bar{\mathbf{x}}^\pm)$ , we may assume  $w(\mathbf{x}) \geq n/2$ . Hence,

$$\text{disc}(C, \mathbf{x}^\pm) = \max_{i=1, \dots, K} \{|w(\mathbf{x}) - w(\mathbf{x} + \mathbf{c}_i)|\},$$

and

$$\begin{aligned} R(C) &= \max_{\mathbf{x} \in \mathbb{F}^n} d(\mathbf{x}, C) \\ &= \max_{\mathbf{x} \in \mathbb{F}^n} \min_{i=1, \dots, K} w(\mathbf{x} + \mathbf{c}_i) \\ &\geq n/2 - \text{disc}(C). \end{aligned} \tag{12.5.3}$$

So, upper bounds on discrepancy give lower bounds on covering radius.

In what follows we make intensive use of Chernoff's inequality.

**Lemma 12.5.4 (Chernoff's inequality)** *Let  $x_i^\pm$ ,  $i = 1, \dots, m$ , be mutually independent random variables with  $P(x_i^\pm = 1) = P(x_i^\pm = -1) = 1/2$ , and let*

$$s_m = x_1^\pm + \dots + x_m^\pm.$$

*Then, for  $a > 0$ ,*

$$P(s_m > a) < e^{-a^2/2m}.$$

**Proof.** Let  $m > 0$  and  $a > 0$  be fixed and  $\lambda > 0$  arbitrary. For every  $i = 1, 2, \dots, m$ ,

$$E(e^{\lambda x_i^\pm}) = \frac{1}{2}(e^\lambda + e^{-\lambda}) \leq e^{\lambda^2/2},$$

where the last inequality immediately follows by comparing the Taylor series expansions of the two functions. Since the variables  $x_i^\pm$  are mutually independent, so are  $e^{\lambda x_i^\pm}$ , and

$$E(e^{\lambda s_m}) = \prod_{i=1}^m E(e^{\lambda x_i^\pm}) \leq e^{\lambda^2 m/2}.$$

For the positive random variable  $y = e^{\lambda s_m}$  we have, using Markov's inequality,

$$P(y > \alpha E(y)) < \frac{1}{\alpha}$$

when  $\alpha > 0$ , and therefore

$$P(s_m > a) = P(e^{\lambda s_m} > e^{\lambda a}) < \frac{E(e^{\lambda s_m})}{e^{\lambda a}} \leq e^{\frac{1}{2}\lambda^2 m - \lambda a}.$$

The claim follows by choosing  $\lambda = a/m$ .  $\square$

We start from the following weaker version of the sphere-covering bound, however giving a (probabilistic) flavour of the methods used later.

**Theorem 12.5.5** *For every  $(n, K)R$  code,*

$$R \geq n/2 - \sqrt{2n \ln(2K)}.$$

**Proof.** Let  $C = \{c_1, \dots, c_K\}$  be an  $(n, K)$  code. Choose  $x^\pm$  at random, setting every symbol independently to 1 or  $-1$  with probability  $1/2$ . Let  $\nu_i$  be the random variable equal to 1 for  $|\chi_{x^\pm}(c_i)| > \alpha$ , and 0 otherwise. Set  $\alpha = \sqrt{2n \ln(2K)}$ . Hence,  $\chi_{x^\pm}(c_i)$  has distribution  $s_{w(c_i)}$  and by Chernoff's bound

$$\begin{aligned} E(\nu_i) &= 0 \cdot P(|\chi_{x^\pm}(c_i)| \leq \alpha) + 1 \cdot P(|\chi_{x^\pm}(c_i)| > \alpha) = P(|\chi_{x^\pm}(c_i)| > \alpha) \\ &< 2e^{-\alpha^2/2w(c_i)} \leq 2e^{-\alpha^2/2n} = 1/K, \end{aligned}$$

by the choice of  $\alpha$ . The expectation of the number  $\nu$  of codewords with  $|\chi_{x^\pm}(c_i)| > \alpha$ , is

$$E(\nu) = \sum_{i=1, \dots, K} E(\nu_i) < K(1/K) = 1.$$

Thus for some  $x^\pm$ ,  $\nu = 0$  must hold. This means  $\text{disc}(C) \leq \alpha$ .  $\square$

We saw that the sphere-covering bound is asymptotically tight for codes of size growing faster than linearly in  $n$ . So, consider now the situation when the size of the code is less than  $n^\alpha$ ,  $\alpha \leq 1$ . We first prove, in a slightly weaker version, the following theorem.

**Theorem 12.5.6** *For all  $(n, n)R$  codes,*

$$R \geq n/2 - 5.32 \cdot \sqrt{n}.$$

Note that Theorem 12.5.5 would only give in this case  $n/2 - O(\sqrt{n \ln n})$ . The best known value for the constant in the theorem is 5.32, but we prove here a simpler result with a weaker constant, namely 11. To do this, we need some auxiliary lemmas.

We choose now  $x^\pm$  in the set  $\{\pm 1, 0\}^n$ , allowing, along with  $\pm 1$ , the occurrence of — usually a small number of — 0's. The discrepancy of such vectors is defined exactly like in the  $\pm 1$  case.

**Lemma 12.5.7** *Let  $C$  be an  $(n, n)$  code. Then there exists a vector  $\mathbf{x}_0^\pm \in \{\pm 1, 0\}^n$ , with at most  $10^{-9}n$  0's and*

$$\text{disc}(C, \mathbf{x}_0^\pm) \leq 10\sqrt{n}.$$

**Proof.** Let  $C = \{\mathbf{c}_1, \dots, \mathbf{c}_n\}$ , and  $\mathbf{x}^\pm$  be chosen randomly from  $\{\pm 1\}^n$ . For  $i = 1, \dots, n$ , define

$$b_i = \text{nearest integer to } \frac{\chi_{\mathbf{x}^\pm}(\mathbf{c}_i)}{20\sqrt{n}}.$$

From Chernoff's bound we can derive the following inequalities:

$$P(b_i = 0) > 1 - 2e^{-50},$$

$$P(b_i = s) = P(b_i = -s) < e^{-50(2s-1)^2}.$$

Now we have for the entropy

$$H(b_i) = \sum_{j=-\infty}^{\infty} -P(b_i = j) \log_2 P(b_i = j)$$

the upper bound

$$(1 - 2e^{-50})(-\log_2(1 - 2e^{-50})) + 2 \sum_{j=1}^{\infty} e^{-50(2j-1)^2} (-\log_2 e^{-50(2j-1)^2}).$$

The latter sum converges and is strongly dominated by the term  $j = 1$ . Calculation gives

$$H(b_i) \leq \varepsilon = 3 \cdot 10^{-20}.$$

Now consider the  $n$ -tuple  $(b_1, \dots, b_n)$ . By the subadditivity of entropy,

$$H((b_1, \dots, b_n)) \leq \sum_{i=1}^n H(b_i) \leq \varepsilon n.$$

If a random variable  $Z$  assumes no value with probability greater than  $2^{-t}$ , then  $H(Z) \geq t$ . Hence, there is a particular  $n$ -tuple  $(s_1, \dots, s_n)$  such that

$$P((b_1, \dots, b_n) = (s_1, \dots, s_n)) \geq 2^{-\varepsilon n}.$$

Since  $\mathbf{x}^\pm$  is chosen from the set of  $2^n$  equiprobable  $\pm 1$ -vectors, there is a subset  $S \subset \{\pm 1\}^n$ , consisting of at least  $2^{(1-\varepsilon)n}$  vectors having the same value  $(b_1, \dots, b_n)$ .

Endowing  $\{\pm 1\}^n$  with the Hamming metric, and recalling that in the Hamming space the set of a given size with minimal diameter is the ball (see

Theorem 2.4.16), we infer that in any set of size at least  $2^{(1-\epsilon)n}$  there always exist two vectors at Hamming distance at least  $n(1 - 10^{-9})$ . Indeed, see (2.4.5), the size of a ball of radius  $\alpha n$ ,  $\alpha < 1/2$ , is

$$V(n, \alpha n) \leq 2^{nH(\alpha)} \leq 2^{n(1-2(1/2-\alpha)^2/\ln 2)}.$$

Direct calculation shows that if  $\alpha = (1/2)(1 - 10^{-9})$ , then  $V(n, \alpha n) < 2^{n(1-\epsilon)}$ . So, there exist two vectors, say  $\mathbf{x}_1^\pm$  and  $\mathbf{x}_2^\pm \in S$ , having the same  $(b_1, \dots, b_n)$  and being at Hamming distance at least  $n(1 - 10^{-9})$ . We set

$$\mathbf{x}_0^\pm = (\mathbf{x}_1^\pm - \mathbf{x}_2^\pm)/2.$$

The vector  $\mathbf{x}_0^\pm$  is a  $\pm 1$ -vector except for at most  $10^{-9}n$  coordinates where it is zero. Finally, for  $i = 1, \dots, n$ ,

$$|\chi_{\mathbf{x}_0^\pm}(\mathbf{c}_i)| = |(\chi_{\mathbf{x}_1^\pm}(\mathbf{c}_i) - \chi_{\mathbf{x}_2^\pm}(\mathbf{c}_i))/2| \leq 10\sqrt{n}$$

as was claimed.  $\square$

For the final transformation of  $\mathbf{x}_0^\pm$  to a  $\pm 1$ -vector, we have to substitute (at most)  $10^{-9}n$  zero coordinates by suitable  $\pm 1$ 's. This is achieved by iterating the procedure of the previous lemma. In fact, we get the following result.

**Lemma 12.5.8** *Let  $C'$  be an  $(r, n)$  code with  $r \leq 10^{-9}n$ ; then there exists a vector  $\mathbf{x}^\pm \in \{\pm 1, 0\}^r$ , having at most  $10^{-40}r$  0's and*

$$\text{disc}(C, \mathbf{x}^\pm) \leq 10\sqrt{r} \sqrt{\ln(n/r)}.$$

**Proof.** Same as in the previous lemma. We omit the details.  $\square$

**Proof of Theorem 12.5.6** Apply Lemma 12.5.7 to find  $\mathbf{x}^\pm(1)$ , and apply Lemma 12.5.8 repeatedly to obtain  $\mathbf{x}^\pm(2), \mathbf{x}^\pm(3), \dots$ . Substituting  $\mathbf{x}^\pm(2)$  on the zero positions of  $\mathbf{x}^\pm(1)$ , etc., we get a vector  $\mathbf{x}^\pm \in \{\pm 1\}^n$ , providing

$$\begin{aligned} \text{disc}(C, \mathbf{x}^\pm) &\leq 10\sqrt{n} + 10\sqrt{10^{-9}n} \sqrt{\ln 10^9} \\ &\quad + 10\sqrt{10^{-49}n} \sqrt{\ln 10^{49}} + \dots \leq 11\sqrt{n}. \end{aligned}$$

Clearly, 11 is not the best achievable constant.  $\square$

**Theorem 12.5.9** *For all  $(n, K)R$  codes with  $n < K$ ,*

$$R \geq n/2 - a \sqrt{n \ln(K/n)},$$

where  $a$  is positive and does not depend on  $n$ .

**Proof.** Follows from iterative application of Lemma 12.5.8 (if  $n > 10^{-9}K$ , apply Lemma 12.5.7 first).  $\square$

As long as  $K = n^{1+o(1)}$ , this is better than the sphere-covering bound.

A more involved technique is based on notions of linear and hereditary discrepancy. We omit details and state only the main result.

**Theorem 12.5.10** *For all  $(n, K)R$  codes,*

$$R \geq n/2 - 12\sqrt{K}.$$

$\square$

The last theorem provides best results for  $K = o(n)$ .

## 12.6 Bounds on the minimum distance

We consider here asymptotic bounds on the minimum distance for codes of a given size. These results are used in the next sections to obtain bounds on covering radius. We consider families of growing length  $n$ , and are interested in the situation when the minimum distance grows linearly in  $n$ . We use the notation  $f(n) \lesssim g(n)$  for  $f(n) \leq g(n)(1+o(1))$  as  $n$  tends to infinity. We start with a lower bound.

**Theorem 12.6.1 (Gilbert-Varshamov bound)** *Let  $0 \leq \delta < 1/2$ . There exists an infinite sequence of  $[n, k, d]$  codes  $C_n$  with  $d/n \rightarrow \delta$  and rate*

$$\kappa(C_n) \gtrsim 1 - H(\delta). \quad (12.6.2)$$

**Proof.** Assume that the minimum distance is  $d$ . We construct a parity check matrix  $\mathbf{H}$  having  $n - k$  rows, column by column. The condition on the minimum distance means that no  $d - 1$  columns of  $\mathbf{H}$  are linearly dependent (see Theorem 2.1.8). Assume we have already chosen  $i$  columns. There are  $V(i, d - 2) - 1$  distinct linear combinations of at least 1 and at most  $d - 2$  columns picked among these  $i$  columns. If  $V(i, d - 2) - 1 < 2^{n-k} - 1$ , then there exists at least one nonzero column we can append to  $\mathbf{H}$  while preserving the minimum distance. This means that, provided  $V(n - 1, d - 2) < 2^{n-k}$ , there exists a linear  $[n, k, d]$  code. The asymptotic expression follows from (2.4.5).  $\square$

Arguments similar to those in the first half of the proof of Theorem 12.3.5 allow proving that (12.6.2) holds for virtually all linear codes.

Now we consider upper bounds. The Hamming bound (Lemma 8.1.19) takes the following asymptotic form.

**Theorem 12.6.3 (Hamming bound)** *For any  $(n, K, d)$  code  $C$ ,*

$$\kappa(C) \lesssim 1 - H(\delta(C)/2).$$

□

The next one is the Plotkin bound.

**Theorem 12.6.4 (Plotkin bound)** *For any  $(n, K, d)$  code  $C$  with  $n < 2d$ ,*

$$\delta(C) \leq \begin{cases} \frac{K}{2(K-1)} & \text{if } K \text{ is even,} \\ \frac{K+1}{2K} & \text{if } K \text{ is odd.} \end{cases}$$

**Proof.** Let us represent  $C$  as a  $K \times n$  matrix whose rows are the codewords. Now, we calculate the sum

$$S = \sum_{\mathbf{u} \in C} \sum_{\mathbf{v} \in C} d(\mathbf{u}, \mathbf{v})$$

in two ways, by rows and by columns. First, since for  $\mathbf{u} \neq \mathbf{v}$  we have  $d(\mathbf{u}, \mathbf{v}) \geq d$ ,  $S \geq K(K-1)d$ . On the other hand, if the number of zeros in the  $i$ -th column is  $x_i$ , then it contributes  $2x_i(K-x_i)$  to the sum. The total impact of the  $n$  columns is therefore

$$\sum_{i=1}^n 2x_i(K-x_i). \quad (12.6.5)$$

This expression is maximized for  $K$  even if all  $x_i = K/2$ , and the sum is at most  $nK^2/2$ . Thus, for  $K$  even,

$$K(K-1)d \leq nK^2/2,$$

and the claim for even  $K$  follows.

For  $K$  odd the sum is maximized if all  $x_i = (K-1)/2$  (or  $(K+1)/2$ ), and the sum is at most  $n(K^2-1)/2$ . Thus, for  $K$  odd,

$$K(K-1)d \leq n(K^2-1)/2,$$

and the claim for odd  $K$  follows. □

We can relate the maximum rate of a code to the maximum rate of a constant weight code. Recall that  $A(n, d, w)$  denotes the largest cardinality of a  $w$  constant weight code with length  $n$  and minimum distance  $d$ .

**Lemma 12.6.6 (Bassalygo-Elias lemma)** *For every  $(n, K, d)$  code  $C$ ,*

$$K \leq \frac{2^n A(n, d, w)}{\binom{n}{w}}. \quad (12.6.7)$$

**Proof.** Consider the  $2^n$  translates  $C + \mathbf{x}$ , corresponding to all possible choices of  $\mathbf{x}$ . Every  $n$ -tuple occurs exactly  $K$  times in the translates. So, there is a translate containing at least the average number  $K \binom{n}{w} 2^{-n}$  of vectors of weight  $w$ . The distance between vectors belonging to the same translate is at least  $d$ . The size of this constant weight code is at most  $A(n, d, w)$ .  $\square$

So, we need some estimates for the function  $A(n, d, w)$ . We start with a simple bound based on induction. Notice that the distance between vectors of the same weight is always even.

**Lemma 12.6.8**

$$A(n, d, w) \leq \left\lfloor \frac{n}{w} \left\lfloor \frac{n-1}{w-1} \cdots \left\lfloor \frac{n-w+d/2}{d/2} \right\rfloor \cdots \right\rfloor \right\rfloor. \quad (12.6.9)$$

**Proof.** In a constant weight code of size  $K = A(n, d, w)$ , there is a coordinate containing at least  $Kw/n$  ones. Taking all the codewords with one in this coordinate and puncturing, we get a code of length  $n-1$ , minimum distance at least  $d$  and constant weight  $w-1$ . Such a code has at most  $A(n-1, d, w-1)$  codewords, and therefore  $A(n, d, w)w/n \leq A(n-1, d, w-1)$ , i.e.,  $A(n, d, w) \leq \lfloor nA(n-1, d, w-1)/w \rfloor$ . The claim follows by induction, using the fact that  $A(n-w+d/2, d, d/2) = \lfloor \frac{n-w+d/2}{d/2} \rfloor$ .  $\square$

An argument similar to the proof of the Plotkin bound gives the next result.

**Theorem 12.6.10 (Johnson bound)**

$$A(n, d, w) \leq \left\lfloor \frac{dn}{2w^2 - 2wn + dn} \right\rfloor,$$

provided that the denominator is positive.

**Proof.** We proceed exactly like in the proof of Theorem 12.6.4. The restriction on the weights of the codewords yields that  $x_i = wK/n$  maximizes (12.6.5). Straightforward calculations end the proof.  $\square$

**Theorem 12.6.11 (Elias bound)** For any  $(n, K, d)$  code  $C$  with  $\delta(C) \leq 1/2$ ,

$$\kappa(C) \lesssim 1 - H \left( \frac{1}{2} - \frac{1}{2} \sqrt{1 - 2\delta(C)} \right). \quad (12.6.12)$$

**Proof.** For

$$w = \left\lfloor \frac{n}{2} - \frac{n}{2} \sqrt{1 - \frac{2(d-2)}{n}} \right\rfloor, \quad (12.6.13)$$

the Johnson bound gives  $A(n, d, w) \leq d/2$ . Substituting this value into (12.6.7) and passing to asymptotic values we get the claim.  $\square$

Now we consider the most powerful technique known, based on linear programming.

**Lemma 12.6.14** Let

$$\alpha(x) = \sum_{i=0}^n \alpha_i P_i(x)$$

be a polynomial such that

- $\alpha_0 > 0$ ,  $\alpha_i \geq 0$  for  $i \in [1, n]$ ;
- $\alpha(j) \leq 0$  for  $j \in [d, n]$ .

Then for any  $(n, K, d)$  code,

$$K \leq \frac{\alpha(0)}{\alpha_0}.$$

**Proof.** We have by Theorem 2.2.3

$$\mathcal{B}_i^\perp = \frac{1}{K} \sum_{j=0}^n \mathcal{B}_j P_i(j),$$

where the  $\mathcal{B}_i^\perp$ 's are nonnegative by Theorem 2.2.7 and  $\mathcal{B}_0^\perp = 1$ . Then

$$\begin{aligned} \alpha_0 &\leq \sum_{i=0}^n \alpha_i \mathcal{B}_i^\perp = \frac{1}{K} \sum_{i=0}^n \alpha_i \sum_{j=0}^n \mathcal{B}_j P_i(j) \\ &= \frac{1}{K} \sum_{j=0}^n \mathcal{B}_j \sum_{i=0}^n \alpha_i P_i(j) = \frac{1}{K} \sum_{j=0}^n \mathcal{B}_j \alpha(j) \leq \frac{\alpha(0)}{K}, \end{aligned}$$

giving the claim.  $\square$

**Theorem 12.6.15 (McEliece-Rodemich-Rumsey-Welch bound)** *For any  $(n, K, d)$  code  $C$ ,*

$$\kappa(C) \lesssim H \left( \frac{1}{2} - \sqrt{\delta(C)(1 - \delta(C))} \right).$$

**Proof.** Follows from a special choice of the polynomial in Lemma 12.6.14. We omit the details.  $\square$

The previous bound can be further improved for  $\delta(C) \leq 0.273$ .

**Theorem 12.6.16** *For any  $(n, K, d)$  code  $C$ ,*

$$\kappa(C) \lesssim f(\delta(C)),$$

where

$$f(\delta) = \min_{0 < \omega \leq 1-2\delta} f(\omega, \delta),$$

and

$$f(\omega, \delta) = 1 + h(\omega^2) - h(\omega^2 + 2\delta\omega + 2\delta),$$

$$h(x) = H \left( \frac{1}{2} - \frac{1}{2} \sqrt{1-x} \right).$$

**Proof.** Use the Bassalygo-Elias lemma along with a linear programming bound for constant weight codes. We omit the details.  $\square$

## 12.7 Covering radius as a function of dual distance

The problem of upperbounding the covering radius when the dual distance is known has been discussed in detail in Section 8.3. Here we derive asymptotic bounds for the normalized covering radius  $\rho$  as a function of the normalized dual distance  $\delta^\perp$ .

Let  $\mathcal{C}$  be a sequence of codes  $C_n$  of length  $n$ , dual distance  $d^\perp$  and covering radius  $R$ , where  $R/n \rightarrow \rho$  and  $d^\perp/n \rightarrow \delta^\perp$  when  $n \rightarrow \infty$ .

We start with a lower bound.

**Theorem 12.7.1** *There exist infinite sequences  $\mathcal{C}$  such that, for  $0 < \delta^\perp < \frac{1}{2}$ ,*

$$\rho \geq H^{-1}(1 - H(\delta^\perp)). \quad (12.7.2)$$

**Proof.** The covering radius of duals of codes which satisfy the Gilbert-Varshamov bound verify the claimed lower bound, by the sphere-covering bound.  $\square$

Now we proceed to upper bounds. Assume that  $\delta^\perp n/2$  is an integer (otherwise, use the floor function). By Theorem 8.3.11,  $R$  is upperbounded by  $x_{1,n}(\delta^\perp n/2)$ , the smallest zero of the Krawtchouk polynomial of degree  $\delta^\perp n/2$  (notice that  $x_{1,n}(\delta^\perp n/2) > x_{1,n-1}(\delta^\perp n/2)$ ). Asymptotically,

$$\lim_{n \rightarrow \infty} \frac{x_{1,n}(\delta^\perp n/2)}{n} = \frac{1}{2} - \frac{1}{2} \sqrt{\delta^\perp(2 - \delta^\perp)}.$$

This gives the following statement.

**Theorem 12.7.3**

$$\rho \leq \frac{1}{2} \left( 1 - \sqrt{\delta^\perp(2 - \delta^\perp)} \right). \quad (12.7.4)$$

$\square$

Now we consider linear codes and present an alternative proof of a part of Theorem 8.3.5, based on exponential sums.

Assume that  $C$  is a binary linear  $[n, k, d \geq 3]R$  code, with dual distance  $d^\perp$ . Let the  $(n - k) \times n$  matrix  $\mathbf{H} = (\mathbf{h}_1, \dots, \mathbf{h}_n)$  be a parity check matrix for  $C$ , and denote the set  $\{\mathbf{h}_1, \dots, \mathbf{h}_n\}$  by  $L$ . Let  $N(L, s, \mathbf{b})$  be the number of solutions  $(\mathbf{x}_1, \dots, \mathbf{x}_s) \in L^s$  of the equation

$$\mathbf{x}_1 + \dots + \mathbf{x}_s = \mathbf{b}. \quad (12.7.5)$$

Recall that  $R$  is the smallest integer  $r$  such that every syndrome of  $C$  is the sum of at most  $r$  columns of  $\mathbf{H}$ . Hence  $R \leq r$  if, for every  $\mathbf{b} \in \mathbb{F}^{n-k}$ , there is a polynomial

$$\gamma(x) = \sum_{s=0}^r \gamma_s x^s$$

such that

$$\sum_{s=0}^r \gamma_s N(L, s, \mathbf{b}) > 0.$$

(In fact, the sum does not have to be positive, as long as it is nonzero.)

We have seen in Section 2.2 that, for all  $\mathbf{k} \in \mathbb{F}^{n-k}$ , the mapping  $\psi_{\mathbf{k}}$  defined by

$$\psi_{\mathbf{k}}(\mathbf{a}) = (-1)^{\langle \mathbf{k}, \mathbf{a} \rangle} \text{ for all } \mathbf{a} \in \mathbb{F}^{n-k}$$

is an additive character of  $\mathbb{F}^{n-k}$ . The characters  $\psi_k$  form the dual group of  $\mathbb{F}^{n-k}$ ; thus

$$\sum_{k \in \mathbb{F}^{n-k}} (-1)^{\langle k, a \rangle} = \begin{cases} 2^{n-k} & \text{if } a = 0 \\ 0 & \text{otherwise,} \end{cases}$$

and

$$\begin{aligned} 2^{n-k} N(L, s, b) &= \sum_{x_1 \in L} \dots \sum_{x_s \in L} \sum_{k \in \mathbb{F}^{n-k}} (-1)^{\langle k, x_1 + \dots + x_s + b \rangle} \\ &= \sum_{k \in \mathbb{F}^{n-k}} (-1)^{\langle k, b \rangle} \sum_{x_1 \in L} (-1)^{\langle k, x_1 \rangle} \dots \sum_{x_s \in L} (-1)^{\langle k, x_s \rangle} \\ &= \sum_{k \in \mathbb{F}^{n-k}} (-1)^{\langle k, b \rangle} \left( \sum_{x \in L} (-1)^{\langle k, x \rangle} \right)^s. \end{aligned}$$

Furthermore,

$$\sum_{x \in L} (-1)^{\langle k, x \rangle} = n - 2w(\mathbf{H}k^T).$$

When  $k$  runs through  $\mathbb{F}^{n-k}$ ,  $\mathbf{H}k^T$  runs through all elements of the dual  $C^\perp$  of  $C$ . Therefore,

$$2^{n-k} N(L, s, b) = \sum_{i=0}^n \beta_i(b) (n-2i)^s$$

where

$$\beta_i(b) = \sum_{k: w(\mathbf{H}k^T) = i} (-1)^{\langle k, b \rangle}. \quad (12.7.6)$$

In particular,  $|\beta_i(b)| \leq \mathcal{B}_i^\perp$ , where  $\mathcal{B}_i^\perp$  is the number of words of weight  $i$  in  $C^\perp$ . Hence

$$2^{n-k} \sum_{s=0}^r \gamma_s N(L, s, b) = \sum_{i=0}^n \beta_i(b) \sum_{s=0}^r \gamma_s (n-2i)^s = \sum_{i=0}^n \beta_i(b) \alpha(i)$$

where  $\alpha(i) = \gamma(n-2i)$ . Since  $\beta_0(b) = 1$ , we obtain the following theorem.

**Theorem 12.7.7** *Assume that for each  $b \in \mathbb{F}^{n-k}$  there is a polynomial  $\alpha(x)$  of degree at most  $r$  such that*

$$\alpha(0) + \sum_{i=1}^n \beta_i(b) \alpha(i) > 0,$$

*where  $\beta_i(b)$  is defined by (12.7.6). Then  $R \leq r$ .*

□

We now search for a polynomial  $\alpha(x)$  of a low degree such that  $|\alpha(i)|$  is small compared to  $\alpha(0)$  whenever  $i \neq 0$  and  $\beta_i(\mathbf{b}) \neq 0$ . To that end, consider the *Chebyshev polynomial* of degree  $r$  of the first kind, defined by

$$T_r(x) = \frac{1}{2} \left( \left( x + \sqrt{x^2 - 1} \right)^r + \left( x - \sqrt{x^2 - 1} \right)^r \right).$$

Let  $0 \leq a < b$ . Among the polynomials  $p_r(x)$  of degree at most  $r$  such that  $p_r(0) = 1$ , the one defined by

$$t_r(x) = \frac{T_r\left(\frac{b+a-2x}{b-a}\right)}{T_r\left(\frac{b+a}{b-a}\right)}$$

minimizes  $\max_{x \in [a, b]} |p_r(x)|$ . Moreover,

$$\max_{x \in [a, b]} |t_r(x)| = \frac{1}{T_r\left(\frac{b+a}{b-a}\right)}.$$

Trivially, for all  $x \geq 1$ ,

$$\frac{1}{2} \left( x + \sqrt{x^2 - 1} \right)^r \leq T_r(x) \leq \frac{1}{2} \left( \left( x + \sqrt{x^2 - 1} \right)^r + 1 \right). \quad (12.7.8)$$

Choose  $\alpha(x) = t_r(x)$  with  $a = d^\perp$  and  $b = n(1 - \lambda')$ , where

$$\lambda' < \lambda := \frac{1}{2} - \sqrt{\frac{1}{2} \left( \frac{1}{2} - \delta^\perp \right)}$$

is an arbitrary positive number smaller than the Elias range  $\lambda$ : the *Elias range*, a function of  $n$  and  $d$ , is the maximum radius of a Hamming ball such that any code with minimum distance  $d$  has a subexponential in  $n$  number of words inside this ball. Its expression can be easily obtained from the Johnson bound, see (12.6.13). Then  $\lambda'^2 - \lambda' + \frac{1}{2}\delta^\perp > 0$  and

$$\sum_{i \geq (1 - \lambda')n} \mathcal{B}_i^\perp \lesssim \frac{\frac{1}{2}\delta^\perp}{\lambda'^2 - \lambda' + \frac{1}{2}\delta^\perp}$$

when  $n \rightarrow \infty$ .

Furthermore,  $1 < \delta^\perp + 1 - \lambda'$ , and therefore using (12.7.8) we obtain

$$\sum_{(1 - \lambda')n \leq i \leq n} \mathcal{B}_i^\perp |t_r(i)| \rightarrow 0$$

when  $n \rightarrow \infty$  and  $r \rightarrow \infty$ .

Thus

$$\alpha(0) + \sum_{i=1}^n \beta_i(\mathbf{b}) \alpha(i) > 1 - \frac{2^{n-k}}{T_r\left(\frac{b+a}{b-a}\right)} + o(1),$$

and so Theorem 12.7.7 implies that  $R \leq r$  if

$$2^{n-k+1} \leq T_r \left( \frac{b+a}{b-a} \right).$$

By the McEliece-Rodemich-Rumsey-Welch bound,

$$\frac{n-k}{n} \lesssim H\left(\frac{1}{2} - \sqrt{\delta^\perp(1-\delta^\perp)}\right)$$

when  $n \rightarrow \infty$ , and we obtain the asymptotic upper bound

$$\rho \leq \frac{H\left(\frac{1}{2} - \sqrt{\delta^\perp(1-\delta^\perp)}\right)}{\log_2\left(\frac{1-\lambda'+\delta^\perp+2\sqrt{\delta^\perp(1-\lambda')}}{1-\lambda'-\delta^\perp}\right)}.$$

Since this is true for all  $\lambda' < \lambda$ , we obtain the following result.

**Theorem 12.7.9** *Let  $(C_n)_{n=1}^\infty$  be an infinite sequence of binary linear codes  $C_n$  of length  $n$ , dual distance  $d^\perp$  and covering radius  $R$ , where  $R/n \rightarrow \rho$  and  $d^\perp/n \rightarrow \delta^\perp$  when  $n \rightarrow \infty$ . Then*

$$\rho \leq \frac{H\left(\frac{1}{2} - \sqrt{\delta^\perp(1-\delta^\perp)}\right)}{\log_2\left(\frac{1-\lambda+\delta^\perp+2\sqrt{\delta^\perp(1-\lambda)}}{1-\lambda-\delta^\perp}\right)},$$

where  $\lambda = \frac{1}{2} - \sqrt{\frac{1}{2}\left(\frac{1}{2} - \delta^\perp\right)}$ . □

Comparing the bounds of Theorems 12.7.3 and 12.7.9, we see that the first one is better when  $\delta^\perp \in [0, 0.279]$ .

## 12.8 Packing radius vs covering radius

In this section we study relations between minimum distance and covering radius. Many numerical examples for short lengths show that usually good error-correcting codes are not very good coverings, and vice versa, good coverings quite often turn out to be bad for error correction. Here, we are interested in achievable pairs of normalized (with respect to length) minimum distance and covering radius for codes of growing length, irrespectively of their size.

Let us state the problem rigorously. Let  $\mathcal{C}$  denote an infinite family of binary codes with length  $n$ , covering radius  $R$  and minimum distance  $d$ . Assume further that the limits  $\rho$  and  $\delta$  for the ratios  $R/n$  and  $d/n$  exist. Our

aim is to study the set  $Y$  (respectively,  $Y_{lin}$ ) of possible values  $(\rho, \delta)$  for unrestricted (respectively, linear) codes. We reduce the problem to codes having two, three, four and infinitely many codewords. We start with results for a small number of codewords.

**Lemma 12.8.1**

$$\delta \leq 2/3 \text{ for } K \geq 3, \quad \delta \leq 3/5 \text{ for } K \geq 5.$$

**Proof.** Follows from Theorem 12.6.4.  $\square$

The following lemma allows discarding codes with “constant” coordinates (where all the codewords take on the same value, zero or one).

**Lemma 12.8.2** *Let  $(x, y) \in Y_{lin}$  (respectively,  $\in Y$ ). Then every point of the line between  $(x, y)$  and  $(1, 0)$  lies in  $Y_{lin}$  (respectively,  $Y$ ).*

**Proof.** Let  $C$  be an  $[n, k, d]R$  code with  $R/n = x$  and  $d/n = y$ . Append  $s = zn$  zeros to all codewords. The resulting code is an  $[n+s, k, d]R+s$  code  $C'$ . For this code,  $x' = (R+s)/(n+s) = (x+z)/(1+z)$  and  $y' = y/(1+z)$ . Now note that  $z$  may be chosen in  $[0, \infty)$  and

$$(1 - x')/y' = (1 - x)/y,$$

so all possible  $(x', y')$  are on the line from  $(x, y)$  to  $(1, 0)$ . For the nonlinear case the proof is the same.  $\square$

Thus, from now on, we consider only codes without constant coordinates.

**Two words:** Trivially,  $(\rho = 0.5, \delta = 1)$  belongs to  $Y$  and  $Y_{lin}$ . From Lemma 12.8.2, we thus have the following result.

**Lemma 12.8.3** *For  $\rho \in [0.5, 1]$ , the line  $\delta = 2(1 - \rho)$  belongs to  $Y$  and  $Y_{lin}$ .*  $\square$

**Three words:** By the Plotkin bound, such codes have  $\delta \leq 2/3$ . Let an  $(n, 3, d)R$  code  $C$  consist of the words  $\mathbf{0}$ ,  $\mathbf{x}$  and  $\mathbf{y}$ . Let  $\mathbf{z} = \mathbf{x} + \mathbf{y}$ . Then

$$d(\mathbf{z}, \mathbf{0}) = w(\mathbf{z}) = d(\mathbf{x}, \mathbf{y}) \geq d,$$

$$d(\mathbf{z}, \mathbf{x}) = w(\mathbf{y}) \geq d,$$

$$d(\mathbf{z}, \mathbf{y}) = w(\mathbf{x}) \geq d.$$

Thus, the covering radius  $R$  of the code is at least  $d$ . So, for three-word codes, we always have  $\rho \geq \delta$ .

Now we construct codes with  $\rho = \delta$ , when  $\delta \geq 1/2$ . Let  $w(\mathbf{x}) = w(\mathbf{y}) = d \geq n/2$ . By symmetry, any deep hole  $\mathbf{z}$  has an equal number of ones on the positions of  $\mathbf{x} \setminus (\mathbf{x} \cap \mathbf{y})$  and  $\mathbf{y} \setminus (\mathbf{x} \cap \mathbf{y})$  (here we identify vectors with their supports). Denote by  $z_1$  the weight of  $\mathbf{z}$  on these positions, and by  $z_2$  the weight of  $\mathbf{z}$  on the positions where  $\mathbf{x}$  and  $\mathbf{y}$  intersect. Then

$$R = d(\mathbf{z}, C) \leq d(\mathbf{z}, \mathbf{x}) = d - z_1 - z_2 + z_1 = d - z_2,$$

i.e., in this case  $\delta \geq \rho$ , and we conclude that  $\delta = \rho$ . Summarizing,

**Lemma 12.8.4** *There exist (three-word) codes satisfying  $\delta = \rho$  for  $1/2 \leq \delta \leq 2/3$ .*  $\square$

**Four words (linear case):** Let  $C$  be a linear  $[n, 2, d]R$  code consisting of  $\mathbf{0}$ ,  $\mathbf{x}$ ,  $\mathbf{y}$  and  $\mathbf{x} + \mathbf{y}$ . Assume that both  $n$  and  $d$  are even,  $n/2 \leq d = w(\mathbf{x}) = w(\mathbf{y})$ . Then, on the one hand there exist vectors at distance exactly  $n/2$  from all the codewords: any vector containing half ones and half zeros on  $\mathbf{x} \cap \mathbf{y}$ ,  $\mathbf{x} \setminus (\mathbf{x} \cap \mathbf{y})$ , and  $\mathbf{y} \setminus (\mathbf{x} \cap \mathbf{y})$ . On the other hand, by the Norse bound (Theorem 8.3.13), a linear code with no constant (zero) coordinate has covering radius at most  $n/2$ .

**Lemma 12.8.5** *There exist linear codes satisfying  $\rho = 1/2$  for  $1/2 \leq \delta \leq 2/3$ .*  $\square$

**Four words (general case):** Assume that  $C$  is an  $(n, 4, d)R$  code and no coordinate is a constant. If we denote by  $f$  the number of coordinates where exactly two of the codewords have 1, then the sum of the six pairwise distances between the codewords is  $4f + 3(n - f)$ , and so  $4f + 3(n - f) \geq 6d$ , i.e.,  $f \geq 6d - 3n$ . On the other hand, the sum of the four distances between an arbitrary vector and the codewords is at most  $2f + 3(n - f) = 3n - f \leq 6n - 6d$ , and hence at least one of these distances is at most  $3(n - d)/2$ , and  $R \leq 3(n - d)/2$ , i.e.,  $\delta \leq 1 - 2\rho/3$ .

For  $1/2 \leq \delta \leq 2/3$ , assuming that  $n$  and  $d$  are even, this bound is achieved by the code consisting of the four words

$$\begin{aligned} &1^x 1^x 1^x 0^x 0^x 0^y 1^y 1^y 1^y \\ &1^x 0^x 0^x 1^x 1^x 0^x 1^y 0^y 1^y 1^y \\ &0^x 1^x 0^x 1^x 0^x 1^x 1^y 1^y 0^y 1^y \\ &0^x 0^x 1^x 0^x 1^x 1^x 1^y 1^y 1^y 0^y \end{aligned}$$

where  $x = (2d - n)/2$  and  $y = (2n - 3d)/2$ . Each codeword has length  $6x + 4y = n$  and weight  $3x + 3y = 3(n - d)/2$ . The all-zero word has distance  $3(n - d)/2$  to the code, and by the previous discussion the covering radius is equal to  $3(n - d)/2$ . Moreover, all pairwise distances between codewords equal  $4x + 2y = d$ .

**Lemma 12.8.6** *There exist nonlinear (four-word) codes for  $1/2 \leq \delta \leq 2/3$ , with  $\delta = 1 - 2\rho/3$ .*  $\square$

**Infinite number of codewords:** In this case we know (see Sections 12.3 and 12.6) that virtually all linear codes of rate  $\kappa$  have  $\rho = H^{-1}(1 - \kappa)$ ,  $\delta = H^{-1}(1 - \kappa)$ . This gives the following

**Lemma 12.8.7** *There exist linear codes with  $\delta = \rho$  for  $\rho \in [0, 0.5]$ .*  $\square$

Now, we pass to nonexistence results.

**Lemma 12.8.8** *For any  $(n, K, d)R$  code with  $K \geq 2$ , we have  $\delta \leq 2(1 - \rho)$ .*

**Proof.** The inequality is true for two codewords. Adding extra codewords can only decrease  $d$  and  $R$ .  $\square$

This lemma, along with the results on two-, three- and four-word codes, gives a complete characterization of  $Y$  for  $\rho \in [0.5, 1]$ . Notice that there is no need to consider codes of size more than four in this range. Indeed, our knowledge about  $Y$  and  $Y_{lin}$  for  $\rho \geq 1/2$ ,  $\delta \leq 3/5$ , is complete, but codes with five or more words (by Lemma 12.8.1) have  $\delta \leq 3/5$ .

**Lemma 12.8.9** *For any  $[n, k, d]R$  linear code with  $k \geq 2$ ,*

$$\delta \leq 4(1 - \rho)/3.$$

**Proof.** It is a particular case of Theorem 8.1.13. We have

$$R \leq n - \sum_{i=1}^k \lceil d/2^i \rceil \leq n - \lceil d/2 \rceil - \lceil d/4 \rceil,$$

and the claim follows.  $\square$

The two previous lemmas, along with the results on two- and four-word linear codes, give a complete characterization of possible pairs  $(\rho, \delta)$  for  $\rho \in [0.5, 1]$ .

**Lemma 12.8.10** *Let  $\mu(\delta)$  be an invertible function yielding an upper bound on the rate  $\kappa$  of the code as a function of the normalized minimum distance  $\delta$ . Then*

$$\delta \leq \mu^{-1}(1 - H(\rho)).$$

**Proof.** By the sphere-covering bound,

$$\rho \geq H^{-1}(1 - \log_2 K/n) \geq H^{-1}(1 - \mu(\delta)).$$

□

**Corollary 12.8.11** *For  $\rho \in [0, 0.5]$ ,  $\delta \leq 2\rho(1 - \rho)$ .*

**Proof.** Use in the previous lemma the Elias upper bound (12.6.12). □

A better result (but not as explicit) is given by using the linear programming bounds.

We summarize the results in the following two theorems.

**Theorem 12.8.12**  $Y_{lin}$  consists of

(i) line

$$\delta = 2(1 - \rho), \text{ for } \rho \in [0.5, 1] \text{ (two words);}$$

(ii) area under lines

$$\delta = \rho, \text{ for } \rho \in [0, 0.5] \text{ (infinite number of words),}$$

$$\delta = 4(1 - \rho)/3, \text{ for } \rho \in [0.5, 1] \text{ (four words).}$$

$Y_{lin}$  is empty elsewhere but, maybe, in the area

$$\rho \leq \delta \leq \mu^{-1}(1 - H(\rho)), \text{ for } \rho \in [0, 0.5],$$

where  $\mu(\delta)$  is an upper bound on the rate of a linear code as a function of  $\delta$ . □

**Theorem 12.8.13**  $Y$  consists of

(i) line

$$\delta = 2(1 - \rho), \text{ for } \rho \in [0.5, 2/3] \text{ (two words);}$$

(ii) area under lines

$$\delta = \rho, \text{ for } \rho \in [0, 0.5] \text{ (infinite number of words),}$$

$$\delta = 1 - 2\rho/3, \text{ for } \rho \in [0.5, 0.6] \text{ (four words),}$$

$$\begin{aligned}\delta &= \rho, \text{ for } \rho \in [0.6, 2/3] \text{ (three words),} \\ \delta &= 2(1 - \rho), \text{ for } \rho \in [2/3, 1] \text{ (two words).}\end{aligned}$$

$Y$  is empty elsewhere but, maybe, in the area

$$\rho \leq \delta \leq \mu^{-1}(1 - H(\rho)), \text{ for } \rho \in [0, 0.5],$$

where  $\mu(\delta)$  is an upper bound on the rate of an unrestricted code as a function of  $\delta$ .  $\square$

## 12.9 Notes

§12.1 Theorems 12.1.2, 12.1.3 and 12.1.4 are from Delsarte and Piret [196].

§12.2 Theorem 12.2.1 was independently discovered by Stein [621], D. S. Johnson [352] and Lovász [457]; we follow the proof of Stein. For an application to coverings see Cohen and Frankl [151].

The greedy method gives a semi-constructive proof of some basic relations in rate-distortion theory, see Cohen, Litsyn and Zémor [164]. For rate-distortion theory in a general setting, see Berger [67]. Information-theoretic variations on this theme can be found in Csiszár and Körner [177, Ch. 4]. For a generalization of coverings to hypergraphs, see Ahlswede [9]. For more uses of the greedy algorithm, see Sections 17.5, 18.5, 18.6 and 20.3.

§12.3 Theorems 12.3.2 and 12.3.4 are from Cohen [143]. A similar result appeared earlier in an unpublished thesis by Goblick [251]. For a nonbinary version, see Cohen and Frankl [151]. For some time it was not known if the sphere-covering bound is asymptotically achieved by almost all linear codes, see the discussion in Delsarte and Piret [196]. This was solved by Blinovskii, see Theorem 12.3.5 (proved in [87] for  $\mathbb{F}_q$ ) and Theorem 12.3.10 [88]. Blinovskii also generalized the results to coverings by translations of an arbitrary body [89]. The idea of applying Theorem 12.3.10 to constructing good infinite families of coverings is due to Roth (private communication).

§12.4 Theorem 12.4.3 is by Cohen, Lobstein and Sloane [165]. The same result holds when  $q$  is not a prime power. To prove this, just use the fact that Hamming codes and their lengthenings constitute, for alphabet sizes being prime numbers, a family of optimal linear coverings, and Theorem 3.7.8 enabling constructions over composite alphabets. See [165] for details. Wyner and Ziv [695] obtained a weaker  $\mu(n, R) = o(p^n)$  for prime alphabet sizes and fixed  $R$ . The greedy algorithm guarantees  $\mu(n, R) = O(\ln n)$ . Beveraggi and Cohen [77] provided estimates for  $\mu^*(1)$ . The cascading construction (covering by coverings) was discovered by Kamps and van Lint [362] and generalized

by Blokhuis and Lam [90]. Lemma 12.4.8 and Theorem 12.4.11 are due to Kabatyanskii and Panchenko [355]; for a sequence of increasing lengths, they upperbound  $\mu(n, 1)$  by

$$\mu(n, 1) \leq 1 + O(\ln \ln n / \ln n).$$

It is also shown in [355] that  $\mu^*(1) = 1$  for all alphabets of size equal to a prime power. Panchenko in [530] derived sufficient conditions ensuring  $\mu^*(1) = 1$  in the case of arbitrary alphabets. It is tempting to conjecture that  $\mu^*(R) = 1$  for every fixed  $R$ , i.e., that the best  $R$ -coverings are asymptotically perfect. The problem looks very difficult. Defining  $\mu_*(R)$  (respectively,  $\mu_*[R]$ ) analogously to  $\mu^*(R)$  (respectively,  $\mu^*[R]$ ) but substituting  $\limsup$  by  $\liminf$ , one can estimate the density of the sparsest infinite families of codes. So far, the best known results in the linear case for radii 2, 3 and 4, are

$$\mu_*[2] \leq 1.4238\dots, \quad \mu_*(3) \leq \mu_*[3] \leq 1.3743\dots, \quad \mu_*(4) \leq \mu_*[4] \leq 2.3391\dots,$$

see (5.4.30), (5.4.31) and (5.4.32), which are due to Davydov [179], Davydov and Drozhzhina-Labinskaya [189]. Struik [630] exhibited an infinite subsequence of lengths for which  $\mu_*(2) = 1$  (cf. Theorem 4.5.8). The construction is based on the blockwise direct sum of Hamming codes partitioned into cosets of punctured Preparata codes (cf. Theorem 2.6.5) with short codes constructed by Gabidulin, Davydov and Tombak [245].

**§12.5** The relation between discrepancy and covering radius was first mentioned in Cohen, Karpovsky, Mattson and Schatz [156]. For Chernoff's inequality see, e.g., Gallager [246] or Alon and Spencer [20]. Theorem 12.5.6 is from Spencer [614], where it is claimed that the constant 5.32 can be further improved. Theorem 12.5.10 is by Lovász, Spencer and Vesztergombi [460]. For earlier results on the discrepancy of sets, see Olson and Spencer [510] and Beck and Fiala [62].

How tight are the bounds? First order Reed-Muller codes of length  $n = 2^m$  have  $K = 2n$  and  $R = n/2 - O(\sqrt{K})$ . The same result holds for codes derived from Hadamard matrices. This suggests that the bound of Theorem 12.5.6 cannot be essentially improved.

We are unaware of constructions achieving the lower bounds. Pach and Spencer [529] give a construction of coverings approaching the sphere-covering bound for low rates. In particular, they prove that given any  $\varepsilon > 0$ , there exists  $c_\varepsilon > 0$  such that for every sufficiently large  $n$  and  $n^\varepsilon < k < n$ , there exist  $[n, k]R$  codes with  $R \leq n/2 - c_\varepsilon \sqrt{nk}$ . See also Solé [601] for estimates of the covering radius of some low-rate codes.

There is an intimate relation between estimating the covering radius of a class of low-rate codes, namely codes being duals of product codes, and the following problem.

**Berlekamp-Gale switching game.** Consider an  $\ell \times m$  array of light bulbs, controlled by  $\ell + m$  switches, one for each row and column. When a switch is activated, all lights in the corresponding row or column that are off turn on, and vice versa. For each initial pattern  $S$  of lights, let  $f(S)$  be the minimum number of lights that are on after using switches in any way. The problem is to determine  $R_{\ell,m} = \max_S f(S)$ .

To translate the problem into the language of codes, consider a linear  $[\ell m, \ell + m - 1]$  code with codewords represented by  $\ell \times m$  rectangles. For generators of this code we choose all  $\ell \times m$  matrices having 0's everywhere but in a single column or in a single row, where it has all 1's. There are  $\ell + m$  such matrices, but their sum is zero, so the rank of their set is  $\ell + m - 1$ . Associating to the initial state  $S$  a matrix having 1's for the lights on, and 0's elsewhere, we notice that any pull of switch corresponds to adding a generator, i.e., leaves the vector in the same coset of the code. Thus  $f(S)$  is just the weight of the coset, and  $\max f(S)$  is the covering radius.

The function  $R_{\ell,m}$  has been especially studied for  $\ell = m$ . Fishburn and Sloane [238] give the following table of exact values of  $R_{m,m}$ :

$m$	1	2	3	4	5	6	7	8	9	10
$R_{m,m}$	0	1	2	4	7	11	16	22	27	34

The value  $R_{10,10}$  is of special interest because of the existence at Bell Labs in Murray Hill of a real game device constructed by Berlekamp.

The best asymptotic result known is

$$(1/2)m^2 - (1/2)m^{3/2} + o(m^{3/2}) \leq R_{m,m} \leq (1/2)m^2 - m^{3/2}/\sqrt{2\pi} + o(m^{3/2}).$$

For other results and generalizations see Alon and Spencer [20], Beck and Spencer [63], Brown and Spencer [98], Fishburn and Sloane [238], Y. Gordon and Witsenhausen [263], Graham and Sloane [265], Katsman [373], Mattson [471], Pach and Spencer [529].

§12.6 The Gilbert-Varshamov bound was derived in the nonlinear case by Gilbert [250] and by Varshamov [663] (in the linear situation). The Hamming bound was published by Hamming [279]. The Plotkin bound is from Plotkin [543]. A proof of the Bassalygo-Elias lemma can be found in Bassalygo [52]. Lemma 12.6.8 and Theorem 12.6.10 are by S. M. Johnson [353]. The linear programming method was developed by Delsarte [193]. The McEliece-Rodemich-Rumsey-Welch bound was published in [479]. A linear programming bound was obtained in the nonbinary case by Aaltonen [1], [2] and Levenshtein [417]. For further improvements see Aaltonen [3] and Laihonen and Litvin [407].

§12.7 The lower bound of Theorem 12.7.1 and the upper bound of Theorem 12.7.3 are by Tietäväinen [644], [646]. In the rest of the section we follow

Honkala, Litsyn and Tietäväinen [327], see also Litsyn and Tietäväinen [445] and Litsyn, Solé and Struik [444]. For earlier asymptotic bounds see Delorme and Solé [192], Solé and Mehrotra [605], Solé and Stokes [606]. Honkala, Laihonan and Litsyn [325] use discrete Chebyshev polynomials to improve on the bound of Theorem 12.7.9. The new bound is better than Tietäväinen's bound of Theorem 12.7.3 when  $\delta^\perp \geq 0.278$ .

**§12.8** We follow Cohen, Honkala, Litsyn and Solé [161]. In [624], Stokes studied possible pairs of rate and normalized covering radius.

# Chapter 13

## Weighted coverings

In this chapter we study a more general class of covering problems. Namely, we attach weights to different layers of the Hamming sphere and consider such weighted spheres centred at the codewords. If several such spheres intersect in a point, we define the density at that point as the sum of the weights of the corresponding layers. A code is called a *weighted covering* if the density at each point is at least one.

Many classes of codes can be viewed in a natural way as weighted coverings, e.g., nearly perfect codes, uniformly packed codes,  $L$ -codes. Two other classes, namely *multiple coverings* and *multiple coverings of deep holes*, are considered in Chapter 14. In Section 13.1 we also discuss how weighted coverings and weighted packings, which can be defined in an analogous way, are related. In Section 13.2 we prove the Lloyd theorem for weighted coverings and in Section 13.3 we study  $q$ -ary linear perfect weighted coverings. In Section 13.4 we use weighted coverings to derive lower bounds on the number of codewords in conventional coverings.

### 13.1 Basic notions

Let  $Q$  denote an arbitrary  $q$ -element alphabet. For any  $(n+1)$ -tuple  $\mathbf{m} = (m_0, m_1, \dots, m_n)$  of rational numbers, we define the  $\mathbf{m}$ -density of  $C \subseteq Q^n$  at  $\mathbf{x}$  as

$$\theta(\mathbf{x}) := \sum_{i=0}^n m_i \mathcal{A}_i(\mathbf{x}) = \langle \mathbf{m}, \mathcal{A}(\mathbf{x}) \rangle, \quad (13.1.1)$$

where  $\mathcal{A}(\mathbf{x})$  is the weight distribution of  $C$  with respect to  $\mathbf{x}$ , i.e.,  $\mathcal{A}(\mathbf{x}) = (\mathcal{A}_0(\mathbf{x}), \mathcal{A}_1(\mathbf{x}), \dots, \mathcal{A}_n(\mathbf{x}))$ .

**Definition 13.1.2** A code  $C \subseteq Q^n$  is an **m-covering** if

$$\theta(\mathbf{x}) \geq 1$$

for all  $\mathbf{x} \in Q^n$ . If  $\theta(\mathbf{x}) = 1$  for all  $\mathbf{x} \in Q^n$ , then  $C$  is a **perfect m-covering**.

In general, the objects in the previous definition are called *weighted coverings*. The *radius* of an **m-covering** is

$$r = r(\mathbf{m}) = \max\{i : m_i \neq 0\}.$$

If  $C \subseteq Q^n$  is an **m-covering**, then

$$\sum_{i=0}^r m_i \mathcal{A}_i(\mathbf{x}) \geq 1$$

for all  $\mathbf{x}$ . Summing over all  $\mathbf{x} \in Q^n$  and permuting sums, we get

$$\sum_{i=0}^r m_i \sum_{\mathbf{x} \in Q^n} \mathcal{A}_i(\mathbf{x}) \geq q^n,$$

and therefore

$$|C| \sum_{i=0}^r m_i \binom{n}{i} (q-1)^i \geq q^n, \quad (13.1.3)$$

which is the *sphere-covering bound* for weighted coverings. Clearly,  $C$  is a perfect **m-covering** if and only if equality holds in (13.1.3).

Many classes of codes can be viewed in a natural way as weighted coverings. Let  $C$  be an **m-covering**. If  $m_0 = m_1 = \dots = m_r = 1$ , then  $C$  is simply a code with covering radius *at most*  $r$ . The code  $C$  is called a *multiple covering* if  $m_0 = m_1 = \dots = m_r = 1/\mu$  for some positive integer  $\mu$ , and a *multiple covering of deep holes* if  $m_0 = m_1 = \dots = m_{r-1} = 1, m_r = 1/\mu$  for some positive integer  $\mu$ . These two classes are studied in Chapter 14. If  $L \subseteq \{0, 1, \dots, [n/2]\}$ ,  $m_i = 1$  for all  $i \in L$  and  $m_i = 0$  for all  $i \notin L$ , then  $C$  is called an *L-covering*; see Section 19.1. In Section 5.4 weighted coverings with  $m_{R_1^*} = m_{R_1^*+1} = \dots = m_{R_0^*} = 1$  and  $m_i = 0$  for all other  $i$  are used as building blocks for covering codes. The approach presented in Section 6.5 is based on showing that a code with covering radius  $R$  is an **m-covering** for a suitable vector  $\mathbf{m}$  and applying the sphere-covering bound (13.1.3) for weighted coverings.

Generalizations of perfect codes studied in Section 11.6 can be viewed as perfect weighted coverings for different choices of  $\mathbf{m}$ . Let  $C$  be a binary perfect **m-covering** with minimum distance  $d$ , and denote  $e = \lfloor (d-1)/2 \rfloor$ . If  $m_0 = m_1 = \dots = m_r = 1$ , then  $C$  is a perfect code with covering radius  $r$ . If

$r = e + 1$  and  $m_0 = m_1 = \dots = m_{e-1} = 1$ ,  $m_e = m_{e+1} = 1/\lfloor (n+1)/(e+1) \rfloor$ , then  $C$  is a nearly perfect code. If  $r$  equals the covering radius of  $C$ , then  $C$  is a generalized uniformly packed code. If  $r = e + 1$  and  $m_0 = m_1 = \dots = m_{e-1} = 1$ ,  $m_e = m_{e+1} = 1/t$  for some positive integer  $t$ , then  $C$  is a strongly uniformly packed code. Finally,  $C$  is a uniformly packed code of the  $j$ -th order if  $R = r = e + j$  and for some positive integer  $t$  and nonnegative integer  $u$  we have  $m_0 = m_1 = \dots = m_{d-e-j-1} = 1$ ,  $m_{d-e-j} = \dots = m_e = 1 - u/t$ ,  $m_{e+1} = \dots = m_{e+j} = 1/t$ .

We say that a code  $C \subseteq Q^n$  is an **m-packing** if

$$\sum_{i=0}^r m_i \mathcal{A}_i(\mathbf{x}) \leq 1$$

for all  $\mathbf{x} \in Q^n$ , i.e., the **m-density** at every  $\mathbf{x} \in Q^n$  is at most 1. Assume that all the  $m_i$ 's are nonnegative. Let  $v = \sum_{i=0}^r m_i \binom{n}{i} (q-1)^i$ . If  $v \leq 1$ , then every  $C \subseteq Q^n$  is an **m-packing** and no  $C$  is an **m-covering** except the whole space if  $v = 1$ . Assume that  $v > 1$  and  $C \subset Q^n$ , and denote  $C' = Q^n \setminus C$ . Then  $\langle \mathbf{m}, \mathcal{A}(\mathbf{x}) \rangle + \langle \mathbf{m}, \mathcal{A}'(\mathbf{x}) \rangle = v$  for all  $\mathbf{x} \in Q^n$ , where  $\mathcal{A}'(\mathbf{x})$  is the weight distribution of  $C'$  with respect to  $\mathbf{x}$ . We see that  $\langle \mathbf{m}, \mathcal{A}(\mathbf{x}) \rangle \geq 1$  is equivalent to the condition  $\langle \mathbf{m}', \mathcal{A}'(\mathbf{x}) \rangle \leq 1$ , where  $\mathbf{m}' = (m_0/(v-1), m_1/(v-1), \dots, m_n/(v-1))$ , i.e.,  $C$  is an **m-covering** if and only if  $C'$  is an **m'-packing**. Similarly,  $C$  is an **m-packing** if and only if  $C'$  is an **m'-covering**. This shows that for given  $q$ ,  $n$  and  $\mathbf{m}$  with  $v > 1$ , finding all the **m-coverings** is equivalent to finding all the **m'-packings**.

## 13.2 Lloyd theorem for perfect weighted coverings

We now prove the Lloyd theorem for weighted coverings. Let  $q \geq 2$  be an arbitrary integer. Recall that the Krawtchouk polynomials  $P_k(x)$  for  $k = 0, 1, 2, \dots$  are defined by (see Section 2.3)

$$P_k(x) = \sum_{j=0}^k (-1)^j (q-1)^{k-j} \binom{x}{j} \binom{n-x}{k-j},$$

where

$$\binom{x}{j} = \frac{x(x-1) \cdots (x-j+1)}{j!}.$$

The polynomial  $P_k(x)$  has degree  $k$ .

Denote  $\omega = e^{2\pi i/q}$ , which is a primitive  $q$ -th root of unity in the field of complex numbers. Define for  $x \in \mathbb{Z}_q$

$$e(x) = \omega^x,$$

and for all  $\mathbf{u}, \mathbf{x} \in \mathbb{Z}_q^n$

$$\psi_{\mathbf{u}}(\mathbf{x}) = e(\langle \mathbf{u}, \mathbf{x} \rangle),$$

where

$$\langle \mathbf{u}, \mathbf{x} \rangle = u_1 x_1 + u_2 x_2 + \dots + u_n x_n \in \mathbb{Z}_q.$$

Clearly,  $\psi_{\mathbf{u}}$  is an additive character of  $\mathbb{Z}_q^n$ , and therefore by Theorem 2.5.11, for all  $\mathbf{u} \neq 0$ ,

$$\sum_{\mathbf{x} \in \mathbb{Z}_q^n} \psi_{\mathbf{u}}(\mathbf{x}) = 0. \quad (13.2.1)$$

Denote by  $S_k$  the set of all vectors of weight  $k$  in  $\mathbb{Z}_q^n$ .

**Lemma 13.2.2** *For every  $\mathbf{u} \in \mathbb{Z}_q^n$ ,*

$$\sum_{\mathbf{y} \in S_k} \psi_{\mathbf{u}}(\mathbf{y}) = P_k(w(\mathbf{u})). \quad (13.2.3)$$

**Proof.** Assume without loss of generality that  $w(\mathbf{u}) = i$  and that the nonzero coordinates of  $\mathbf{u}$  are in the first  $i$  positions. Choose  $k$  positions  $1 \leq h_1 < h_2 < \dots < h_j \leq i < h_{j+1} < \dots < h_k \leq n$  and denote by  $H$  the set of all vectors of weight  $k$  whose nonzero coordinates are in these positions. Then

$$\begin{aligned} \sum_{\mathbf{x} \in H} \psi_{\mathbf{u}}(\mathbf{x}) &= \sum_{x_{h_1} \in \mathbb{Z}_q \setminus \{0\}} \dots \sum_{x_{h_k} \in \mathbb{Z}_q \setminus \{0\}} e(u_{h_1} x_{h_1} + \dots + u_{h_k} x_{h_k}) \\ &= (q-1)^{k-j} \prod_{\ell=1}^j \sum_{x \in \mathbb{Z}_q \setminus \{0\}} e(u_{h_\ell} x) = (q-1)^{k-j} (-1)^j. \end{aligned}$$

There are  $\binom{i}{j} \binom{n-i}{k-j}$  choices for  $H$ , and the claim follows.  $\square$

**Lemma 13.2.4** *If the real numbers  $\beta(\mathbf{x})$  satisfy the condition*

$$\sum_{\mathbf{x} \in \mathbb{Z}_q^n} \beta(\mathbf{x}) \psi_{\mathbf{u}}(\mathbf{x}) = 0$$

for all  $\mathbf{u} \in \mathbb{Z}_q^n$ , then  $\beta(\mathbf{x}) = 0$  for all  $\mathbf{x} \in \mathbb{Z}_q^n$ .

**Proof.** For any  $\mathbf{v} \in \mathbb{Z}_q^n$ ,

$$0 = \sum_{\mathbf{u} \in \mathbb{Z}_q^n} \psi_{\mathbf{u}}(-\mathbf{v}) \sum_{\mathbf{x} \in \mathbb{Z}_q^n} \beta(\mathbf{x}) \psi_{\mathbf{u}}(\mathbf{x}) = \sum_{\mathbf{x} \in \mathbb{Z}_q^n} \beta(\mathbf{x}) \sum_{\mathbf{u} \in \mathbb{Z}_q^n} \psi_{\mathbf{u}}(\mathbf{x} - \mathbf{v}) = q^n \beta(\mathbf{v})$$

by (13.2.1).  $\square$

Let  $\mathbf{m} = (m_0, m_1, \dots, m_r)$ . The *generalized Lloyd polynomial*  $L_{\mathbf{m}}(x)$  is defined by

$$L_{\mathbf{m}}(x) = \sum_{i=0}^r m_i P_i(x).$$

The following result is the *Lloyd theorem* for weighted coverings.

**Theorem 13.2.5** *If a perfect  $\mathbf{m}$ -covering  $C$  of length  $n$  and covering radius  $R$  over  $\mathbb{Z}_q$  exists, then at least  $R$  of the integers  $1, 2, \dots, n$  are zeros of the polynomial  $L_{\mathbf{m}}(x)$ .*

**Proof.** Because  $C$  is perfect, we know that  $\sum_{i=0}^r m_i \mathcal{A}_i(\mathbf{x}) = 1$  for all  $\mathbf{x} \in \mathbb{Z}_q^n$ . Furthermore, the quantity  $\mathcal{A}_i(\mathbf{x})$  is equal to the number of pairs  $(\mathbf{c}, \mathbf{s})$  such that  $\mathbf{c} \in C$ ,  $\mathbf{s} \in S_i$ , and  $\mathbf{x} = \mathbf{s} + \mathbf{c}$ . Therefore

$$\begin{aligned} & \left( \sum_{i=0}^r \sum_{\mathbf{s} \in S_i} m_i \psi_{\mathbf{u}}(\mathbf{s}) \right) \left( \sum_{\mathbf{c} \in C} \psi_{\mathbf{u}}(\mathbf{c}) \right) = \sum_{i=0}^r \sum_{\mathbf{s} \in S_i} \sum_{\mathbf{c} \in C} m_i \psi_{\mathbf{u}}(\mathbf{s} + \mathbf{c}) \\ &= \sum_{i=0}^r \sum_{\mathbf{x} \in \mathbb{Z}_q^n} m_i \mathcal{A}_i(\mathbf{x}) \psi_{\mathbf{u}}(\mathbf{x}) = \sum_{\mathbf{x} \in \mathbb{Z}_q^n} \psi_{\mathbf{u}}(\mathbf{x}) = \begin{cases} 0 & \text{if } \mathbf{u} \neq \mathbf{0} \\ q^n & \text{if } \mathbf{u} = \mathbf{0} \end{cases} \quad (13.2.6) \end{aligned}$$

by (13.2.1). By Lemma 13.2.2,

$$\sum_{i=0}^r \sum_{\mathbf{s} \in S_i} m_i \psi_{\mathbf{u}}(\mathbf{s}) = \sum_{i=0}^r m_i P_i(w(\mathbf{u})) = L_{\mathbf{m}}(w(\mathbf{u})), \quad (13.2.7)$$

and by (13.2.6),  $L_{\mathbf{m}}(j) = 0$  for every integer  $j, 1 \leq j \leq n$ , such that

$$\sum_{\mathbf{c} \in C} \psi_{\mathbf{u}}(\mathbf{c}) \neq 0$$

for some  $\mathbf{u} \in S_j$ . Denote by  $D^\perp$  the set of such integers  $j$  and  $s^\perp = |D^\perp|$ . Define

$$\alpha(x) = \frac{q^n}{|C|} \prod_{j \in D^\perp} \left(1 - \frac{x}{j}\right),$$

which is called the *annihilator polynomial* of  $C$ . Let  $\alpha(x) = \sum_{i=0}^{s^\perp} \alpha_i P_i(x)$  be the Krawtchouk expansion of  $\alpha(x)$ .

Assume that  $s^\perp < R$ . By the definition of  $D^\perp$ ,

$$\alpha(w(\mathbf{u})) \sum_{\mathbf{c} \in C} \psi_{\mathbf{u}}(\mathbf{c}) = \begin{cases} 0 & \text{if } \mathbf{u} \neq \mathbf{0} \\ q^n & \text{if } \mathbf{u} = \mathbf{0} \end{cases} \quad (13.2.8)$$

and by Lemma 13.2.2 the left hand side of (13.2.8) is

$$\begin{aligned} \left( \sum_{i=0}^{s^\perp} \alpha_i \sum_{\mathbf{y} \in S_i} \psi_{\mathbf{u}}(\mathbf{y}) \right) \sum_{\mathbf{c} \in C} \psi_{\mathbf{u}}(\mathbf{c}) &= \sum_{i=0}^{s^\perp} \alpha_i \sum_{\mathbf{y} \in S_i} \sum_{\mathbf{c} \in C} \psi_{\mathbf{u}}(\mathbf{y} + \mathbf{c}) \\ &= \sum_{\mathbf{x} \in \mathbb{Z}_q^n} \gamma(\mathbf{x}) \psi_{\mathbf{u}}(\mathbf{x}), \end{aligned}$$

for some real numbers  $\gamma(\mathbf{x})$  such that  $\gamma(\mathbf{x}) = 0$  when  $s^\perp < d(\mathbf{x}, C) \leq R$ . But now (13.2.6), (13.2.8) and Lemma 13.2.4 with  $\beta(\mathbf{x}) = \gamma(\mathbf{x}) - 1$  imply that  $\gamma(\mathbf{x}) = 1$  for all  $\mathbf{x} \in \mathbb{Z}_q^n$ , a contradiction. Hence we must have  $s^\perp \geq R$  and our claim follows.  $\square$

Consider now the case when the alphabet is  $\mathbb{F}_q$  instead of  $\mathbb{Z}_q$ . Assume that  $p$  is a prime and  $q = p^m$ , and that  $C$  is a perfect weighted covering over  $\mathbb{F}_q$ . If we define  $e(x) = e^{2\pi i T^r(x)/p}$  for all  $x \in \mathbb{F}_q$  and  $\psi_{\mathbf{u}}(\mathbf{x}) = e(\langle \mathbf{u}, \mathbf{x} \rangle)$  for  $\mathbf{x}, \mathbf{u} \in \mathbb{F}_q^n$ , then the functions  $\psi_{\mathbf{u}}$  are the additive characters of  $\mathbb{F}_q^n$ , and we see that exactly the same proof as before holds. In particular, every integer  $j$  such that

$$\sum_{\mathbf{c} \in C} \psi_{\mathbf{u}}(\mathbf{c}) \neq 0 \tag{13.2.9}$$

for some  $\mathbf{u} \in S_j$ , is a zero of the Lloyd polynomial  $L_{\mathbf{m}}(x)$ . The previous proof shows that

$$R \leq s^\perp \leq r.$$

If  $r = R$ ,  $m_0 = m_1 = \dots = m_R = 1$  and  $C$  is a perfect code with covering radius  $R$ , we of course have

$$R = s^\perp. \tag{13.2.10}$$

If  $C$  is a linear code, then (13.2.9) holds if and only if  $\mathbf{u} \in C^\perp$ . Then  $s^\perp$  is the number of nonzero weights in the dual code, and every nonzero weight of the dual code  $C^\perp$  is a zero of the Lloyd polynomial.

A code can be a perfect weighted covering for several different choices of the weight vector  $\mathbf{m}$ . For instance, the code of length  $n$  consisting of all  $q^n$  possible  $n$ -tuples is a perfect weighted covering for  $m_0 = m_1 = \dots = m_r = 1/V_q(n, r)$  and arbitrary  $r \in [0, n]$ . On the other hand, using arguments similar to the proof of the Lloyd theorem, we now show that any code  $C$  is a perfect weighted covering for at least one choice of  $\mathbf{m}$ , namely the vector whose coordinates are the coefficients of the Krawtchouk expansion of its annihilator polynomial. Let

$$\mathcal{A}_i^\perp(\mathbf{x}) = \frac{1}{|C|} \sum_{k=0}^n \mathcal{A}_k(\mathbf{x}) P_i(k).$$

The inverse transform is

$$\mathcal{A}_k(\mathbf{x}) = \frac{|C|}{q^n} \sum_{i=0}^n \mathcal{A}_i^\perp(\mathbf{x}) P_k(i). \quad (13.2.11)$$

Now, let  $\alpha(x) = \sum_{k=0}^{s^\perp} \alpha_k P_k(x)$  be the annihilator polynomial of the code. Then, from (13.2.11),

$$\begin{aligned} \sum_{k=0}^{s^\perp} \alpha_k \mathcal{A}_k(\mathbf{x}) &= \frac{|C|}{q^n} \sum_{k=0}^{s^\perp} \alpha_k \sum_{i=0}^n \mathcal{A}_i^\perp(\mathbf{x}) P_k(i) \\ &= \frac{|C|}{q^n} \sum_{i=0}^n \mathcal{A}_i^\perp(\mathbf{x}) \sum_{k=0}^{s^\perp} \alpha_k P_k(i) \\ &= \frac{|C|}{q^n} \sum_{i=0}^n \alpha(i) \mathcal{A}_i^\perp(\mathbf{x}). \end{aligned}$$

By Corollary 8.3.3 (whose  $q$ -ary generalization is straightforward),  $\mathcal{A}_i^\perp(\mathbf{x}) \neq 0$  only if either  $i \in D^\perp$ , or  $i = 0$  in which case  $\mathcal{A}_0^\perp(\mathbf{x}) = 1$ . Hence,

$$\sum_{k=0}^{s^\perp} \alpha_k \mathcal{A}_k(\mathbf{x}) = \frac{|C|}{q^n} \alpha(0) = 1.$$

### 13.3 Perfect weighted coverings with radius one

In this section we study perfect weighted coverings over  $\mathbb{F}_q$ . Elementary methods and concatenation turn out to be sufficient for determining all the parameters for which  $q$ -ary linear perfect weighted coverings with radius 1 exist; using the previous section we obtain a complete characterization. For some further results on perfect multiple coverings, see Section 14.2.

If  $C \subset \mathbb{F}_q^n$  is an  $(m_0, m_1)$ -covering, then  $m_1 > 0$ . If, furthermore,  $C$  is a perfect  $(m_0, m_1)$ -covering, then considering the density at non-codewords (respectively, codewords) we conclude that  $m_1 \leq 1$  (respectively,  $m_0 \leq 1$ ).

**Theorem 13.3.1** *Assume that the codes  $C(\alpha) \subset \mathbb{F}_q^n$ ,  $\alpha \in \mathbb{F}_{q'}$ , are disjoint (perfect)  $(m_0, m_1)$ -coverings and their union is  $\mathbb{F}_q^n$ . Assume further that  $D \subset \mathbb{F}_{q'}^N$  is a (perfect)  $(M_0, M_1)$ -covering. Then the code*

$$\bigcup_{(\mathbf{x}_1, \dots, \mathbf{x}_N) \in D} C(\mathbf{x}_1) \oplus \dots \oplus C(\mathbf{x}_N)$$

*is a (perfect)  $(M_0 - NM_1(1 - m_0), m_1 M_1)$ -covering in  $\mathbb{F}_q^{Nn}$ .*

**Proof.** Suppose  $\mathbf{z} = (\mathbf{z}_1, \mathbf{z}_2, \dots, \mathbf{z}_N) \in \mathbb{F}_q^{Nn}$  where each  $\mathbf{z}_i$  has length  $n$ . Because the union of the codes  $C(\alpha)$  is the whole space  $\mathbb{F}_q^n$ , there exists a vector  $\mathbf{y} = (y_1, y_2, \dots, y_N) \in \mathbb{F}_{q'}^N$  such that  $\mathbf{z} \in C(y_1) \oplus \dots \oplus C(y_N)$ .

Assume first that  $d(\mathbf{y}, D) = 1$ . Then there are at least  $1/M_1$  words  $\mathbf{x} = (x_1, x_2, \dots, x_N) \in D$  such that  $d(\mathbf{y}, \mathbf{x}) = 1$ , and for each such word  $\mathbf{x}$  there are at least  $1/m_1$  words in  $C(x_1) \oplus \dots \oplus C(x_N)$  that have distance 1 to  $\mathbf{z}$ .

Assume second that  $\mathbf{y} \in D$ . Then  $\mathbf{z} \in C(y_1) \oplus \dots \oplus C(y_N)$ , and in each  $C(y_i)$  there are at least  $(1 - m_0)/m_1$  words that have distance 1 to  $\mathbf{z}_i$ . Therefore, together there are at least  $N(1 - m_0)/m_1$  words in  $C(y_1) \oplus \dots \oplus C(y_N)$  that have distance 1 to  $\mathbf{z}$ . Furthermore, there are at least  $(1 - M_0)/M_1$  words  $\mathbf{x} \in D$  such that  $d(\mathbf{y}, \mathbf{x}) = 1$ , and for each such word  $\mathbf{x}$  there are again at least  $1/m_1$  words in  $C(x_1) \oplus \dots \oplus C(x_N)$  that have distance 1 to  $\mathbf{z}$ .

In both cases it is easy to check that the  $(M_0 - NM_1(1 - m_0), m_1 M_1)$ -density at  $\mathbf{z}$  is at least 1.

If the codes  $C(\alpha)$  and  $D$  are perfect, then in the previous discussion the estimated numbers of words are exact and the  $(M_0 - NM_1(1 - m_0), m_1 M_1)$ -density at  $\mathbf{z}$  equals 1.  $\square$

**Theorem 13.3.2** *If  $C$  is a perfect  $q$ -ary  $(m_0, m_1)$ -covering, then the code  $C \oplus \mathbb{F}_q$  is a perfect  $(m_0 - (q - 1)m_1, m_1)$ -covering.*

**Proof.** Let  $(\mathbf{x}, \alpha), \mathbf{x} \in \mathbb{F}_q^n, \alpha \in \mathbb{F}_q$  be arbitrary and denote  $D = C \oplus \mathbb{F}_q$ .

If  $\mathbf{x} \in C$ , then  $(\mathbf{x}, \alpha) \in D$  and the words of  $D$  that have distance 1 to  $(\mathbf{x}, \alpha)$  are the  $q - 1$  words  $(\mathbf{x}, \beta) \in D, \beta \neq \alpha$ , and the  $(1 - m_0)/m_1$  words  $(\mathbf{y}, \alpha)$  where  $\mathbf{y} \in C$  and  $d(\mathbf{y}, \mathbf{x}) = 1$ .

If  $d(\mathbf{x}, C) = 1$ , then also  $d((\mathbf{x}, \alpha), D) = 1$  and the words of  $D$  that have distance 1 to  $(\mathbf{x}, \alpha)$  are precisely the  $1/m_1$  words  $(\mathbf{y}, \alpha)$  where  $\mathbf{y} \in C$  and  $d(\mathbf{y}, \mathbf{x}) = 1$ .  $\square$

If  $C \subset \mathbb{F}_q^n$  is a perfect linear  $(m_0, m_1)$ -covering with dimension  $n - i$  ( $0 < i \leq n$ ), then because (13.1.3) holds with equality, we have  $m_0 + (q - 1)m_1 = q^i$ . Here  $m_0$  and  $m_1$  are rational numbers and by the remark preceding Theorem 13.3.1,  $m_0 \leq 1$  and  $0 < m_1 \leq 1$ . Thus  $m_0 = a/t$  and  $m_1 = b/t$  for some integers  $t > 0, a \leq t, 0 < b \leq t$ . Because  $C \neq \mathbb{F}_q^n$ , there exists a vector  $\mathbf{x} \notin C$ , and  $\theta(\mathbf{x}) = 1$  implies that some multiple of  $b/t$  equals one, and hence  $b$  divides  $t$ . On the other hand, if  $\mathbf{x} \in C$ , then  $\theta(\mathbf{x}) = 1$  implies that some multiple of  $b/t$  equals  $1 - a/t$  and hence  $b$  divides  $a$ . We may therefore assume that  $b = 1$ .

**Theorem 13.3.3** *A perfect  $q$ -ary linear  $(m_0, m_1)$ -covering  $C \subset \mathbb{F}_q^n$  exists if and only if*

$$m_0 = a/t, m_1 = 1/t \text{ for some integers } t > 0, a \leq t$$

and for some integer  $i > 0$

$$n = \frac{tq^i - a}{q - 1}.$$

**Proof.** We have already seen that  $m_0$  and  $m_1$  are as described in the theorem. By the sphere-covering equality we have  $n = (tq^i - a)/(q - 1)$ . In particular,  $a \equiv t \pmod{q - 1}$ .

To construct such codes, assume first that  $a = t$ . Then we can in Theorem 13.3.1 choose

$$C(\alpha) = \{\mathbf{x} = (x_1, x_2, \dots, x_t) \in \mathbb{F}_q^t : x_1 + x_2 + \dots + x_t = \alpha\}$$

for  $\alpha \in \mathbb{F}_q$  and

$$D = \text{the } q\text{-ary linear Hamming code of length } (q^i - 1)/(q - 1).$$

Each  $C(\alpha)$  is a perfect  $(1, 1/t)$ -covering and  $D$  is a perfect  $(1, 1)$ -covering. Then Theorem 13.3.1 yields a perfect  $(1, 1/t)$ -covering  $C$  of length  $t(q^i - 1)/(q - 1)$ , clearly linear by the construction and the definitions of  $C(\alpha)$  and  $D$ . If  $a$  is smaller than  $t$ , then  $a = t - (q - 1)j$  for some integer  $j \geq 1$ , and we obtain the required perfect  $(a/t, 1/t)$ -covering of length  $j + t(q^i - 1)/(q - 1)$  by applying Theorem 13.3.2 to  $C$   $j$  times.  $\square$

To characterize all the  $q$ -ary linear perfect weighted coverings with radius one we need the following theorem.

**Theorem 13.3.4** *If all the nonzero codewords of a  $q$ -ary  $[n, k]$  code have the same weight and no coordinate is identically zero, then the code has a generator matrix of the form  $(\mathbf{G}_1, \mathbf{G}_2, \dots, \mathbf{G}_t)$ , where each  $\mathbf{G}_i$  is a generator matrix of the  $k$ -dimensional simplex code over  $\mathbb{F}_q$ , i.e., a  $k \times (q^k - 1)/(q - 1)$  matrix whose columns are pairwise linearly independent.*

**Proof.** Because no coordinate is identically 0, each element of  $\mathbb{F}_q$  appears  $q^{k-1}$  times in each coordinate. Therefore the sum of the weights of all the codewords equals  $n(q - 1)q^{k-1}$ . On the other hand, if we denote by  $w$  the only nonzero weight in the code, this sum is equal to  $w(q^k - 1)$ . As  $q^{k-1}$  and  $(q^k - 1)/(q - 1)$  are mutually prime,  $n = t(q^k - 1)/(q - 1)$  for some positive integer  $t$ , and  $w = tq^{k-1}$ .

Consider now the codewords that are nonzero in the  $i$ -th coordinate. We know that there are  $(q-1)q^{k-1}$  such codewords and therefore the sum of their weights equals  $S = w(q-1)q^{k-1}$ . We can also calculate this sum in another way. Let  $j$  be any other coordinate. If the columns  $i$  and  $j$  of the generator matrix are linearly independent, then for all  $\alpha, \beta \in \mathbb{F}_q$  there are exactly  $q^{k-2}$  codewords  $\mathbf{c}$  such that  $c_i = \alpha$  and  $c_j = \beta$ . Hence among the codewords that are nonzero in the  $i$ -th coordinate there are exactly  $(q-1)^2q^{k-2}$  words in which also the  $j$ -th coordinate is nonzero. If the columns  $i$  and  $j$  are linearly dependent, i.e., the column  $j$  is a nonzero multiple of the column  $i$ , then the  $j$ -th coordinate is nonzero if and only if the  $i$ -th coordinate is nonzero. Denote by  $f_i$  the number of columns in the generator matrix that are nonzero multiples of the column  $i$  (including the column  $i$ ). Then  $S = f_i(q-1)q^{k-1} + (n-f_i)(q-1)^2q^{k-2}$  and consequently  $f_i(q-1)q^{k-1} + (n-f_i)(q-1)^2q^{k-2} = w(q-1)q^{k-1}$ . Substituting the expressions for  $n$  and  $w$  and solving for  $f_i$  we obtain  $f_i = t$ , independently of  $i$ . However, the maximum number of pairwise linearly independent columns over  $\mathbb{F}_q$  is  $(q^k - 1)/(q - 1)$ , and  $n = t(q^k - 1)/(q - 1)$ . Hence there are exactly  $t$  nonzero multiples of each nonzero column, and the generator matrix is as claimed.  $\square$

Assume now that  $C$  is a linear perfect  $(m_0, m_1)$ -covering. The discussion following Theorem 13.2.5 implies that  $s^\perp \leq r = 1$ , where  $s^\perp$  denotes the number of nonzero weights in the dual code  $C^\perp$ . If  $s^\perp = 0$  then  $C = \mathbb{F}_q^n$ . Assume that  $s^\perp = 1$ . By the previous theorem, the generator matrix of  $C^\perp$  has the form

$$\mathbf{H} = (\mathbf{G}_1, \mathbf{G}_2, \dots, \mathbf{G}_t, \mathbf{0}) \quad (13.3.5)$$

where each  $\mathbf{G}_i$  is a generator matrix of the  $j$ -dimensional simplex code for some  $j$  and  $\mathbf{0}$  is the  $j \times \ell$  zero matrix for some  $\ell \geq 0$ . In the parity check matrix  $\mathbf{H}$  of  $C$  the number of nonzero multiples of any nonzero column is  $t$ , and therefore the density of  $C$  at each non-codeword equals  $tm_1$ . Similarly, the density at every codeword equals  $m_0 + (q-1)\ell m_1$ . Hence  $tm_1 = m_0 + (q-1)\ell m_1 = 1$ . We see that  $n = t(q^j - 1)/(q - 1) + \ell$ ,  $m_0 = 1 - (q-1)\ell/t$ , and  $m_1 = 1/t$ , and that given  $q$ ,  $n$ ,  $m_0$ , and  $m_1$ , the integers  $t$ ,  $\ell$  and  $j$  are uniquely determined. We have therefore proved the following result.

**Theorem 13.3.6** *For every  $q, n, m_0, m_1$  for which there exists a  $q$ -ary perfect linear  $(m_0, m_1)$ -covering of length  $n$ , such a code is unique up to equivalence.*  $\square$

In the nonlinear case all the parameters for which a perfect weighted covering with radius one exists are not known. If  $C \subset \mathbb{Z}_q^n$  is a perfect  $(m_0, m_1)$ -covering with  $K$  codewords, then as in the linear case we may assume that

$m_0 = a/t$  and  $m_1 = 1/t$  for some integers  $t > 0$  and  $a \leq t$ . In contrast to the linear case, the condition  $K(a + (q - 1)n) = tq^n$  is not sufficient for the existence of a  $q$ -ary  $(a/t, 1/t)$ -covering of length  $n$ . The following theorem shows that, for instance, no binary perfect  $(1, 1/3)$ -covering of length 5 exists.

**Theorem 13.3.7** *If a perfect  $(1, 1/t)$ -covering  $C \subset \mathbb{F}^n$  exists and  $n \neq t$ , then  $n \geq 2t + 1$ .*

**Proof.** If necessary we translate  $C$  so that it does not contain the all-zero vector. Then there are exactly  $t$  codewords of weight 1 in  $C$ . Suppose  $\mathbf{x}$  is any other vector of weight 1. Then  $\mathbf{x}$  is covered by  $t$  codewords of  $C$  of weight 2, none of which has any 1's in common with the codewords of weight 1. Therefore  $n \geq t + (t + 1) = 2t + 1$ .  $\square$

## 13.4 Weighted coverings and nonexistence results

Weighted coverings are useful in obtaining nonexistence results for conventional coverings. The argument is as follows: we prove first that the existence of a (usual) covering yields a weighted covering of radius greater than the covering radius of the initial code, with some explicitly calculated weights; second, we check if the derived weighted covering satisfies the generalized sphere-covering condition. If the condition does not hold, a covering with the initial parameters does not exist. Recall that the sphere-covering bound for binary weighted  $\mathbf{m}$ -coverings reads:

$$K \geq \frac{2^n}{\sum_{i=0}^n m_i \binom{n}{i}}. \quad (13.4.1)$$

For example, assume that there exists an  $(n, K)_R$  code  $C$ . By Lemma 6.4.2 — or the discussion in Section 6.5 — we know that inequality (6.5.12) holds, i.e.,

$$\sum_{i=0}^{R-1} \lceil \frac{n+1}{R+1} \rceil \mathcal{A}_i(\mathbf{x}) + \mathcal{A}_R(\mathbf{x}) + \mathcal{A}_{R+1}(\mathbf{x}) \geq \lceil \frac{n+1}{R+1} \rceil.$$

In other words,  $C$  is an  $\mathbf{m}$ -covering when  $m_i = 1$  for  $i = 0, \dots, R - 1$ ,  $m_R = m_{R+1} = \lceil (n+1)/(R+1) \rceil^{-1}$ ,  $m_i = 0$  for  $i > R + 1$ . The sphere-covering bound for such  $\mathbf{m}$ -coverings is:

$$K \geq \frac{2^n}{\sum_{i=0}^{R-1} \binom{n}{i} + \lceil (n+1)/(R+1) \rceil^{-1} (\binom{n}{R} + \binom{n}{R+1})},$$

which is slightly weaker than the first excess bound (Theorem 6.4.4).

If we consider coverings by spheres of radius 2, we get the pair covering inequality (Theorem 6.5.9), which shows that an  $(n, K)R$  code is an  $\mathbf{m}$ -covering with  $m_0 = \dots = m_{R-2} = 1$ ,  $m_{R-1} = m_R = t_1/t_0$ ,  $m_{R+1} = m_{R+2} = 1/t_0$  and  $m_i = 0$  for  $i > R + 2$ , where

$$t_1 = \max_{i \geq 2} \frac{F(n - R + 1, R + 2) - F(n - iR + 1, R + 2)}{i - 1},$$

$t_0 = t_1 + F(n - R + 1, R + 2)$  and  $F(v, s)$  is the minimum cardinality of a  $2-(v, s, 1)$  covering design (cf. Section 2.7).

Now, we restrict ourselves to linear coverings.

**Theorem 13.4.2** *Assume that for a given  $\mathbf{m}$ , every linear  $[n, k]R$  code  $C$  is also an  $\mathbf{m}$ -covering. Then*

$$|L_{\mathbf{m}}(w(\mathbf{u}))| \leq L_{\mathbf{m}}(0) - 2^{n-k} = \sum_{i=0}^n m_i \binom{n}{i} - 2^{n-k} \quad (13.4.3)$$

for every nonzero  $\mathbf{u} \in C^\perp$ .

**Proof.** We proceed similarly to the proof of the Lloyd theorem. Assume that a linear  $[n, k]R$  code  $C$  exists and is an  $\mathbf{m}$ -covering. For any nonzero  $\mathbf{u} \in \mathbb{F}^n$ , we have (cf. (13.2.6))

$$\begin{aligned} & \left| \left( \sum_{i=0}^r \sum_{\mathbf{s} \in S_i} m_i \psi_{\mathbf{u}}(\mathbf{s}) \right) \left( \sum_{\mathbf{c} \in C} \psi_{\mathbf{u}}(\mathbf{c}) \right) \right| \\ &= \left| \sum_{\mathbf{x} \in \mathbb{F}^n} \theta(\mathbf{x}) \psi_{\mathbf{u}}(\mathbf{x}) \right| \\ &\leq \left| \sum_{\mathbf{x} \in \mathbb{F}^n} \psi_{\mathbf{u}}(\mathbf{x}) \right| + \left| \sum_{\mathbf{x} \in \mathbb{F}^n} (\theta(\mathbf{x}) - 1) \psi_{\mathbf{u}}(\mathbf{x}) \right| \\ &= \left| \sum_{\mathbf{x} \in \mathbb{F}^n} (\theta(\mathbf{x}) - 1) \psi_{\mathbf{u}}(\mathbf{x}) \right| \\ &\leq \left( \sum_{\mathbf{x} \in \mathbb{F}^n} \theta(\mathbf{x}) \right) - 2^n. \end{aligned}$$

Furthermore, since

$$\sum_{\mathbf{x} \in \mathbb{F}^n} \theta(\mathbf{x}) = 2^k \sum_{i=0}^r m_i \binom{n}{i} = 2^k L_{\mathbf{m}}(0),$$

$$\sum_{\mathbf{c} \in C} \psi_{\mathbf{u}}(\mathbf{c}) = 2^k \quad \text{for } \mathbf{u} \in C^\perp,$$

and

$$\sum_{i=0}^r \sum_{s \in S_i} m_i \psi_u(s) = L_m(w(u))$$

by (13.2.7), we conclude that for every nonzero  $u \in C^\perp$

$$|L_m(w(u))| \leq L_m(0) - 2^{n-k}.$$

□

Now, the following argument can be used. In order to prove the nonexistence of an  $[n, k]R$  code, find the vector  $m$  of a derived weighted covering, and the corresponding  $L_m(x)$ . Comparing  $|L_m(x)|$  with  $L_m(0) - 2^{n-k}$ , find all  $x$  satisfying (13.4.3). They are candidates for weights of the dual code. In particular, the minimal  $x$  lowerbounds the minimum distance of the dual code. If we are able to demonstrate the nonexistence of an  $[n, n-k]$  code having weights in the found range, we are done.

**Example 13.4.4** We prove the nonexistence of a  $[36, 15]6$  code. The pair covering inequality shows that such a code is an  $m$ -covering with  $r = 8$ ,  $m_0 = \dots = m_4 = 1$ ,  $m_5 = m_6 = 7/27$  and  $m_7 = m_8 = 1/27$ . We have

$$\begin{aligned} L_m(x) &= \sum_{i=0}^4 P_i(x) + \frac{7}{27}(P_5(x) + P_6(x)) + \frac{1}{27}(P_7(x) + P_8(x)) \\ &= \frac{18894244}{9} - \frac{960603916}{945}x + \frac{359428658}{1701}x^2 - \frac{29960972}{1215}x^3 + \\ &\quad \frac{79592}{45}x^4 - \frac{97088}{1215}x^5 + \frac{20}{9}x^6 - \frac{296}{8505}x^7 + \frac{2}{8505}x^8. \end{aligned}$$

Now,

$$L_m(0) - 2^{21} = \frac{19876}{9}.$$

Furthermore, the first ten values (for  $x = 0, \dots, 9$ ) of  $L_m(x) - \frac{19876}{9}$ , rounded to the nearest integer, are 2097152, 1268976, 737951, 408949, 213294, 102623, 43859, 15162, 2725 and -1712. Hence, the minimum distance of  $C^\perp$  is at least 9. However, it is known that the largest possible minimum distance of a  $[36, 21]$  code is 8 (Brouwer and Verhoeff [96]), a contradiction. □

## 13.5 Notes

§13.1 The discussion of the whole chapter is based on Cohen, Honkala, Litsyn and Mattson [155]; but see already S. M. Johnson [354], Cohen, Litsyn and Mattson [160], [159] and Cohen, Honkala and Litsyn [154].

List decoding and spelling checkers are mentioned as possible applications of weighted packings in [155]. In list decoding the output of the decoder is a list consisting of some codewords, and correct decoding means that the actually transmitted codeword appears in the list. It is natural that if the received vector is close to a codeword, such a list is short, but otherwise the list is longer. We therefore want the size of the list to be a function of the distances between the received vector and the codewords.

Many constructions for usual codes can be generalized to weighted coverings. Consider, for instance, the matrix construction of Section 3.5. Let  $\mathbf{A} = (\mathbf{I}_k, \mathbf{D})$  be a  $k \times n$  matrix over  $\mathbb{F}_q$  and  $S$  a subset of  $\mathbb{F}_q^k$ . For all  $\mathbf{x} \in \mathbb{F}_q^k$ , we denote by  $f_i(\mathbf{x})$  the number of pairs  $(\mathbf{y}, \mathbf{s})$  such that  $\mathbf{y} \in \mathbb{F}_q^n$ ,  $w(\mathbf{y}) = i$ ,  $\mathbf{s} \in S$  and  $\mathbf{x} = \mathbf{Ay} + \mathbf{s}$ . Then the code  $C = \{\mathbf{c} \in \mathbb{F}_q^n : \mathbf{Ac} \in S\}$  is an  $\mathbf{m}$ -covering where  $\mathbf{m} = (m_0, m_1, \dots, m_n)$  if  $\sum_{i=0}^n f_i(\mathbf{x})m_i \geq 1$  for all  $\mathbf{x}$ . A number of other constructions for weighted coverings can be found in [155].

§13.2 Theorem 13.2.5 was originally proved for binary perfect codes by Lloyd [447]. For the history of the Lloyd theorem, see van Lint [437] and MacWilliams and Sloane [464]. Our proof of Theorem 13.2.5 is a modified version of the one given in Honkala and Tietäväinen [329]. Sometimes we are interested in configurations in which the same codeword may appear more than once; see, e.g., Chapter 14. It is clear that Theorem 13.2.5 also holds for such configurations.

§13.3 Theorem 13.3.4 is from Assmus and Mattson [23]; see also MacDonald [461]. The other results are from Cohen, Honkala, Litsyn and Mattson [155].

There are some partial results about the existence of  $q$ -ary nonlinear perfect weighted coverings with radius one in [155]. In particular, if there exists a perfect  $(m_0, m_1)$ -covering of length  $n$ , then there exists a perfect  $(m_0, m_1/s)$ -covering of length  $ns$ . It is also shown that if  $q$  is a prime and  $t$  is a power of  $q$ , then a perfect  $(a/t, 1/t)$ -covering exists in  $\mathbb{F}_q^n$  if and only if  $a \equiv t \pmod{q-1}$  and  $n = (tq^i - a)/(q-1)$  for some integer  $i > 0$ .

§13.4 For the relation between excess bounds and weighted coverings, see S. M. Johnson [354] and Zhang [704]. Theorem 13.4.2 was obtained for  $m_0 = \dots = m_R = 1$  by Calderbank and Sloane [114], and then generalized to arbitrary weights by Zhang and Lo [706].

The approach of Chapter 8 to upperbound the covering radius by a function of the dual distance can also be seen as an application of weighted cov-

erings. Indeed, if there exists an  $m$ -covering with positive weights of radius  $r$ , then  $r$  is an upper bound on  $R$ .

This Page Intentionally Left Blank

# Chapter 14

## Multiple coverings

In this chapter we study two special types of weighted coverings. A code with the property that every vector in the Hamming space is covered at least a given number of times is called a *multiple covering*. Such codes provide a natural generalization of the usual covering codes whose covering radius is at most a prescribed integer — in the same way as designs generalize Steiner systems. Many of the results for the usual 1-fold coverings can be generalized, but much less is known about the general class of multiple coverings.

We now also consider configurations where the same codeword appears more than once. We give a simple example where we obtain a smaller multiple covering by taking one codeword twice. Section 14.2 is devoted to the study of perfect multiple coverings. The Lloyd theorem for multiple coverings follows as a special case from the Lloyd theorem for weighted coverings proved in the previous chapter. For multiple coverings, there is also a partial converse to the Lloyd theorem. Most of the section discusses classification results for radii one and two. The concept of normality can be generalized to multiple coverings and is treated in Section 14.3. In Section 14.4 we discuss how several constructions of Chapter 3 can be used in the context of multiple coverings. In Section 14.5 we give tables of the best known bounds on multiple coverings.

The final section is devoted to a different problem. We require that all the vectors in the space are  $r$ -covered at least once and the points at distance  $r$  from the code are  $r$ -covered several times. We call such codes *multiple coverings of deep holes*. Tables of the best known upper bounds are given.

### 14.1 Definitions

We wish to find a collection of Hamming spheres of a given radius that cover the whole space a given number of times. We may find it useful to take the

same sphere more than once.

**Definition 14.1.1** A collection  $C$  of  $K$  (not necessarily distinct)  $q$ -ary words  $\mathbf{c}_1, \mathbf{c}_2, \dots, \mathbf{c}_K$  form a  $q$ -ary  $(n, K, r, \mu)$  multiple covering with repeated words, or a  $q$ -ary  $(n, K, r, \mu)$  MCR for short, if for every  $q$ -ary vector  $\mathbf{x}$  of length  $n$ ,

$$d(\mathbf{x}, \mathbf{c}_i) \leq r \text{ for at least } \mu \text{ of the indices } i = 1, 2, \dots, K.$$

The minimum cardinality of a  $q$ -ary  $(n, \cdot, r, \mu)$  MCR is denoted by  $\overline{K}_q(n, r, \mu)$ . If all the  $K$  words are different, then  $C$  is called a  $q$ -ary  $(n, K, r, \mu)$  multiple covering, or a  $q$ -ary  $(n, K, r, \mu)$  MC for short. The minimum cardinality of a  $q$ -ary  $(n, \cdot, r, \mu)$  MC is denoted by  $K_q(n, r, \mu)$ . As usual, if  $q = 2$ , the subscripts are often omitted.

In fact, we shall be dealing almost exclusively with codes, i.e., require that no codeword appears more than once in  $C$ . We call an  $(n, K, r, \mu)$  MC a  $\mu$ -fold  $r$ -covering.

In terms of weighted coverings, an  $(n, K, r, \mu)$  MC is simply an  $\mathbf{m}$ -covering with  $\mathbf{m} = (1/\mu, 1/\mu, \dots, 1/\mu, 0, 0, \dots, 0)$  where  $1/\mu$  occurs  $r + 1$  times.

A natural way of obtaining an MC is to take a union of disjoint translates of a 1-fold covering. However, as we shall see, we can often do much better.

The basic sphere-covering bound for  $K_q(n, r, \mu)$  and  $\overline{K}_q(n, r, \mu)$  is

$$K_q(n, r, \mu) \geq \overline{K}_q(n, r, \mu) \geq \frac{\mu q^n}{\sum_{i=0}^r \binom{n}{i} (q-1)^i}.$$

An MC or an MCR attaining this bound is called *perfect*.

As in Section 6.2 this bound can be slightly improved by considering separately how the vectors that begin with 0 and the vectors that begin with 1 are covered.

**Example 14.1.2** By the sphere-covering bound  $\overline{K}(4, 1, 4) \geq 13$ . If  $C$  is a binary  $(4, 13, 1, 4)$  MCR, then, without loss of generality, there are at most six codewords in  $C$  that begin with 0. We now check how the vectors that begin with 0 are covered. Each codeword that begins with 0 covers four such vectors, and a codeword that begins with 1 covers only one such vector. Therefore all the eight vectors that begin with 0 are not covered four times, because  $6 \cdot 4 + 7 \cdot 1 = 31 < 32$ . Hence  $\overline{K}(4, 1, 4) \geq 14$ . In fact, choosing  $C = \mathbb{F}^4 \setminus \{0000, 1111\}$  we see that  $K(4, 1, 4) = \overline{K}(4, 1, 4) = 14$ .  $\square$

We can also study how the vectors of different weights in the space are covered.

**Example 14.1.3** Here we prove that  $K(4, 1, 2) = 8$  whereas  $\overline{K}(4, 1, 2) = 7$ . This shows that sometimes using the same codeword more than once really helps.

By the sphere-covering bound  $K(4, 1, 2) \geq \overline{K}(4, 1, 2) \geq 7$ . Assume that  $C$  is a binary  $(4, 7, 1, 2)$  MC. By taking a suitable translate of  $C$  if necessary we may assume that  $\mathcal{A}_0 = \mathcal{A}_4 = 0$ . When we consider how the vectors of weight 0, 1, 2, 3 and 4 in  $\mathbb{F}^4$  are covered we get the following inequalities:  $\mathcal{A}_1 \geq 2$ ,  $\mathcal{A}_1 + 2\mathcal{A}_2 \geq 8$ ,  $3\mathcal{A}_1 + \mathcal{A}_2 + 3\mathcal{A}_3 \geq 12$ ,  $\mathcal{A}_3 + 2\mathcal{A}_2 \geq 8$ , and  $\mathcal{A}_3 \geq 2$ . Trivially,  $\mathcal{A}_1 + \mathcal{A}_2 + \mathcal{A}_3 = 7$ . By adding the second and fourth inequalities we get  $\mathcal{A}_1 + \mathcal{A}_3 \leq 4$  and hence  $\mathcal{A}_1 = \mathcal{A}_3 = 2$  by the first and last inequalities, and  $\mathcal{A}_2 = 3$ . Without loss of generality the codewords of weight one in  $C$  are 0001 and 0010. Because  $\mathcal{A}_2 = 3$  and every vector of weight one is covered by exactly two codewords (by the argument leading to the second inequality), exactly one of the codewords of weight two has 1 in the last coordinate; without loss of generality this codeword is 0101 (if it were 0011, the other two codewords of weight two both would have to be 1100). Similarly, there is a codeword of weight two that has 1 in the third coordinate, and it has to be 1010. Then the remaining codeword of weight two can only be 1100. The five codewords that we know so far cover twice every vector of  $\mathbb{F}^4$  of weight two, except 1100, 1001 and 0110 which are only covered once. One of the two remaining codewords (both of which have weight three) has to cover two of them, i.e., 1110 or 1101 is a codeword. But in either case 1011 and 0111 still remain to be covered by the last remaining codeword, a contradiction. Hence  $K(4, 1, 2) \geq 8$ . The direct sum of the codes  $\{0, 1\}$  and  $\{000, 111, 001, 110\}$  is a  $(4, 8, 1, 2)$  MC proving that  $K(4, 1, 2) = 8$ .

However, if the same codeword may appear more than once we can do better: the words 0001, 0010, 0011, 1100, 1100, 0111, 1011 form a  $(4, 7, 1, 2)$  MCR proving that  $\overline{K}(4, 1, 2) = 7$ .  $\square$

## 14.2 Perfect multiple coverings

In this section we discuss what is known about the existence of perfect multiple coverings (PMC).

Assume that  $C$  is a  $q$ -ary  $(n, K, r, \mu)$  PMC. Because  $C$  attains the sphere-covering bound,

$$KV_q(n, r) = \mu q^n.$$

We say that a multiple covering  $C \subseteq \mathbb{Z}_q^n$  is *trivial* if  $C = \mathbb{Z}_q^n$ . By the Lloyd theorem for weighted coverings, we know that if there is a nontrivial

$q$ -ary  $(n, K, r, \mu)$  PMC, then the (generalized) Lloyd polynomial

$$L_r(x) = \frac{1}{\mu} \sum_{i=0}^r P_i(x)$$

has an integer zero in  $\{1, 2, \dots, n\}$ . Whether or not such a zero exists depends only on  $q$ ,  $n$  and  $r$  and not on  $\mu$ .

For multiple coverings, we have a partial converse to the Lloyd theorem. Namely, if for given  $q$ ,  $n$  and  $r$ , the Lloyd polynomial has a zero in  $\{1, 2, \dots, n\}$ , then for *some*  $\mu$  there is a nontrivial  $q$ -ary  $(n, \cdot, r, \mu)$  PMC. Notice that if  $C \subseteq \mathbb{Z}_q^n$  is a  $q$ -ary  $(n, K, r, \mu)$  PMC, then the code  $\mathbb{Z}_q^n \setminus C$  is a  $q$ -ary  $(n, q^n - K, r, V_q(n, r) - \mu)$  PMC.

**Theorem 14.2.1** *If the Lloyd polynomial  $L_r(x)$  has a zero in  $\{1, 2, \dots, n\}$ , then there exists a  $q$ -ary  $(n, q^{n-1}, r, V_q(n, r)/q)$  PMC.*

**Proof.** Assume that  $m \in \{1, 2, \dots, n\}$  satisfies  $L_r(m) = 0$ . Define

$$C_a = \{\mathbf{x} \in \mathbb{Z}_q^n : x_1 + \dots + x_m = a\}$$

for all  $a \in \mathbb{Z}_q$ . We claim that  $C_0$  is as required.

Denote  $\varphi_a(\mathbf{x}) = |B_r(\mathbf{x}) \cap C_a|$ . In other words,  $\varphi_a(\mathbf{x})$  is the number of vectors of weight at most  $r$  in the set  $-\mathbf{x} + C_a$ . If  $\mathbf{x} \in C_a$ , then  $-\mathbf{x} + C_0 = C_{-a}$  and hence  $\varphi_0(\mathbf{x}) = \varphi_{-a}(\mathbf{0})$ . It therefore suffices to show that  $\varphi_a(\mathbf{0})$  is independent of  $a$ .

Consider the equation  $y_1 + y_2 + \dots + y_j = a$  where  $a \in \mathbb{Z}_q$ . The number of solutions such that some given  $i < j$  variables are zero is equal to  $q^{j-i-1}$ . By the principle of inclusion and exclusion, the number of solutions such that  $y_1, y_2, \dots, y_j$  are all nonzero is equal to

$$\nu_j = \frac{1}{q} \left( q^j - \binom{j}{1} q^{j-1} + \dots + (-1)^{j-1} \binom{j}{j-1} q \right)$$

if  $a \neq 0$ ; and  $\nu_j + (-1)^j$  if  $a = 0$ . Therefore  $\varphi_a(\mathbf{0}) = \varphi_b(\mathbf{0})$  for all  $a, b \in \mathbb{Z}_q \setminus \{0\}$ , and for any nonzero  $a$  we have

$$\begin{aligned} \varphi_0(\mathbf{0}) - \varphi_a(\mathbf{0}) &= \sum_{k=0}^r \sum_{j=0}^k \binom{m}{j} \binom{n-m}{k-j} (q-1)^{k-j} (\nu_j + (-1)^j - \nu_j) \\ &= \sum_{k=0}^r P_k(m) \\ &= \mu L_r(m) \end{aligned}$$

which is zero by assumption. □

Therefore there exists a nontrivial  $q$ -ary  $(n, \cdot, r, \mu)$  PMC for at least one value of  $\mu$  if and only if the Lloyd polynomial  $L_r(x)$  has an integer zero in the set  $\{1, 2, \dots, n\}$ . By (2.3.10),  $L_r(x) = \frac{1}{\mu} P_r^{n-1}(x-1)$ , and the problem hence reduces to studying integer zeros of Krawtchouk polynomials.

**Theorem 14.2.2** *Suppose  $q > 1$  and  $r$  are positive integers. Then there is a nontrivial  $q$ -ary  $(qr+1, q^{qr}, r, \mu)$  PMC with  $\mu = V_q(n, r)/q$ .*

**Proof.** A direct calculation shows that

$$L_r(qr) = \frac{1}{\mu} P_r^{qr}(qr-1) = \frac{(-1)^r}{\mu} \left( \binom{qr-1}{r} - (q-1) \binom{qr-1}{r-1} \right) = 0$$

and the result follows from the previous theorem.  $\square$

**Example 14.2.3** If  $r = 1$ , a nontrivial  $q$ -ary  $(n, \cdot, 1, \mu)$  PMC exists for at least one value of  $\mu$  if and only if  $L_1(x) = P_1^{n-1}(x-1) = (nq - n + 1) - qx$  has an integer zero in the set  $\{1, 2, \dots, n\}$ , i.e.,  $n \equiv 1 \pmod{q}$ .  $\square$

In the case  $r = 1$  we have already classified all linear PMC in Theorems 13.3.3 and 13.3.6: if  $q$  is a prime power, a  $q$ -ary perfect linear  $(n, \cdot, 1, \mu)$  MC exists if and only if  $n = (\mu q^i - 1)/(q-1)$  for some integer  $i \geq 0$ .

If  $q$  is a prime, we do not even need to assume linearity to obtain all the parameters for which a  $q$ -ary  $(n, K, r, \mu)$  PMC exists.

**Theorem 14.2.4** *Assume that  $q$  is a prime. A  $q$ -ary  $(n, \cdot, 1, \mu)$  PMC exists if and only if there are integers  $i \geq 0$ ,  $\mu_0 > 0$  such that  $\mu_0 \mid \mu$ ,  $\mu \leq q^i \mu_0$  and  $n = (\mu_0 q^i - 1)/(q-1)$ .*

**Proof.** If a  $q$ -ary  $(n, K, 1, \mu)$  PMC exists, then by the sphere-covering bound  $K(1 + (q-1)n) = \mu q^n$  and hence  $1 + (q-1)n = \mu_0 q^i$  for some integers  $i \geq 0$  and  $\mu_0 > 0$  such that  $\mu_0 \mid \mu$ . Then  $\mu_0 q^i = \mu q^n / K \geq \mu$ .

Conversely, we know that there is a linear  $(n, \cdot, 1, \mu_0)$  PMC and its dimension is  $n - i$ . The union of any  $\mu/\mu_0$  cosets of this code gives the required PMC.  $\square$

We now consider binary linear perfect multiple 2-coverings. Assume that  $C$  is a binary linear  $[n, k]$  code which is a perfect  $\mu$ -fold covering.

Assume further that the number  $s^\perp$  of nonzero weights in the dual code of  $C$  is one. The Lloyd polynomial  $L_2(x)$  of  $C$  satisfies

$$\mu L_2(x) = 2x^2 - 2(n+1)x + \frac{1}{2}(n^2 + n + 2).$$

By the Lloyd theorem, the right hand side has an integer root. But the sum of the roots is  $n + 1$ , and so both roots are integers, given by

$$\frac{1}{2}(n + 1 \pm \sqrt{n - 1}) = 1 + \frac{\lambda^2 \pm \lambda}{2},$$

where

$$n = 1 + \lambda^2$$

for some integer  $\lambda$ .

Because  $s^\perp = 1$ , we know by Theorem 13.3.4 that  $C$  has a parity check matrix

$$\mathbf{H} = (\mathbf{G}_1, \mathbf{G}_2, \dots, \mathbf{G}_t, \mathbf{0}), \quad (14.2.5)$$

where each  $\mathbf{G}_j$  is an  $i \times (2^i - 1)$  generator matrix of the  $i$ -dimensional simplex code and  $\mathbf{0}$  is the  $i \times \ell$  zero matrix for some  $\ell \geq 0$ . By allowing  $\lambda$  to take both negative and positive values, we may assume that  $w$ , the only nonzero weight in  $C^\perp$ , satisfies  $w = 1 + (\lambda^2 - \lambda)/2$ . Furthermore,  $w = t2^{i-1}$ , because all nonzero codewords in the  $i$ -dimensional simplex code have weight  $2^{i-1}$ . We get the equations

$$\begin{aligned} n &= 1 + \lambda^2 = t(2^i - 1) + \ell, \\ 2w &= \lambda^2 - \lambda + 2 = t2^i, \end{aligned}$$

and

$$n - 2w = \lambda - 1 = \ell - t.$$

We can now prove the following result.

**Theorem 14.2.6** *Let  $\lambda$  be any integer. Define  $n = 1 + \lambda^2$ , and let  $i \geq 1$  and  $t \geq 1$  be any integers satisfying  $\lambda^2 - \lambda + 2 = t2^i$ . If  $\ell = t + \lambda - 1$  is nonnegative, then the  $[n, n - i]$  code with parity check matrix (14.2.5) is a perfect multiple 2-covering. No other perfect binary linear multiple 2-coverings with  $s^\perp = 1$  exist.*

**Proof.** We have already proved the necessity of the conditions.

It remains to prove that if the conditions hold, then the code with parity check matrix  $\mathbf{H}$  in (14.2.5) with  $\ell = t + \lambda - 1$  is a perfect multiple 2-covering.

The number of codewords  $\mathcal{A}_i(\mathbf{x})$  that have distance  $i$  to a vector  $\mathbf{x}$  equals the number of times the syndrome  $\mathbf{H}\mathbf{x}^T$  can be written as a sum of exactly  $i$  columns of  $\mathbf{H}$ .

If  $\mathbf{x} \in C$ , then its syndrome is the zero vector. Trivially  $\mathcal{A}_0(\mathbf{x}) = 1$  and  $\mathcal{A}_1(\mathbf{x}) = \ell$ . The zero vector can be obtained as a sum of exactly two columns by taking any two identical columns, and hence  $\mathcal{A}_2(\mathbf{x}) = \binom{t}{2}(2^i - 1) + \binom{\ell}{2}$ . Therefore each codeword is within distance two from exactly  $N_0 := 1 + \ell + \binom{t}{2}(2^i - 1) + \binom{\ell}{2}$  codewords.

If  $\mathbf{x} \notin C$ , then its syndrome  $\mathbf{s}$  is nonzero. It occurs  $t$  times as a column in  $\mathbf{H}$ . Thus  $\mathcal{A}_1(\mathbf{x}) = t$ . Furthermore, there are  $\ell$  zero columns and  $t\ell$  ways of obtaining  $\mathbf{s}$  as a sum of a zero column and a nonzero column. The set of all  $2^i - 1$  nonzero columns can be partitioned into the set  $\{\mathbf{s}\}$  and  $2^{i-1} - 1$  sets  $\{\mathbf{u}, \mathbf{s} + \mathbf{u}\}$  whose elements add up to  $\mathbf{s}$ . Each nonzero column occurs  $t$  times in  $\mathbf{H}$  and therefore there are  $(2^{i-1} - 1)t^2$  ways of obtaining  $\mathbf{s}$  as a sum of two nonzero columns of  $\mathbf{H}$ . All in all,  $\mathcal{A}_2(\mathbf{x}) = (2^{i-1} - 1)t^2 + t\ell$ , and therefore each non-codeword is within distance two from exactly  $N_1 := t + (2^{i-1} - 1)t^2 + t\ell$  codewords.

A routine calculation shows that  $2N_0 - 2N_1 = t^2 - t(2^i + 1 + 2\ell) + (\ell^2 + \ell + 2) = (\ell - t)^2 + 2(\ell - t) + 2 - n = (\lambda - 1)^2 + 2(\lambda - 1) + 2 - n = 0$  completing the proof.  $\square$

In fact, all the PMC in the previous theorem have minimum distance one with only one exception.

**Theorem 14.2.7** *The only perfect binary linear multiple 2-covering with  $\mathbf{s}^\perp = 1$  and  $d = 2$  is the  $[2, 1, 2]$  code.*

**Proof.** Using the previous notations  $d = 2$  only if  $\ell = 0$ , and then  $t(2^i - 1) = 1 + \lambda^2$ . If  $i \geq 2$  this equation has no integer solutions. Namely, if  $p$  is a prime dividing  $2^i - 1$  then  $-1$  is a quadratic residue mod  $p$  and hence  $p \equiv 1 \pmod{4}$ . Applying this to every prime factor of  $2^i - 1$  yields  $2^i - 1 \equiv 1 \pmod{4}$ , a contradiction. Therefore  $i = 1$  and  $C$  has to be the  $[n, n - 1, 2]$  code with  $n = 2$ .  $\square$

The following theorems show that a code can be a PMC for several different values of  $\mu$ .

**Theorem 14.2.8** *If  $C$  is a binary perfect  $(n, K, 1, \mu)$  MC and  $r$  is odd, then  $C$  is also a perfect  $(n, K, r, \mu V(n, r)/V(n, 1))$  MC.*

**Proof.** The proof is by induction on  $r$ . Assume that  $r \geq 3$  and we already know that  $C$  is a perfect  $(n, K, r - 2, \cdot)$  MC. This means that the quantity  $|B_{r-2}(\mathbf{x}) \cap C|$  is independent of  $\mathbf{x} \in \mathbb{F}^n$ . Consider the sum

$$S(\mathbf{x}) = \sum_{\mathbf{y} \in B_{r-1}(\mathbf{x})} |B_1(\mathbf{y}) \cap C|.$$

Since  $C$  is a perfect  $(n, K, 1, \mu)$  MC, each summand  $|B_1(\mathbf{y}) \cap C|$  is equal to  $\mu$ , and so  $S(\mathbf{x}) = V(n, r - 1)\mu$  independently of  $\mathbf{x}$ . If  $\mathbf{c} \in C$  has distance  $r - 1$  or  $r$  to  $\mathbf{x}$ , then  $|B_{r-1}(\mathbf{x}) \cap B_1(\mathbf{c})| = r$ , and therefore  $\mathbf{c}$  contributes 1 to exactly  $r$  of the summands. If  $d(\mathbf{c}, \mathbf{x}) \leq r - 2$ , then  $|B_{r-1}(\mathbf{x}) \cap B_1(\mathbf{c})| = n + 1$ , and  $\mathbf{c}$

contributes 1 to  $n + 1$  of the summands. Other codewords do not contribute to the sum. Therefore

$$S(\mathbf{x}) = (n + 1)|B_{r-2}(\mathbf{x}) \cap C| + r|(B_r(\mathbf{x}) \setminus B_{r-2}(\mathbf{x})) \cap C|.$$

Because  $S(\mathbf{x})$  and  $|B_{r-2}(\mathbf{x}) \cap C|$  are independent of  $\mathbf{x}$ , so is  $|(B_r(\mathbf{x}) \setminus B_{r-2}(\mathbf{x})) \cap C|$  and consequently  $|B_r(\mathbf{x}) \cap C| = |B_{r-2}(\mathbf{x}) \cap C| + |(B_r(\mathbf{x}) \setminus B_{r-2}(\mathbf{x})) \cap C|$ .

We know that each vector in the space is  $r$ -covered by the same number of codewords, say  $\mu'$ . Therefore  $\mu'2^n = KV(n, r)$ , and  $\mu2^n = KV(n, 1)$ , from which we obtain  $\mu' = \mu V(n, r)/V(n, 1)$ .  $\square$

**Theorem 14.2.9** *Every binary perfect  $(n, K, r, \mu)$  MC is also a perfect  $(n, K, n - r - 1, K - \mu)$  MC.*

**Proof.** Complement all the words of a binary  $(n, K, r, \mu)$  PMC. Since every vector is either within distance  $r$  from  $\mathbf{c}$  or within distance  $n - r - 1$  from the complement of  $\mathbf{c}$ , the resulting code  $C'$  is an  $(n, K, n - r - 1, K - \mu)$  PMC. Being a translate of  $C'$ , the code  $C$  itself is also an  $(n, K, n - r - 1, K - \mu)$  PMC.  $\square$

### 14.3 Normality of multiple coverings

In the remainder of this chapter we only consider the binary case. The concept of normality and subnormality can be generalized to multiple coverings. When dealing with  $\mu$ -fold coverings it is natural to be interested not just in the distance  $d(\mathbf{x}, C)$ , but in all the  $\mu$  smallest distances from  $\mathbf{x}$  to the nearest codewords. Assume therefore that  $\mathbf{x} \in \mathbb{F}^n$  is given and that the codewords  $\mathbf{c}_1, \mathbf{c}_2, \dots, \mathbf{c}_K$  of  $C$  are indexed so that

$$d(\mathbf{x}, \mathbf{c}_1) \leq d(\mathbf{x}, \mathbf{c}_2) \leq \dots \leq d(\mathbf{x}, \mathbf{c}_K).$$

We then denote

$$d^t(\mathbf{x}, C) = d(\mathbf{x}, \mathbf{c}_t).$$

Thus,  $d^t(\mathbf{x}, C)$  is the  $t$ -th smallest of the distances between  $\mathbf{x}$  and the codewords of  $C$ . If  $t > K$ , then we define  $d^t(\mathbf{x}, C) = \infty$ .

The  $\mu$ -fold covering radius  $R^\mu(C)$  of  $C$  is defined to be the smallest integer  $r$  such that

$$d^\mu(\mathbf{x}, C) \leq r \text{ for all } \mathbf{x} \in \mathbb{F}^n.$$

The following two definitions show how normality and subnormality can be generalized in a natural way to multiple coverings.

**Definition 14.3.1** Suppose  $C$  is a binary  $(n, K)$  code. We say that  $C$  has  $\mu$ -fold subnorm  $S$  if there is a partition  $C_1 \cup C_2$  of  $C$  such that

$$d^i(\mathbf{x}, C_1) + d^{\mu+1-i}(\mathbf{x}, C_2) \leq S \text{ for all } i = 1, 2, \dots, \mu \text{ and } \mathbf{x} \in \mathbb{F}^n.$$

If  $C$  has  $\mu$ -fold subnorm  $2r+1$  we say that  $C$  is a subnormal  $\mu$ -fold  $r$ -covering. If  $C$  is a subnormal  $\mu$ -fold  $R^\mu(C)$ -covering then  $C$  is called  $\mu$ -fold subnormal.

If  $C$  has  $\mu$ -fold subnorm  $2r+1$ , then  $C$  is indeed a  $\mu$ -fold  $r$ -covering: for every  $\mathbf{x} \in \mathbb{F}^n$  and  $i = 1, 2, \dots, \mu$ , we have  $d^i(\mathbf{x}, C_1) \leq r$  or  $d^{\mu+1-i}(\mathbf{x}, C_2) \leq r$ , and hence if  $|B_r(\mathbf{x}) \cap C_1| = t$  then  $|B_r(\mathbf{x}) \cap C_2| \geq \mu - t$ .

**Definition 14.3.2** Suppose  $C$  is a binary  $(n, K)$  code. We say that  $C$  has  $\mu$ -fold norm  $N$  if there is an index  $i$  such that

$$d^j(\mathbf{x}, C_0^{(i)}) + d^{\mu+1-j}(\mathbf{x}, C_1^{(i)}) \leq N \text{ for all } j = 1, 2, \dots, \mu \text{ and } \mathbf{x} \in \mathbb{F}^n.$$

If  $C$  has  $\mu$ -fold norm  $2r+1$  we say that  $C$  is a normal  $\mu$ -fold  $r$ -covering. If  $C$  is a normal  $\mu$ -fold  $R^\mu(C)$ -covering then  $C$  is called  $\mu$ -fold normal.

As usual, a partition  $C_1 \cup C_2$  in Definition 14.3.1 (respectively, a coordinate  $i$  in Definition 14.3.2) is called *acceptable*, if it can be used to show that  $C$  is a subnormal (respectively, normal)  $\mu$ -fold  $r$ -covering.

A code  $C$  is 1-fold (sub)normal if and only if it is (sub)normal.

The following theorem shows how the ADS construction can be applied to multiple coverings, and motivates the previous definitions.

**Theorem 14.3.3** Suppose that an  $(n_A, K_A)$  code  $A$  is a subnormal  $\mu_A$ -fold  $r_A$ -covering with the partition  $A_1 \cup A_2$  acceptable, and that an  $(n_B, K_B)$  code  $B$  is a normal  $\mu_B$ -fold  $r_B$ -covering with the first coordinate acceptable. Then the ADS of  $A$  and  $B$

$$A \dot{\oplus} B = \{(\mathbf{a}, \mathbf{b}) : \mathbf{a} \in A_1, (0, \mathbf{b}) \in B\} \cup \{(\mathbf{a}, \mathbf{b}) : \mathbf{a} \in A_2, (1, \mathbf{b}) \in B\}$$

is an  $(n_A + n_B - 1, K)$  code which is a subnormal  $\mu_A \mu_B$ -fold  $(r_A + r_B)$ -covering, where  $K = |A_1||B_0^{(1)}| + |A_2||B_1^{(1)}|$ . If, moreover,  $A$  is a normal  $\mu_A$ -fold  $r_A$ -covering with the last coordinate acceptable and we choose  $A_1 = A_0^{(n_A)}$  and  $A_2 = A_1^{(n_A)}$ , then  $A \dot{\oplus} B$  is a normal  $\mu_A \mu_B$ -fold  $(r_A + r_B)$ -covering.

**Proof.** Denote  $C = A \dot{\oplus} B$ , and  $C_1 = \{(\mathbf{a}, \mathbf{b}) : \mathbf{a} \in A_1, (0, \mathbf{b}) \in B\}$  and  $C_2 = \{(\mathbf{a}, \mathbf{b}) : \mathbf{a} \in A_2, (1, \mathbf{b}) \in B\}$ . Let  $\mathbf{x} \in \mathbb{F}^{n_A}$  and  $\mathbf{y} \in \mathbb{F}^{n_B-1}$  be arbitrary. By Definitions 14.3.1 and 14.3.2 we can find different words  $\mathbf{a}_1, \mathbf{a}_2, \dots, \mathbf{a}_{\mu_A} \in A_1$ ,  $\mathbf{a}'_1, \mathbf{a}'_2, \dots, \mathbf{a}'_{\mu_A} \in A_2$  and different words  $(0, \mathbf{b}_1), (0, \mathbf{b}_2), \dots, (0, \mathbf{b}_{\mu_B}) \in B_0^{(1)}$ ,  $(1, \mathbf{b}'_1), (1, \mathbf{b}'_2), \dots, (1, \mathbf{b}'_{\mu_B}) \in B_1^{(1)}$  such that

$$d(\mathbf{a}_i, \mathbf{x}) + d(\mathbf{a}'_i, \mathbf{x}) \leq 2r_A + 1$$

for all  $i = 1, 2, \dots, \mu_A$ , and

$$d((0, \mathbf{b}_j), (0, \mathbf{y})) + d((1, \mathbf{b}'_j), (0, \mathbf{y})) \leq 2r_B + 1$$

for all  $j = 1, 2, \dots, \mu_B$ . Consequently, if we choose

$$\mathbf{c}_{i,j} = (\mathbf{a}_i, \mathbf{b}_j) \in C_1 \text{ and } \mathbf{c}'_{i,j} = (\mathbf{a}'_i, \mathbf{b}'_j) \in C_2,$$

then we have

$$\begin{aligned} & d(\mathbf{c}_{i,j}, (\mathbf{x}, \mathbf{y})) + d(\mathbf{c}'_{i,j}, (\mathbf{x}, \mathbf{y})) \\ & \leq d(\mathbf{a}_i, \mathbf{x}) + d((0, \mathbf{b}_j), (0, \mathbf{y})) + d(\mathbf{a}'_i, \mathbf{x}) + d((1, \mathbf{b}'_j), (0, \mathbf{y})) - 1 \\ & \leq (d(\mathbf{a}_i, \mathbf{x}) + d(\mathbf{a}'_i, \mathbf{x})) + (d((0, \mathbf{b}_j), (0, \mathbf{y})) + d((1, \mathbf{b}'_j), (0, \mathbf{y}))) - 1 \\ & \leq 2r_A + 1 + 2r_B + 1 - 1 \\ & = 2(r_A + r_B) + 1, \end{aligned}$$

which proves the first claim. The second claim is now immediate.  $\square$

**Corollary 14.3.4** *Assume that an  $[n_A, k_A]$  code  $A$  is a normal  $\mu_A$ -fold  $r_A$ -covering with the last coordinate acceptable and an  $[n_B, k_B]$  code  $B$  is a normal  $\mu_B$ -fold  $r_B$ -covering with the first coordinate acceptable. Then there is an  $[n_A + n_B - 1, k_A + k_B - 1]$  code  $A \dot{\oplus} B$  that is a normal  $\mu_A \mu_B$ -fold  $(r_A + r_B)$ -covering.*  $\square$

By definition, a  $\mu$ -fold (sub)normal code has at least  $2\mu$  codewords. For example, the code  $\mathbb{F}^{2r}$  is a  $\mu$ -fold  $r$ -covering for

$$\mu = \sum_{i=0}^r \binom{2r}{i} > K/2,$$

where  $K = 2^{2r}$  is the number of codewords. Therefore this code is not  $\mu$ -fold (sub)normal.

The proof of the following theorem is long and tedious, and is omitted; see Honkala [318].

**Theorem 14.3.5** *If  $r \leq 2$  and a binary  $[n, k]$  code  $C$  is a  $\mu$ -fold  $r$ -covering with  $n \geq 2r + 1$ , then  $C$  is  $\mu$ -fold normal.*  $\square$

## 14.4 Constructions

Many constructions presented in Chapter 3 naturally carry over to multiple coverings.

Recall that a piecewise constant code of length  $n_1 + n_2 + \dots + n_i$  consists of all the vectors  $(\mathbf{c}_1, \mathbf{c}_2, \dots, \mathbf{c}_i)$  such that  $(w(\mathbf{c}_1), w(\mathbf{c}_2), \dots, w(\mathbf{c}_i)) \in W$ , where  $\mathbf{c}_j \in \mathbb{F}^{n_j}$  and  $W$  is a given subset of  $\mathbb{N}^i$ .

**Example 14.4.1** Choose  $n_1 = 4$ ,  $n_2 = 2$  and take as codewords all the binary vectors  $(\mathbf{c}_1, \mathbf{c}_2) \in \mathbb{F}^6$  such that  $\mathbf{c}_1 \in \mathbb{F}^4$ ,  $\mathbf{c}_2 \in \mathbb{F}^2$  and  $(w(\mathbf{c}_1), w(\mathbf{c}_2))$  is one of the pairs  $(0,0), (0,1), (0,2), (1,0), (1,1), (1,2), (3,0), (3,1), (3,2), (4,0), (4,1), (4,2)$ . It is easy to verify that these 40 words form a  $(6, 40, 1, 4)$  MC.  $\square$

The matrix construction is also well suited for multiple coverings. In the following discussion all the vectors are assumed to be column vectors. Let  $\mathbf{A} = (\mathbf{I}_k, \mathbf{D}) = (\mathbf{a}_1, \mathbf{a}_2, \dots, \mathbf{a}_n)$  be a binary  $k \times n$  matrix where  $\mathbf{I}_k$  is the identity matrix. Suppose  $\mathbf{s}_1, \mathbf{s}_2, \dots, \mathbf{s}_t$  are distinct vectors in  $\mathbb{F}^k$ . We say that they form a  $\mu$ -fold  $r$ -covering of  $\mathbb{F}^k$  using  $\mathbf{A}$  if every  $\mathbf{x} \in \mathbb{F}^k$  can be represented in at least  $\mu$  different ways as a sum of exactly one  $\mathbf{s}_j$  and at most  $r$  of the columns  $\mathbf{a}_i$ . In other words, for each  $\mathbf{x} \in \mathbb{F}^k$  we require that the cardinality of the set  $\{(j, \mathbf{y}) : j \in \{1, 2, \dots, t\}, \mathbf{y} \in \mathbb{F}^n, w(\mathbf{y}) \leq r, \mathbf{x} = \mathbf{A}\mathbf{y} + \mathbf{s}_j\}$  is at least  $\mu$ . Then we easily obtain the following generalization of Theorem 3.5.1.

**Theorem 14.4.2** *If  $\mathbf{s}_1, \mathbf{s}_2, \dots, \mathbf{s}_t$  form a  $\mu$ -fold  $r$ -covering of  $\mathbb{F}^k$  using  $\mathbf{A}$ , and  $C_j = \{\mathbf{y} \in \mathbb{F}^n : \mathbf{A}\mathbf{y} = \mathbf{s}_j\}$ , then the union  $C = C_1 \cup C_2 \cup \dots \cup C_t$  is an  $(n, t2^{n-k}, r, \mu)$  MC.*

**Proof.** Let  $\mathbf{z} \in \mathbb{F}^n$  be arbitrary. The vector  $\mathbf{x} = \mathbf{A}\mathbf{z}$  can be represented as a sum  $\mathbf{x} = \mathbf{A}\mathbf{y} + \mathbf{s}_j$  for at least  $\mu$  different pairs  $(j, \mathbf{y})$  such that  $w(\mathbf{y}) \leq r$ . Then  $\mathbf{z} + \mathbf{y} \in C_j$  and  $d(\mathbf{z} + \mathbf{y}, \mathbf{z}) \leq r$ . Because there are  $\mu$  different representations and the sets  $C_j$  are disjoint,  $C$  is an  $(n, t2^{n-k}, r, \mu)$  MC.  $\square$

**Theorem 14.4.3**  $K(2n + 1, 1, \mu) \leq 2^n K(n, 1, \mu)$ .

**Proof.** If  $C$  is an  $(n, K, 1, \mu)$  MC, then in the proof of Theorem 3.4.3 we can instead of just one  $\mathbf{v}$  find  $\mu$  different codewords  $\mathbf{v}_1, \mathbf{v}_2, \dots, \mathbf{v}_\mu$  and apply the argument separately for each  $\mathbf{v}_i$ .  $\square$

**Example 14.4.4** The code  $C = \{00, 01, 11\}$  shows that  $K(2, 1, 2) \leq 3$ . Apply the construction of Theorem 3.4.3 to  $C$ . By the proof of Theorem 14.4.3 the resulting twelve codewords — which are listed in Example 1.1.10 — form a binary  $(5, 12, 1, 2)$  MC.  $\square$

**Theorem 14.4.5** Suppose  $C$  is an  $(n, K, r, \mu + 1)$  MC and  $C' \subseteq C$  has  $K'$  codewords and minimum distance at least  $2r + 1$ . Then  $C \setminus C'$  is an  $(n, K - K', r, \mu)$  MC.  $\square$

**Corollary 14.4.6**  $K(n, r, \mu + 1) \geq K(n, r, \mu) + A(n, 4r + 1)$ .

**Proof.** Suppose  $C$  is an  $(n, K, r, \mu + 1)$  MC with  $K = K(n, r, \mu + 1)$ . Every vector  $\mathbf{x}_i$  in a code of length  $n$ , minimum distance  $4r + 1$  and cardinality  $A(n, 4r + 1)$  is covered by some codeword  $\mathbf{c}_i \in C$ . Furthermore,  $d(\mathbf{x}_i, \mathbf{x}_j) \leq d(\mathbf{x}_i, \mathbf{c}_i) + d(\mathbf{c}_i, \mathbf{c}_j) + d(\mathbf{c}_j, \mathbf{x}_j)$  and hence  $d(\mathbf{c}_i, \mathbf{c}_j) \geq 4r + 1 - r - r = 2r + 1$ . The result now follows from the previous theorem by choosing  $C'$  to be the subcode formed by the  $A(n, 4r + 1)$  words  $\mathbf{c}_i$ .  $\square$

**Corollary 14.4.7**  $K(n, r, \mu + 1) > K(n, r, \mu)$ .  $\square$

## 14.5 Tables for multiple coverings

In Tables 14.1 – 14.4 we give the best known bounds on  $K(n, r, \mu)$  when  $n \leq 16$ ,  $r \leq 4$  and  $\mu \leq 4$ . Clearly,  $K(r, r, \mu) = \overline{K}(r, r, \mu) = \mu$  for every  $\mu \leq 2^r$ , and  $K(n, r, \mu) \geq \overline{K}(n, r, \mu) > \mu$  whenever  $n > r$ . Furthermore,  $K(r+1, r, \mu) = \overline{K}(r+1, r, \mu) = \mu + 1$  for every  $\mu \leq 2^{r+1} - 1$ . In fact, any  $\mu + 1$  different vectors in  $\mathbb{F}^{r+1}$  form an  $(r+1, \mu+1, r, \mu)$  MC. It is also easy to verify that  $K(n, r, \mu) = 3$  if and only if  $\mu = 2$  and  $r < n \leq \lceil 3r/2 \rceil$ ; or  $\mu = 3$  and  $n = r \geq 2$ .

### Key to Tables 14.1 – 14.4

All the bounds for  $\mu = 1$  are from Table 6.1.

The other lower bounds are by Hämäläinen, Honkala, Kaikonen and Litsyn [275].

L	linear code from [275]
M	matrix construction from [275]
N	matrix construction from Östergård [518]
P	$K(n+1, r, \mu) \leq 2K(n, r, \mu)$
Q	ADS
R	Theorem 14.4.3
S	piecewise constant code [275]
T	$K(n+1, r+1, \mu) \leq K(n, r, \mu)$
U	union of translates of a code with smaller $\mu$
X	miscellaneous constructions [275]
Z	[518]

Table 14.1: Bounds on  $K(n, 1, \mu)$ .

$n$	$\mu = 1$	$\mu = 2$	$\mu = 3$	$\mu = 4$
1	1	2		
2	2	3	4	
3	2	4 U	6 U	8 U
4	4	8 P	11 X	14 S
5	7	12 R	16 R	22 X
6	12	19 – 20 M	30 – 32 P	38 – 40 S
7	16	32 U	48 U	64 U
8	32	58 – 64 P	90 – 94 M	114 – 124 N
9	55 – 62	104 – 112 M	154 – 160 M	206 – 216 Z
10	105 – 120	187 – 216 N	289 – 316 N	374 – 408 N
11	178 – 192	342 – 368 N	512 R	684 – 704 R
12	342 – 380	631 – 704 N	972 – 1024 P	1262 – 1344 N
13	598 – 736	1172 – 1280 R	1756 – 1920 N	2342 – 2528 N
14	1172 – 1408	2186 – 2560 P	3356 – 3712 N	4370 – 4864 N
15	2048	4096 U	6144 U	8192 U
16	4096	7711 – 8192 P	11809 – 12288 P	15422 – 16384 P

Table 14.2: Bounds on  $K(n, 2, \mu)$ .

$n$	$\mu = 1$	$\mu = 2$	$\mu = 3$	$\mu = 4$
2	1	2	3	4
3	2	3	4	5
4	2	4 U	5 X	7 X
5	2	4 U	6 U	8 U
6	4	7 – 8 P	10 – 11 Q	12 – 14 Q
7	7	10 – 12 Q	14 – 16 Q	18 – 20 M
8	12	14 – 19 X	22 – 24 N	28 – 32 L
9	15 – 16	24 – 32 Q	34 – 44 M	46 – 56 M
10	23 – 30	40 – 48 M	56 – 64 L	74 – 88 M
11	36 – 44	62 – 64 L	92 – 100 N	123 – 128 U
12	61 – 78	108 – 128 P	156 – 192 M	212 – 256 P
13	97 – 128	190 – 240 N	268 – 336 N	360 – 448 M
14	157 – 256	310 – 448 M	464 – 640 M	619 – 768 M
15	309 – 384	557 – 768 M	814 – 1024 L	1105 – 1280 M
16	512 – 768	1008 – 1536 P	1436 – 2048 P	1932 – 2560 P

Table 14.3: Bounds on  $K(n, 3, \mu)$ .

$n$	$\mu = 1$	$\mu = 2$	$\mu = 3$	$\mu = 4$
3	1	2	3	4
4	2	3	4	5
5	2	3 X	4 X	6 X
6	2	4 U	6 U	7 X
7	2	4 U	6 U	8 U
8	4	7 – 8 P	9 – 11 Q	12 – 14 Q
9	7	8 – 12 Q	12 – 16 Q	16 – 20 Q
10	9 – 12	13 – 18 N	18 – 24 Q	24 – 30 N
11	12 – 16	18 – 24 N	27 – 36 N	36 – 48 M
12	18 – 28	29 – 48 P	42 – 60 M	56 – 76 M
13	28 – 42	44 – 64 Q	67 – 96 M	88 – 112 M
14	44 – 64	74 – 120 N	108 – 160 M	140 – 192 M
15	70 – 112	114 – 160 X	172 – 224 M	228 – 256 L
16	114 – 192	197 – 304 M	286 – 448 P	377 – 512 P

Table 14.4: Bounds on  $K(n, 4, \mu)$ .

$n$	$\mu = 1$	$\mu = 2$	$\mu = 3$	$\mu = 4$
4	1	2	3	4
5	2	3	4	5
6	2	3 T	4 T	5 X
7	2	4 U	5 X	7 T
8	2	4 U	6 U	8 U
9	2	4 U	6 U	8 U
10	4	6 – 8 P	8 – 11 Q	11 – 14 Q
11	7	8 – 12 Q	12 – 16 Q	15 – 20 Q
12	8 – 12	11 – 18 Q	16 – 24 Q	22 – 30 Q
13	11 – 16	16 – 26 N	23 – 36 Q	30 – 48 Q
14	15 – 28	23 – 48 Q	34 – 60 Q	46 – 72 M
15	22 – 32	36 – 64 Q	52 – 96 Q	68 – 112 M
16	33 – 64	54 – 112 M	80 – 128 L	105 – 188 M

## 14.6 Multiple coverings of deep holes

In this section we study objects that are closely related to multiple coverings.

**Definition 14.6.1** A binary  $(n, K)$  code  $C$  is called an  $(n, K, r, \mu)$  multiple covering of deep holes, multiple covering of the farthest-off points, or an  $(n, K, r, \mu)$  MCF for short, if the Hamming spheres of radius  $r$  centred at the codewords cover the whole space  $\mathbb{F}^n$  and if every  $\mathbf{x} \in \mathbb{F}^n$  such that  $d(\mathbf{x}, C) = r$  is covered by at least  $\mu$  codewords. The minimum possible cardinality of an  $(n, \cdot, r, \mu)$  MCF is denoted by  $F(n, r, \mu)$ .

Using the terminology of weighted coverings,  $C$  is an  $\mathbf{m}$ -covering with  $\mathbf{m} = (m_0, m_1, \dots, m_r)$ , where  $m_0 = \dots = m_{r-1} = 1, m_r = 1/\mu$ . The general results on weighted coverings therefore apply to MCF. The covering radius of an  $(n, K, r, \mu)$  MCF  $C$  is at most  $r$  and every  $\mathbf{x} \in \mathbb{F}^n$  for which  $d(\mathbf{x}, C) = r$  is covered by at least  $\mu$  codewords. It is therefore possible that there are actually no vectors  $\mathbf{x} \in \mathbb{F}^n$  whose distance from  $C$  is as large as  $r$ .

We now discuss several constructions for MCF. We again denote the sum (in  $\mathbb{F}$ ) of the coordinates of a vector  $\mathbf{x} \in \mathbb{F}^n$  by  $\pi(\mathbf{x})$ .

**Theorem 14.6.2** If  $C$  is an  $(n, K, r, \mu)$  MC, then the extended code  $\widehat{C} = \{(\mathbf{c}, \pi(\mathbf{c})) \in \mathbb{F}^{n+1} : \mathbf{c} \in C\}$  is an  $(n+1, K, r+1, \lceil \mu(n+1)/(r+1) \rceil)$  MCF.

**Proof.** Let  $\mathbf{x} \in \mathbb{F}^n, \mathbf{x}' \in \mathbb{F}$  be arbitrary. We assume that  $d((\mathbf{x}, \mathbf{x}'), \widehat{C}) = r+1$ , and show that  $(\mathbf{x}, \mathbf{x}')$  is covered by at least  $\mu(n+1)/(r+1)$  codewords of  $\widehat{C}$ . Clearly  $d(\mathbf{x}, C) = r$ . Because  $(\mathbf{x}, \mathbf{x}')$  has distance  $r+1$  to  $\widehat{C}$ , the vector  $(\mathbf{x}, \mathbf{x}')$  has to disagree in the last coordinate with every  $(\mathbf{c}, \pi(\mathbf{c})) \in \widehat{C}$  for which  $d(\mathbf{x}, \mathbf{c}) = r$  and therefore  $\mathbf{x}' = \pi(\mathbf{x}) + 1$  if  $r$  is even and  $\mathbf{x}' = \pi(\mathbf{x})$  if  $r$  is odd. If  $d(\mathbf{x}, \mathbf{c}) = r+1$  or  $r$ , then  $|B_r(\mathbf{c}) \cap B_1(\mathbf{x})| = r+1$  and because  $C$  covers  $\mu$  times all the vectors in  $B_1(\mathbf{x})$ , we have  $|B_{r+1}(\mathbf{x}) \cap C| \geq \mu(n+1)/(r+1)$ . We show that the codewords  $(\mathbf{c}, \pi(\mathbf{c}))$  where  $\mathbf{c} \in B_{r+1}(\mathbf{x}) \cap C$  will do, i.e., each of them is within distance  $r+1$  from  $(\mathbf{x}, \mathbf{x}')$ . This is immediate if  $d(\mathbf{c}, \mathbf{x}) = r$ . If  $d(\mathbf{c}, \mathbf{x}) = r+1$ , then  $\pi(\mathbf{c}) = \pi(\mathbf{x}) + 1 = \mathbf{x}'$  when  $r$  is even and  $\pi(\mathbf{c}) = \pi(\mathbf{x}) = \mathbf{x}'$  when  $r$  is odd, completing the proof.  $\square$

**Corollary 14.6.3** If  $C$  is a perfect  $(n, K, r, 1)$  MC then the extended code  $\widehat{C}$  is a perfect  $(n+1, K, r+1, (n+1)/(r+1))$  MCF.

**Proof.** By the previous theorem, the extended code  $\widehat{C}$  is an  $(n+1, K, r+1, \lceil (n+1)/(r+1) \rceil)$  MCF. Furthermore,

$$\begin{aligned} & K\left(\binom{n+1}{0} + \binom{n+1}{1} + \dots + \binom{n+1}{r} + \binom{r+1}{n+1} \binom{n+1}{r+1}\right) \\ &= K\left(\binom{n}{0} + \left(\binom{n}{0} + \binom{n}{1}\right) + \dots + \left(\binom{n}{r-1} + \binom{n}{r}\right) + \binom{n}{r}\right) \\ &= 2K\left(\binom{n}{0} + \binom{n}{1} + \dots + \binom{n}{r}\right) = 2 \cdot 2^n = 2^{n+1} \end{aligned}$$

which shows that  $\hat{C}$  attains the sphere-covering bound and in particular  $(n+1)/(r+1)$  has to be an integer.  $\square$

**Example 14.6.4** By the previous corollary the extended Hamming code is a linear perfect  $(2^m, 2^{2^m-1-m}, 2, 2^{m-1})$  MCF.  $\square$

**Theorem 14.6.5** Suppose  $C$  is an  $(n, K, r, \mu)$  MCF and that no two codewords differ only in the first coordinate. Then the code  $C^*$  obtained by puncturing the first coordinate is an  $(n-1, K, r, 2\mu)$  MCF.

**Proof.** If a vector  $\mathbf{x}^* \in \mathbb{F}^{n-1}$  has distance at least  $r$  to every word of  $C^*$ , then  $d(0\mathbf{x}^*, C) = r$  and  $d(1\mathbf{x}^*, C) = r$ . Hence there are at least  $\mu$  different codewords  $\mathbf{c}_i^0 \in C$  such that  $d(\mathbf{c}_i^0, 0\mathbf{x}^*) = r$ , and at least  $\mu$  different codewords  $\mathbf{c}_i^1 \in C$  such that  $d(\mathbf{c}_i^1, 1\mathbf{x}^*) = r$ . Since  $d(0\mathbf{x}^*, C) = r$ , all the words  $\mathbf{c}_i^0$  begin with 0, and similarly the words  $\mathbf{c}_i^1$  all begin with 1. Puncturing the first coordinate in these  $2\mu$  distinct words, we obtain the claim.  $\square$

The piecewise constant code construction of Section 3.3 is also immediately applicable to MCF.

**Example 14.6.6** It is easy to verify that the vectors of weight 0, 2, 5 and 7 in  $\mathbb{F}^7$  form a  $(7, 44, 1, 3)$  MCF.  $\square$

**Example 14.6.7** Take as codewords all the vectors  $(\mathbf{c}_1, \mathbf{c}_2)$  such that  $\mathbf{c}_1 \in \mathbb{F}^4$ ,  $\mathbf{c}_2 \in \mathbb{F}^{2k-1}$  and  $(w(\mathbf{c}_1), w(\mathbf{c}_2)) \in \{(1, 0), (4, 0), (0, 2k-1), (3, 2k-1)\}$ . It is easy to check that these 10 vectors form a  $(2k+3, 10, k, 2)$  MCF and that therefore  $F(2k+3, k, 2) \leq 10$  for all  $k \geq 1$ .  $\square$

The matrix construction of Section 3.5 can easily be modified for MCF. Here all the vectors are again assumed to be column vectors. Let  $\mathbf{A} = (\mathbf{I}_k, \mathbf{D}) = (\mathbf{a}_1, \mathbf{a}_2, \dots, \mathbf{a}_n)$  be a  $k \times n$  binary matrix where  $\mathbf{I}_k$  is the identity matrix, and suppose  $\mathbf{s}_1, \mathbf{s}_2, \dots, \mathbf{s}_t$  are different vectors in  $\mathbb{F}^k$ .

**Theorem 14.6.8** Assume that for every  $\mathbf{x} \in \mathbb{F}^k$  there is a pair  $(j, \mathbf{y})$  such that  $\mathbf{y} \in \mathbb{F}^n$ ,  $w(\mathbf{y}) < r$  and  $\mathbf{x} = \mathbf{A}\mathbf{y} + \mathbf{s}_j$ ; or there are at least  $\mu$  different pairs  $(j, \mathbf{y})$  such that  $\mathbf{y} \in \mathbb{F}^n$ ,  $w(\mathbf{y}) = r$  and  $\mathbf{x} = \mathbf{A}\mathbf{y} + \mathbf{s}_j$ . Then the vectors in the sets

$$C_j = \{\mathbf{y} \in \mathbb{F}^n : \mathbf{A}\mathbf{y} = \mathbf{s}_j\},$$

$j = 1, 2, \dots, t$ , together form an  $(n, t2^{n-k}, r, \mu)$  MCF.  $\square$

Many of the best known MCF have been found using the matrix construction and local search techniques.

**Theorem 14.6.9**  $F(2n, 1, 2\mu) \leq 2^n F(n, 1, \mu)$ .

**Proof.** Let  $C$  be an  $(n, F(n, 1, \mu), 1, \mu)$  MCF and  $D = \{(\mathbf{x}, \mathbf{x} + \mathbf{c}) : \mathbf{x} \in \mathbb{F}^n, \mathbf{c} \in C\}$ . If  $(\mathbf{a}, \mathbf{a} + \mathbf{b}) \in \mathbb{F}^{2n}$ , where  $\mathbf{a}, \mathbf{b} \in \mathbb{F}^n$ , has distance 1 to  $D$ , then we can choose  $\mathbf{c} \in C$  in  $\mu$  different ways so that  $d((\mathbf{a}, \mathbf{a} + \mathbf{b}), (\mathbf{a}, \mathbf{a} + \mathbf{c})) = 1$ . All the vectors  $\mathbf{b} + \mathbf{c}$  have weight one and we find another  $\mu$  codewords  $(\mathbf{a} + (\mathbf{b} + \mathbf{c}), \mathbf{a} + \mathbf{b}) = (\mathbf{a} + (\mathbf{b} + \mathbf{c}), \mathbf{a} + (\mathbf{b} + \mathbf{c}) + \mathbf{c}) \in D$  that have distance 1 to  $(\mathbf{a}, \mathbf{a} + \mathbf{b})$ .  $\square$

**Theorem 14.6.10**  $F(2n + \mu, 1, \mu) \leq 2^{n+\mu-1} F(n, 1, \mu)$ .

**Proof.** Let  $C$  be an  $(n, F(n, 1, \mu), 1, \mu)$  MCF and  $D = \{(\mathbf{x}_0, \mathbf{x}, \mathbf{x} + \mathbf{c}) : \mathbf{x}_0 \in \mathbb{F}^\mu, \mathbf{x} \in \mathbb{F}^n, \mathbf{c} \in C, w((\mathbf{x}_0, \mathbf{x})) \text{ is even}\}$ . Let  $(\mathbf{a}_0, \mathbf{a}, \mathbf{a} + \mathbf{b}) \in \mathbb{F}^{\mu+2n}$ , where  $\mathbf{a}_0 \in \mathbb{F}^\mu, \mathbf{a}, \mathbf{b} \in \mathbb{F}^n$ , be arbitrary.

Assume first that  $d(\mathbf{b}, C) = 1$  and that  $\mathbf{c} \in C$  is such that  $d(\mathbf{b}, \mathbf{c}) = 1$ . Let  $i$  be the unique coordinate in which  $\mathbf{b}$  and  $\mathbf{c}$  disagree. If  $w((\mathbf{a}_0, \mathbf{a}))$  is even, then  $(\mathbf{a}_0, \mathbf{a}, \mathbf{a} + \mathbf{c}) \in D$  and  $d((\mathbf{a}_0, \mathbf{a}, \mathbf{a} + \mathbf{c}), (\mathbf{a}_0, \mathbf{a}, \mathbf{a} + \mathbf{b})) = 1$ ; otherwise  $(\mathbf{a}_0, \mathbf{a}^i, \mathbf{a}^i + \mathbf{c}) \in D$  and  $d((\mathbf{a}_0, \mathbf{a}^i, \mathbf{a}^i + \mathbf{c}), (\mathbf{a}_0, \mathbf{a}, \mathbf{a} + \mathbf{b})) = 1$  where  $\mathbf{a}^i = \mathbf{a} + \mathbf{e}_i$ . The same argument applies to all the  $\mu$  different words  $\mathbf{c} \in C$  such that  $d(\mathbf{b}, \mathbf{c}) = 1$  and gives  $\mu$  different words of  $D$ .

Assume that  $\mathbf{b} \in C$ . If  $w((\mathbf{a}_0, \mathbf{a}))$  is even, then  $(\mathbf{a}_0, \mathbf{a}, \mathbf{a} + \mathbf{b}) \in D$ . Finally, if  $w((\mathbf{a}_0, \mathbf{a}))$  is odd, then  $(\mathbf{a}_0^i, \mathbf{a}, \mathbf{a} + \mathbf{b}) \in D$  for all  $i = 1, 2, \dots, \mu$ , where  $\mathbf{a}_0^i = \mathbf{a}_0 + \mathbf{e}_i$ .  $\square$

In many cases the ADS of an  $(n, K, r, \mu)$  MCF and the code  $\{000, 111\}$  gives an  $(n + 2, K, r + 1, \mu)$  MCF. The upper bounds obtained in this way have been marked with G in Table 14.5.

Table 14.5: Upper bounds on  $F(n, r, \mu)$ .

n	r = 1			r = 2		
	$\mu = 2$	$\mu = 3$	$\mu = 4$	$\mu = 2$	$\mu = 3$	$\mu = 4$
1	2 Z	2 Z	2 Z			
2	2 Z	4 Z	4 Z	2 Z	2 Z	2 Z
3	4 T	4 Y	8 A	2 Z	2 Z	2 Z
4	7 S	8 T	8 S	2 Z	4 Z	4 Z
5	10 S	16 T	16 A	4 T	4 P	6 S
6	16 Y	24 M	32 A	7 T	7 P	8 S
7	32 A	44 S	58 M	10 S	12 T	12 P
8	62 B	80 M	104 M	16 T	16 T	16 P
9	106 M	128 Y	186 S	26 M	32 A	32 A
10	192 B	256 A	320 R	32 L	56 M	62 P
11	368 M	512 A	592 M	64 A	96 M	112 M
12	640 W	976 M	1024 Y	128 A	160 M	192 P
13	1248 M	1728 M	2048 A	224 M	256 L	368 M
14	2048 Y	3072 M	4096 A	384 M	512 A	640 M
15	4096 A	6144 A	8192 A	768 A	896 M	1024 L
16	8192 A	12288 A	14336 M	1344 M	1792 A	2048 A

n	r = 3			r = 4		
	$\mu = 2$	$\mu = 3$	$\mu = 4$	$\mu = 2$	$\mu = 3$	$\mu = 4$
3	2 Z	2 Z	2 Z			
4	2 Z	2 Z	2 Z	2 Z	2 Z	2 Z
5	2 Z	2 Z	2 Z	2 Z	2 Z	2 Z
6	2 Z	4 Z	4 Z	2 Z	2 Z	2 Z
7	4 T	4 P	6 S	2 Z	2 Z	2 Z
8	7 T	7 P	8 S	2 Z	4 Z	4 Z
9	10 S	12 T	12 G	4 T	4 P	6 S
10	16 T	16 T	16 G	7 T	7 P	8 S
11	24 T	24 Z	30 P	10 S	12 T	12 G
12	32 G	44 T	44 P	16 T	16 T	16 G
13	64 A	78 T	78 P	24 T	24 G	28 P
14	88 Z	128 T	128 P	32 G	40 M	42 P
15	160 X	192 M	256 A	64 T	64 T	64 P
16	256 L	384 A	448 M	96 M	112 T	112 P

## Key to Table 14.5

A	$F(n+1, r, \mu) \leq 2F(n, r, \mu)$
B	puncturing
G	ADS of a code with $\{000, 111\}$
L	linear code from Hääläinen, Honkala, Litsyn and Östergård [276]
M	matrix construction [276]
P	Theorem 14.6.2
R	Theorem 14.6.9
S	piecewise constant code [276]
T	$F(n, r, \mu) \leq F(n, r, \mu + 1)$
W	Theorem 14.6.10
X	multiple covering, see Tables 14.1–14.4
Y	perfect weighted covering from Theorem 13.3.3
Z	miscellaneous construction [276]

## 14.7 Notes

§14.1 Some lower bounds for multiple coverings have been presented in Hääläinen, Honkala, Kaakkonen and Litsyn [275] and Chen and Li [135]. Examples 14.1.2 and 14.1.3 are essentially from [275]. Some exact values of the function  $\overline{K}_q(n, r, \mu)$  have been given in Clayton [141], e.g., the bound  $\overline{K}(4, 1, 2) = 7$  proved in Example 14.1.3 and  $\overline{K}(5, 1, 2) = 12$ . Clayton [141] has shown that  $\overline{K}_q(3, 1, 2) \geq \frac{7}{8}q^2$  and conjectures that the code  $\{(x, x, y) : x, y \in \mathbb{Z}_q\}$  with  $q^2$  codewords is optimal. It is shown in [141] that

$$\overline{K}_q(n, n-1, 1) = q \text{ for all } q;$$

$$\overline{K}_q(2, 1, 2t+1) \geq (t+1)q \text{ with equality if } q > t;$$

$$\overline{K}_q(2, 1, 2t) \geq \frac{2t(t+1)}{2t+1}q \text{ with equality if and only if } 2t+1 \text{ divides } q;$$

$$\overline{K}_q(n, n-1, 2) \geq \frac{2n}{2n-1}q \text{ with equality if and only if } 2n-1 \text{ divides } q.$$

§14.2 Theorems 14.2.1 and 14.2.2 and Example 14.2.3 are from Clayton [141]. A perfect  $q$ -ary MCR  $C$  of length  $n$  over  $\mathbb{Z}_q$  is called *trivial* if every vector in  $\mathbb{Z}_q^n$  occurs the same number of times in  $C$ . By using Theorem 14.2.1 Clayton has shown that a nontrivial perfect  $q$ -ary  $(n, \cdot, r, \cdot)$  MCR exists

- (i) if and only if  $n = m^2 + 1$  for some integer  $m$ , when  $q = 2$  and  $r = 2$ ;
- (ii) if and only if  $n = \binom{m}{2} + 1$  for some integer  $m$ , when  $q = 3$  and  $r = 2$ ;
- (iii) for infinitely many  $n$ , when  $q$  is fixed and  $r = 2$ ;

- (iv) if and only if  $n$  is odd or  $n = 3k^2 + 2k + 2$  for some integer  $k$ , when  $q = 2$  and  $r = 3$ ;
- (v) for only finitely many  $n$ , when  $q \geq 3$  is fixed and  $r = 3$ ;
- (vi) for only finitely many  $n$ , when  $q$  is fixed and  $r = 4$ .

Theorem 14.2.4 and the corresponding result for the linear codes over an arbitrary finite field are from van Wee, Cohen and Litsyn [681]. Theorem 14.2.4 no longer holds if we only assume that  $q$  is a prime power; see [681].

Theorems 14.2.6 and 14.2.7 are from Cohen, Honkala, Litsyn and Mattson [155]. The following perfect binary linear multiple 2-coverings  $C$  with  $d = s = 2$  are known [155]:

$C$		$C^\perp$
$[5, 1, 5]$	$\mu = 1$	$[5, 4; 2, 4]$
$[5, 2, 2]$	$\mu = 2$	$[5, 3; 2, 4]$
$[5, 3, 2]$	$\mu = 4$	$[5, 2; 2, 4]$
$[10, 7, 2]$	$\mu = 7$	$[10, 3; 4, 7]$
$[37, 32, 2]$	$\mu = 22$	$[37, 5; 16, 22]$
$[8282, 8269, 2]$	$\mu = 4187$	$[8282, 13; 4096, 4187]$

where the notation  $[n, k; w_1, w_2]$  stands for an  $[n, k]$  code in which the nonzero weights are  $w_1$  and  $w_2$ . The first code is  $\{00000, 11111\}$  and the second one is  $\{00000, 11000, 00111, 11111\}$ . The other ones arise from the following construction. Let  $\mathbf{G}_1$  denote the generator matrix of the binary  $i$ -dimensional simplex code. Consider the code  $C$  whose parity check matrix is  $\mathbf{H} = (\mathbf{G}_1, \mathbf{a}, \mathbf{a}, \dots, \mathbf{a})$  where  $\mathbf{a} = (1, 0, 0, \dots, 0)^T$  is repeated  $h$  times. It is not difficult to show that  $\mathcal{A}_0(\mathbf{x}) + \mathcal{A}_1(\mathbf{x}) + \mathcal{A}_2(\mathbf{x})$  is independent of  $\mathbf{x} \in \mathbb{F}^n$  if and only if  $1 + \binom{h}{2} = 2^{i-1}$ . All solutions of this Diophantine equation are known; see Skolem, Chowla and Lewis [588]. They exist precisely for  $h = 0, 1, 2, 3, 6$  and 91. The four largest values of  $h$  lead to the remaining four PMC. It is conjectured in [155] that there are no other binary linear PMC with  $d = s = r = 2$ .

Theorem 14.2.8 was obtained by Clayton [141] for MCR as a corollary to the following more general result. Assume that  $C_0$  and  $C_1$  are two binary perfect  $(n, K, 1, \mu)$  MCR of odd length. Form an MCR  $C$  of length  $n + m$  that consists of all the words  $(\mathbf{c}, \mathbf{y})$  where  $\mathbf{c} \in C_0$  and  $\mathbf{y}$  is even and all the words  $(\mathbf{c}, \mathbf{y})$  where  $\mathbf{c} \in C_1$  and  $\mathbf{y}$  is odd. If  $r$  is a positive integer such that

$$\sum_{i=0}^{\lceil r/2 \rceil} (-1)^i \binom{m}{r-2i} \binom{(n-1)/2}{i} = 0,$$

then  $C$  is a perfect  $(n + m, 2^m K, r, \mu V(n + m, r)/V(n, 1))$  MCR.

Theorem 14.2.9 is from Clayton [141] where the following statement for arbitrary  $q$  is also obtained: if a nontrivial perfect  $q$ -ary  $(n, \cdot, r, \cdot)$  MCR exists, there also exists a nontrivial perfect  $q$ -ary  $(n, \cdot, n - r - 1, \cdot)$  MCR.

Clayton [141] also discusses the decomposability of perfect MCR into unions of perfect MCR and shows that there is no unique decomposition theorem for perfect MCR.

**§14.3** The discussion of this section is based on Honkala [318]. These concepts can also be generalized to MCR; see Hämäläinen, Honkala, Kaikkonen and Litsyn [275]. By checking all the possible partitions with a computer it has been verified in Östergård [518] that the  $(11, 24, 3, 2)$  MC referred to in Table 14.5 is neither  $\mu$ -fold normal nor  $\mu$ -fold subnormal.

**§14.4** This section is based on Hämäläinen, Honkala, Kaikkonen and Litsyn [275]. Theorem 14.4.3 is from Clayton [141] where it is proved in the general  $q$ -ary case. A generalization of Theorem 3.4.5 can be found in [275], and a generalization of Theorem 3.7.8 in [141].

**§14.5** The remarks are from [275].

**§14.6** The discussion of this section is based on Hämäläinen, Honkala, Litsyn and Östergård [276]. As with multiple coverings, we may also study configurations where the same codeword is allowed to appear more than once. They are called MCF with repeated words (MCFR for short). Denote by  $\overline{F}(n, r, \mu)$  the smallest possible cardinality of an  $(n, \cdot, r, \mu)$  MCFR. A nontrivial example of a case where  $\overline{F}(n, r, \mu)$  is smaller than  $F(n, r, \mu)$  is given in [276] where it is shown that  $F(4, 1, 2) = 7 > \overline{F}(4, 1, 2) = 6$ .

This Page Intentionally Left Blank

# Chapter 15

## Football pools

This chapter is devoted to the study of the recreational problem of finding good *football pool systems*. Assume that  $n$  football matches are played, and we wish to bet on these matches. Each bet costs an equal amount. A *bet* is a prediction of the winners in these  $n$  matches, and we accept a tie as a possible outcome. Hence a bet is a ternary vector of length  $n$ . We say that a bet in which all the  $n$  predictions are correct wins the first prize and in general a bet with  $n - i$  correct predictions wins the  $(i + 1)$ -st prize. The *football pool problem* is to determine what is the smallest number of bets to be placed in order to guarantee winning at least the second prize — no matter what the outcomes. In our terminology such a set is simply a ternary code of length  $n$  and covering radius at most 1. If ties were not allowed we would have the corresponding binary problem.

Although in the mathematical literature the term football pool problem has the restricted meaning just described, there are in fact a large number of similar problems that immediately arise. First of all, we may of course ask what is the smallest number of bets guaranteeing at least the  $(r + 1)$ -st prize for some small  $r$ , i.e., to find the minimum cardinality of a code with covering radius at most  $r$ .

From a probabilistic point of view a randomly placed bet is a waste of money, since the total prize money is only a certain percentage, e.g. 50 percent, of the placed bets. However, based on our knowledge of the teams we may consider certain outcomes highly unlikely, and decide to exclude them from our scheme. We then wish to find a similar covering, but now only for a part of the ternary space. Each match where we exclude two of the three outcomes in effect decreases  $n$  by one, and each match where we exclude just one of the three possibilities replaces a ternary coordinate by a binary one. This leads to the problem of covering the *mixed* space  $\mathbb{Z}_3^t \mathbb{Z}_2^b$ . In general, we can manage with a much smaller number of bets.

A number of problems studied in previous chapters arise naturally in this context.

If we place bets, it is natural to try and cover as many outcomes as possible, which leads to studying the function  $p(n, K, r)$  discussed in Section 6.1.

Assume that  $\mu$  persons separately use a football pool system which guarantees at least the  $(r + 1)$ -st prize. They can place their bets together and use a  $\mu$ -fold  $r$ -covering instead, which often decreases the required number of bets. Usually the  $r$ -th prize is several times the  $(r + 1)$ -st prize. If  $\mu$  is small they may therefore opt for a multiple covering of the farthest-off points. If  $\mu$  is large they can resort to a weighted covering taking into account the sizes of all the prizes (which can be estimated reasonably well beforehand).

Football pool systems have been studied for a long time by mathematicians and non-mathematicians alike, certainly for at least fifty years; see Taussky and Todd [635] and Hämäläinen and Rankinen [278].

In this chapter we study mixed codes with binary and ternary coordinates. In Section 15.1 we present some constructions and show that it is often useful to replace coordinates over one alphabet with coordinates over another. Tables of the best currently known lower and upper bounds are presented in Section 15.2. In a paper by Hämäläinen and Rankinen [278] it is mentioned that the ternary Golay code was published in the Finnish football pool magazine *Veikkaaja* in 1947. This discovery is briefly discussed in Section 15.3.

## 15.1 Constructions for mixed binary/ternary codes

Denote

$$K_{3,2}(t, b, R) = \text{the smallest cardinality of a code } C \subseteq \mathbb{Z}_3^t \mathbb{Z}_2^b \text{ with covering radius } R.$$

Actually we are not interested in the order of the coordinates. Denote the elements in the ternary alphabet by 0, 1, 2 and in the binary alphabet by 0, 1. Many of the constructions of Chapter 3 extend to mixed codes. Using the direct sum, for instance, we trivially obtain the upper bounds

$$K_{3,2}(t, b + 1, R) \leq 2K_{3,2}(t, b, R)$$

and

$$K_{3,2}(t + 1, b, R) \leq 3K_{3,2}(t, b, R).$$

### Theorem 15.1.1

$$K_{3,2}(t, b + 1, R) \leq K_{3,2}(t + 1, b, R).$$

**Proof.** Assume that  $C$  attains the bound  $K_{3,2}(t+1, b, R)$  and that the first coordinate is ternary. Change all 2's in the first coordinate to 0's. Trivially the covering radius of the resulting code is at most  $R$ .  $\square$

A more interesting result tells how to move in the other direction.

**Theorem 15.1.2**  $K_{3,2}(t+1, b, R) \leq \frac{3}{2}K_{3,2}(t, b+1, R)$ .

**Proof.** Assume that  $C$  attains the bound  $K_{3,2}(t, b+1, R)$  and that its first coordinate is binary. For  $a = 0, 1$ , we form the codes

$$C_a = C \cup \{(2, c_2, \dots, c_{t+b+1}) : (a, c_2, \dots, c_{t+b+1}) \in C\}. \quad (15.1.3)$$

The covering radius of  $C_a$  is clearly at most  $R$ , and  $C_0$  or  $C_1$  has at most  $3K_{3,2}(t, b+1, R)/2$  codewords.  $\square$

**Example 15.1.4** The four codewords 000000, 111111, 022222, 122222 form a code of length six and covering radius three with one binary coordinate and five ternary coordinates. Indeed, any vector with at most one 2 is covered by the first two codewords and any vector with more than one 2 by the other two codewords. Now the previous theorem shows that there is a ternary code of length six and covering radius at most three with six codewords. By the sphere-covering bound the covering radius is equal to three. The optimality of this code is proved in Example 6.7.5.  $\square$

The proofs of the next two theorems utilize the substitution construction presented in Theorem 3.6.1.

**Theorem 15.1.5**  $K_{3,2}(t, b+3, R) \leq \frac{8}{3}K_{3,2}(t+1, b, R)$ .

**Proof.** Assume that  $C$  attains the bound  $K_{3,2}(t+1, b, R)$ . Using the same idea as in the proof of Theorem 15.1.2 we obtain a code  $C' \subseteq \mathbb{Z}_4\mathbb{Z}_3^t\mathbb{Z}_2^b$  with covering radius at most  $R$  and cardinality at most  $\frac{4}{3}K_{3,2}(t+1, b, R)$ . Now the claim follows from Theorem 3.6.1 when we choose  $q = 4$  and  $C_0 = \{000, 111\}$ ,  $C_1 = \{100, 011\}$ ,  $C_2 = \{010, 101\}$  and  $C_3 = \{001, 110\}$ .  $\square$

**Theorem 15.1.6** If  $t > 0$ , then  $K_{3,2}(t+3, b, R+1) \leq 4K_{3,2}(t, b, R)$ .

**Proof.** Assume that  $C$  attains the bound  $K_{3,2}(t, b, R)$ . Again, using the idea leading to Theorem 15.1.2 we obtain a code  $C' \subseteq \mathbb{Z}_4\mathbb{Z}_3^{t-1}\mathbb{Z}_2^b$  with covering radius at most  $R$  and cardinality at most  $\frac{4}{3}K_{3,2}(t, b, R)$ . Now use the substitution construction of Theorem 3.6.1 for the first coordinate of  $C'$ , i.e., choose  $q = 4$ . The ternary codes  $C_0 = \{0001, 1112, 2220\}$ ,  $C_1 = \{0010, 1121, 2202\}$ ,  $C_2 = \{0100, 1211, 2022\}$  and  $C_3 = \{1000, 2111, 0222\}$  all have covering radius two, and their union has covering radius one. We therefore obtain a code  $C''$  with  $t+3$  ternary and  $b$  binary coordinates whose covering radius is at most  $R+1$ . The cardinality of  $C''$  is at most  $4K_{3,2}(t, b, R)$  proving our claim.  $\square$

All perfect codes are natural building blocks in the substitution construction. It is known, see B. Lindström [426], that if  $p$  is a prime, then there is a perfect group code  $C \subseteq \mathbb{Z}_{p^a}\mathbb{Z}_{p^b}^{n-1}$  with covering radius 1, if and only if  $a \geq b$  and  $p^r = p^a + (n-1)(p^b - 1)$  for some integer  $r \geq a+b$ .

**Example 15.1.7** By the previous discussion there exists a perfect code  $C \subseteq \mathbb{Z}_4\mathbb{Z}_2^4$  with covering radius 1 and size eight. Using the same idea as in the proof of Theorem 15.1.1 we see that  $K_{3,2}(1, 4, 1) \leq 8$ . Similarly  $K_{3,2}(1, 12, 1) \leq 1024$ .  $\square$

**Example 15.1.8** There is a perfect code  $C \subseteq \mathbb{Z}_8\mathbb{Z}_2^8$  with covering radius 1 and size 128. By applying the same idea as in the proof of Theorem 15.1.2, we obtain a code  $C' \subseteq \mathbb{Z}_9\mathbb{Z}_2^8$  with at most  $\frac{9}{8} \cdot 128 = 144$  codewords. Substituting the coordinate over  $\mathbb{Z}_9$  in  $C'$  with the nine cosets of the perfect ternary Hamming code of length four, we obtain the upper bound  $K_{3,2}(4, 8, 1) \leq 9 \cdot 144 = 1296$  from Theorem 3.6.1.  $\square$

**Example 15.1.9** Let  $C_1$  be a binary  $(7, 16)1$  code and  $C_2$  a binary  $(5, 7)1$  code. We form a code with  $t = 3$ ,  $b = 5$  and  $R = 2$  as follows. Take as codewords all the vectors in the extended code  $\widehat{C}_1$  and all the vectors in the set  $\{(c, 2, 2, 2) : c \in C_2\}$ . Any vector with at most one 2 in the last three coordinates is 2-covered by  $\widehat{C}_1$ , since puncturing  $\widehat{C}_1$  in any coordinate again gives a code with covering radius one. But any vector with at least two 2's in the last three coordinates is 2-covered by the other codewords. Hence  $K_{3,2}(3, 5, 2) \leq 23$ .  $\square$

The matrix construction of Section 3.5 also generalizes to mixed codes. In the binary/ternary case, we choose a set  $S \subseteq \mathbb{Z}_3^u\mathbb{Z}_2^v$  of column vectors and a matrix  $\mathbf{A}$  of the form

$$\begin{pmatrix} \mathbf{A}_1 & \mathbf{0} \\ \mathbf{0} & \mathbf{A}_2 \end{pmatrix},$$

where  $\mathbf{A}_1$  is a ternary  $u \times t$  matrix and  $\mathbf{A}_2$  is a binary  $v \times b$  matrix. The code  $C$  consists of all the words  $(\begin{smallmatrix} \mathbf{c}_1 \\ \mathbf{c}_2 \end{smallmatrix}) \in \mathbb{Z}_3^t \mathbb{Z}_2^b$  such that

$$\left( \begin{array}{c} \mathbf{A}_1 \mathbf{c}_1 \\ \mathbf{A}_2 \mathbf{c}_2 \end{array} \right) \in S.$$

A result similar to Theorem 3.5.1 clearly holds.

## 15.2 Tables for mixed binary/ternary codes

In the following tables we give the best currently known lower and upper bounds on  $K_{3,2}(t, b, R)$ .

No references for codes with at most four codewords are given. The majority of the upper bounds are from Hämäläinen and Rankinen [278]. Many of them were constructed by the authors; others were collected in several football pool magazines and booklets. For detailed information about sources and constructors we refer to [278]. Anyone interested in the actual codes should also consult Östergård and Hämäläinen [525] where revised tables and explicit constructions of a large number of old and new codes are presented.

### Key to Table 15.1

For the ternary cases, see Table 6.2.

#### Lower bounds

- a sphere-covering bound
- b Theorem 3.7.1
- h van Lint, Jr. and van Wee [441]
- k Kolev and Landgev [385] and Östergård and Hämäläinen [525]
- m Kolev [384]
- n Östergård and Hämäläinen [525]

#### Upper bounds

- A  $K_{3,2}(t, b + 1, R) \leq 2K_{3,2}(t, b, R)$
- C Theorem 15.1.1
- D Theorem 15.1.2
- E Theorem 15.1.5
- G Examples in Section 15.1
- K ADS with the code  $\{000, 111\}$
- L Hämäläinen and Rankinen [278]
- M matrix construction from Östergård and Hämäläinen [525]
- N explicitly listed code [525]
- Q other construction [525]

Table 15.1: Bounds on  $K_{3,2}(t, b, R)$ , Part I.

$t$	$b$	$R = 1$	$R = 2$	$R = 3$
1	0	1		
1	1	a 2	1	
1	2	a 3	a 2	1
1	3	k 6 A	a 2	a 2
1	4	h 8 G	a 3	a 2
1	5	k 16 A	k 6 A	a 2
1	6	h 24 D	n 8 K	a 3
1	7	h 40 – 48 A	h 10 – 12 L	k 6 A
1	8	h 76 – 84 L	h 16 – 20 L	h 6 – 8 K
1	9	h 130 – 160 M	a 24 – 35 L	h 8 – 12 K
1	10	h 253 – 284 N	h 44 – 60 L	h 12 – 20 K
1	11	h 444 – 548 L	h 74 – 96 L	h 19 – 32 M
1	12	h 869 – 1024 G	h 120 – 179 N	h 30 – 52 M
2	0	3	1	
2	1	h 4	a 2	1
2	2	a 6 L	n 3	a 2
2	3	n 12 A	h 4	a 2
2	4	k 20 L	k 6 K	n 3
2	5	h 31 – 36 D	a 7 – 11 L	k 4
2	6	h 56 – 64 E	h 12 – 16 L	k 6 K
2	7	h 99 – 126 D	h 19 – 28 L	a 6 – 11 K
2	8	h 187 – 234 L	h 32 – 48 L	a 9 – 16 K
2	9	h 337 – 419 N	h 56 – 74 M	h 15 – 24 M
2	10	h 646 – 768 L	h 92 – 144 D	h 23 – 42 N
2	11	h 1172 – 1504 M	h 165 – 256 E	h 35 – 70 L
3	0	5	3	1
3	1	n 9 D	a 3	a 2
3	2	n 16 L	k 5 L	n 3
3	3	h 24 E	n 8 E	a 3
3	4	h 41 – 48 A	a 9 – 13 L	k 5 K
3	5	h 76 – 92 L	h 15 – 23 G	a 5 – 8 K
3	6	h 139 – 176 L	h 24 – 36 L	a 7 – 12 L
3	7	h 256 – 320 M	h 43 – 56 N	h 12 – 20 L
3	8	h 480 – 576 L	h 71 – 96 L	h 18 – 32 M
3	9	h 887 – 1120 M	h 123 – 192 A	h 28 – 55 N
3	10	h 1689 – 2080 Q	h 223 – 358 Q	h 45 – 96 K

Table 15.1: Bounds on  $K_{3,2}(t, b, R)$ , Part II.

$t$	$b$	$R = 1$	$R = 2$	$R = 3$
4	0	9	3	3
4	1	h 18 A	k 6 A	b 3
4	2	m 36 A	a 7 – 10 L	n 4
4	3	h 58 – 72 A	h 12 – 18 K	n 6 K
4	4	h 103 – 132 L	a 18 – 24 L	a 6 – 10 K
4	5	h 194 – 240 L	h 32 – 48 A	h 9 – 16 L
4	6	h 356 – 432 L	h 55 – 72 L	h 14 – 24 K
4	7	h 671 – 864 A	h 92 – 144 A	h 22 – 45 N
4	8	h 1257 – 1296 G	h 168 – 252 L	h 34 – 68 N
4	9	h 2366 – 2592 A	h 290 – 480 Q	h 58 – 114 N
5	0	27	8	3
5	1	h 44 – 54 A	h 9 – 12 L	h 4
5	2	h 76 – 96 L	a 14 – 21 N	h 5 – 7 L
5	3	h 147 – 168 L	h 24 – 36 D	a 7 – 12 K
5	4	h 265 – 324 M	h 42 – 64 L	h 11 – 21 K
5	5	h 508 – 639 M	h 70 – 108 D	h 17 – 32 L
5	6	h 936 – 1206 M	h 126 – 192 E	h 27 – 54 L
5	7	h 1787 – 1944 D	h 222 – 348 Q	h 44 – 90 L
5	8	h 3353 – 3888 A	h 385 – 672 Q	h 76 – 144 L
6	0	63 – 73	14 – 17	6
6	1	h 112 – 132 L	h 18 – 27 L	h 6 – 9 L
6	2	h 197 – 252 D	h 33 – 48 L	a 8 – 16 L
6	3	h 384 – 468 M	h 53 – 72 L	h 14 – 24 L
6	4	h 697 – 864 L	h 94 – 144 A	h 21 – 44 L
6	5	h 1349 – 1656 M	h 170 – 276 L	h 33 – 72 K
6	6	h 2500 – 2916 D	h 290 – 519 N	h 58 – 96 N
6	7	h 4818 – 5832 A	h 532 – 960 Q	h 96 – 180 Q

Table 15.1: Bounds on  $K_{3,2}(t, b, R)$ , Part III.

$t$	$b$	$R = 1$	$R = 2$	$R = 3$
7	0	153 – 186	26 – 34	9 – 12
7	1	h 291 – 333 M	h 41 – 54 L	h 11 – 18 L
7	2	h 519 – 648 M	h 70 – 108 A	h 17 – 33 M
7	3	h 1019 – 1296 D	h 130 – 216 A	a 25 – 54 K
7	4	h 1864 – 2304 Q	h 220 – 396 L	h 44 – 90 L
7	5	h 3634 – 4374 D	h 397 – 720 L	h 74 – 144 L
7	6	h 6762 – 8640 M	h 729 – 1296 L	h 121 – 249 N
8	0	397 – 486	54 – 81	14 – 27
8	1	h 770 – 972 A	h 99 – 162 A	h 20 – 45 L
8	2	h 1390 – 1728 Q	h 167 – 288 L	h 33 – 72 L
8	3	h 2740 – 3456 A	h 295 – 504 L	h 57 – 108 L
8	4	h 5047 – 6480 L	h 555 – 972 Q	h 93 – 216 A
8	5	h 9886 – 12960 A	h 964 – 1620 M	h 155 – 324 L
9	0	1060 – 1341	130 – 219	25 – 54
9	1	h 2067 – 2592 Q	h 219 – 396 L	h 45 – 93 Q
9	2	h 3768 – 4860 M	h 422 – 729 C	h 72 – 144 N
9	3	h 7448 – 9720 D	h 731 – 1215 M	h 118 – 252 Q
9	4	h 13802 – 17496 M	h 1321 – 1944 C	h 207 – 432 L
10	0	2818 – 3645	323 – 558	57 – 108
10	1	h 5611 – 7047 M	h 555 – 729 C	h 91 – 189 Q
10	2	h 10311 – 13122 M	h 983 – 1458 A	h 154 – 324 L
10	3	h 20423 – 25272 E	h 1894 – 1944 E	h 283 – 648 A
11	0	7822 – 9477	729	115 – 243
11	1	h 15376 – 18954 A	h 1436 – 1458 A	h 217 – 486 A
11	2	h 28439 – 37908 A	h 2528 – 2916 A	h 365 – 729 L
12	0	21531 – 27702	1919 – 2187	282 – 729
12	1	h 42448 – 52488 M	h 3405 – 4374 A	h 470 – 972 L
13	0	59049	5062 – 6561	611 – 1215

Lower bounds for ternary codes have been studied in a number of papers. There are only few papers about lower bounds for the mixed case; almost all lower bounds in Table 15.1 are from van Lint, Jr. and van Wee [441]. Some exact values were proved independently by Kolev and Landgev [385] using combinatorial arguments and by Östergård and Hämäläinen [525] using computer search. Kolev [384] showed that  $K_{3,2}(4, 2, 1) = 36$ .

### 15.3 On the early history of the ternary Golay code

Several covering codes published in the mathematical literature were in fact already known to football pool system enthusiasts, and even published in a football pool magazine or booklet, see Hämäläinen and Rankinen [278]. Many systems have been published in the Finnish magazine *Veikkaaja* or *Veikkaus-Lotto* — the name has varied over the years — and in the Swedish magazine *Vi Tippa*. It is clear that the discoveries have been done independently. Here, we briefly describe one particularly interesting case mentioned in [278].

In the issue 27/1947, which appeared on 1 August, 1947, a Finnish football pool specialist Juhani Virtakallio published — under the pseudonym Jukka — a ternary code of length 11 with 729 words and covering radius 2, i.e., the ternary Golay code, presented as a nice football pool system. In the accompanying text Virtakallio writes:

The following system with 729 columns [= codewords] was born in my brains during a period of depression in football pool prizes. Because the prizes were too small at that time to compensate the investments that would have been required if the system had been used week after week, the system remained unpublished and was forgotten among other systems. When during the last winter the football pool prizes reached a peak, there was talk with the editors [of the magazine *Veikkaaja*] about publishing the system but fitting in the 729 columns in the magazine did not succeed. Only now, when I discovered a method of obtaining the required saving of space, this system gets a chance to enrich the possibilities of the players and a chance to make some players rich, too.

729 columns, 1 sure match and 11 matches with all three possibilities. [At that time in Finland there were 12 matches to be forecast every week.] If the match chosen to be the sure match has been forecast correctly the system guarantees at least 10 correct

results. In the model we only present how to forecast the 11 other matches, the sure match has not been written down.

According to this, Virtakallio knew the code in the winter 1946–47 but the discovery of the code may have taken place earlier. Golay discovered his code more than a year later, see, e.g., Thompson [638].

Then follows a list of the first 243 codewords, 30 groups of 8 codewords and three more codewords, each codeword being written as a column. Finally, the passage in the issue 27/1947 ends with the remark that it will be explained in the next issue how to get the remaining codewords. In the ninth group the eighth row consists of only 7 letters (and not of 8 as it should). This misprint was corrected in the issue 33/1947 of *Veikkaaja* published on 12 September, 1947.

In the issue 28/1947 published on 8 August, 1947, Virtakallio explains how to get the remaining words: replace in the 243 words first every 1 by x, every x by 2, and every 2 by 1, to get another 243 words, and second every 1 by 2, every 2 by x and every x by 1, to obtain the last 243 words. Then the author explains that the player can also use only a part of the system and that it is up to the user of the system to decide which codewords to take and which to omit. E.g., if one is convinced that the number of draws is at most three, all the codewords with more than five x's are unnecessary.

## 15.4 Notes

§15.1 Theorems 15.1.1, 15.1.2 and 15.1.5 are from Hämäläinen and Rankinen [278]. Example 15.1.4 is also based on [278]. Theorem 15.1.6 is from Östergård and Hämäläinen [525]; for the codes  $C_0, C_1, C_2, C_3$ , used in the proof, see [278]. The upper bounds on the mixed binary/ternary codes obtained in Examples 15.1.7, 15.1.8 and 15.1.9 are from [278]; our presentations are from [525] and Östergård [516]. For a discussion of the matrix construction and other constructions for arbitrary mixed codes, see [516] and [525]. For other problems related to football pools, see Hämäläinen, Honkala, Litsyn and Östergård [277]. For a short survey on the football pool problem, see also Östergård [520].

§15.2 For some notes on lower and upper bounds on nonbinary and mixed covering codes, see the Notes of Chapters 3 and 6.

§15.3 In connection with the publication of Hämäläinen and Rankinen [278] a short appendix was written by Honkala and sent along with the manuscript of [278] to several people. This section is based on this unpublished appendix that has been referred to in some papers. See also Barg [49].

# Chapter 16

## Tilings

Given a body in an  $n$ -dimensional metric space, is it possible to tile the space with some of its translates? Here we are interested in tiling the binary Hamming space  $\mathbb{F}^n$ , and our aim is to describe those sets of  $\mathbb{F}^n$  that are tiles.

Tilings of  $\mathbb{F}^n$  with Hamming spheres are just perfect binary codes (see Chapter 11). Although their parameters have been determined, a complete classification remains an open problem. Another example is tilings of  $\mathbb{F}^n$  by so-called  $L$ -spheres, which are unions of some shells of the Hamming sphere (see Section 19.1).

This chapter is organized as follows. We start with some notation and definitions in Section 16.1. In Section 16.2 we present a sufficient condition for a given set  $V$  to be a linear tile. In Section 16.3 we provide a complete classification of tiles of cardinality  $\leq 8$ . Tilings  $(V, A)$  with sets of large rank are also considered. In Section 16.4 we study periodicity of tilings. In Section 16.5 we show that the classification of tilings of  $\mathbb{F}^n$  may be reduced to the study of so-called proper tilings. This leads to a recursive decomposition of tilings into tilings of smaller and smaller size, and ultimately shows that any tiling of  $\mathbb{F}^n$  may be constructed from tilings that are either trivial or have full rank. In Section 16.6 we show that a tiling  $(V, A)$  is uniquely associated with a perfect binary code of length  $|V| - 1$ . A construction of tilings from perfect codes is also presented. In Section 16.7 we generalize the Lloyd theorem, originally stated for spheres (see Sections 11.2 and 13.2), to the case of arbitrary tilings.

### 16.1 Preliminaries

Given subsets  $A$  and  $B$  of  $\mathbb{F}^n$ , we denote by  $A + B$  the set

$$\{\mathbf{a} + \mathbf{b} : \mathbf{a} \in A, \mathbf{b} \in B\}.$$

Furthermore, for a subset  $V$  of  $\mathbb{F}^n$  we write

$$iV := \underbrace{V + V + \dots + V}_{i \text{ times}}.$$

Thus  $iV$  is the set of all vectors in  $\mathbb{F}^n$  that may be represented as a sum of some  $i$  elements of  $V$ . Assume that  $\mathbf{0} \in V$ . The linear span of  $V$ , denoted by  $\langle V \rangle$ , is the subspace of  $\mathbb{F}^n$  generated by  $V$ . The rank of  $V$  is given by  $\text{rank}(V) = \dim(\langle V \rangle)$ . We let  $\mathcal{R}(V)$  denote the minimum number of elements of  $V$  required to generate any vector in its linear span, namely

$$\mathcal{R}(V) := \min \{ j : jV = \langle V \rangle \}.$$

It is easy to see that  $\mathcal{R}(V)$  is the covering radius of the linear code  $C(V^*)$  defined by a parity check matrix  $\mathbf{H}(V^*)$ , having the elements of  $V \setminus \{\mathbf{0}\}$  as its columns.

We say that a given set  $V$  is a *tile* of  $\mathbb{F}^n$  if it is possible to partition  $\mathbb{F}^n$  into disjoint additive cosets of  $V$ :  $V + \mathbf{a}_0, V + \mathbf{a}_1, \dots, V + \mathbf{a}_m$ . Note that the set of *coset representatives*  $A = \{\mathbf{a}_0, \mathbf{a}_1, \dots, \mathbf{a}_m\}$  is also a tile of  $\mathbb{F}^n$ . Without loss of generality we assume that both  $V$  and  $A$  contain the  $\mathbf{0}$  element. Evidently, each  $\mathbf{x} \in \mathbb{F}^n$  has a unique representation of the form  $\mathbf{x} = \mathbf{v} + \mathbf{a}$ , where  $\mathbf{v} \in V$  and  $\mathbf{a} \in A$ . Thus we have the following definition.

**Definition 16.1.1** *The pair  $(V, A)$  is a tiling of  $\mathbb{F}^n$  if*

$$V + A = \mathbb{F}^n$$

and

$$2V \cap 2A = \{\mathbf{0}\}.$$

More generally, we speak of tilings  $(V, A)$  of a subset  $B$  of  $\mathbb{F}^n$ , if both  $V + A = B$  and  $2V \cap 2A = \{\mathbf{0}\}$  hold.

A trivial necessary condition for  $(V, A)$  to be a tiling of  $\mathbb{F}^n$  is that  $|V| = 2^k$  and  $|A| = 2^{n-k}$ . Thus, hereafter, when denoting a subset of  $\mathbb{F}^n$  by  $V$  we assume that  $|V| = 2^k$ .

**Theorem 16.1.2** *A set  $V \subseteq \mathbb{F}^n$  is a tile of  $\mathbb{F}^n$  if and only if it is a tile of  $\langle V \rangle$ .*

**Proof.** ( $\Leftarrow$ ) Since  $\langle V \rangle$  is linear it is a tile of  $\mathbb{F}^n$ . Thus, if  $(\langle V \rangle, A_1)$  is a tiling of  $\mathbb{F}^n$  and  $(V, A_0)$  is a tiling of  $\langle V \rangle$ , then evidently  $(V, A_0 + A_1)$  is a tiling of  $\mathbb{F}^n$ .

( $\Rightarrow$ ) Let  $(V, A)$  be a tiling of  $\mathbb{F}^n$  and define  $A_0 = A \cap \langle V \rangle$ . We claim that  $(V, A_0)$  is a tiling of  $\langle V \rangle$ . Indeed, since  $A_0 \subseteq A$  and  $2V \cap 2A = \{\mathbf{0}\}$ , it follows that  $2V \cap 2A_0 = \{\mathbf{0}\}$ . Further, since  $\langle V \rangle \subseteq \mathbb{F}^n = V + A$ , any  $\mathbf{w} \in \langle V \rangle$  can be

written as  $\mathbf{w} = \mathbf{v} + \mathbf{a}$ , where  $\mathbf{v} \in V$  and  $\mathbf{a} \in A$ . However, since  $\langle V \rangle$  is linear we have  $\mathbf{a} = \mathbf{v} + \mathbf{w} \in \langle V \rangle$ , so that  $\mathbf{a} \in A_0$ . It follows that  $\langle V \rangle \subseteq V + A_0$ . The converse inclusion  $V + A_0 \subseteq \langle V \rangle$  is obvious from  $V, A_0 \subseteq \langle V \rangle$ .  $\square$

If both  $V$  and  $A$  are linear subspaces of  $\mathbb{F}^n$ , then  $(V, A)$  is a tiling if and only if  $A = \mathbb{F}^n/V$ . Hence in the sequel we restrict our attention to those tilings where at least one of the sets  $V, A$  is not linear.

**Definition 16.1.3** A set  $V \subseteq \mathbb{F}^n$  is a linear tile if there is a tiling  $(V, A)$  such that  $A$  is a linear subspace of  $\mathbb{F}^n$ .

## 16.2 A sufficient condition

A well-known example of a linear tile is the Hamming sphere, in which case the set of coset representatives  $A$  is a perfect binary code. More precisely, a sphere of positive radius  $e < (n - 1)/2$  is a (linear) tile of  $\mathbb{F}^n$  if and only if  $e = 1, n = 2^m - 1$  or  $e = 3, n = 23$  (Theorem 11.2.2). In this section we present a sufficient condition for a set  $V$  to be a linear tile.

**Theorem 16.2.1** If  $|2V| < 2|V|$ , then  $V$  is a linear tile.

**Proof.** Let  $|V| = 2^k$  and suppose that  $|2V| < 2^{k+1}$ . Then either  $k = n$ , in which case  $V = \mathbb{F}^n$  is a trivial linear tile, or  $|2V| < 2^n$  and there exists an  $\mathbf{a}_1 \in \mathbb{F}^n \setminus 2V$ . Set  $V_1 = V \cup (\mathbf{a}_1 + V)$ . Since  $\mathbf{a}_1 \notin 2V$ , we have  $V \cap (\mathbf{a}_1 + V) = \emptyset$  and  $|V_1| = 2|V| = 2^{k+1}$ . If  $V_1 = \mathbb{F}^n$ , then  $(V, \{\mathbf{0}, \mathbf{a}_1\})$  is a tiling of  $\mathbb{F}^n$  and we are done. Otherwise, since  $|2V_1| = |2V \cup (\mathbf{a}_1 + 2V)| < 2|V_1|$ , there exists an  $\mathbf{a}_2 \in \mathbb{F}^n \setminus 2V_1$  and we set  $V_2 = V_1 \cup (\mathbf{a}_2 + V_1)$  with  $V_1 \cap (\mathbf{a}_2 + V_1) = \emptyset$  and  $|V_2| = 2|V_1|$ . Continuing in this manner we construct  $V_{n-k} = \mathbb{F}^n$  and a tiling  $(V, A)$  of  $\mathbb{F}^n$ , where  $A$  is a subspace of  $\mathbb{F}^n$  generated by  $\mathbf{a}_1, \mathbf{a}_2, \dots, \mathbf{a}_{n-k}$ .  $\square$

The condition  $|2V| < 2|V|$  of Theorem 16.2.1 may be somewhat relaxed if additional information pertaining to  $V$  is available. For instance, we have the following result.

**Corollary 16.2.2** If  $|2V| = 2|V|$ , then  $V$  is a linear tile if and only if  $2V$  is not linear.

**Proof.** ( $\Leftarrow$ ) If  $2V$  is not linear, then  $2V \neq 4V$  and there exists an  $\mathbf{a}_1 \in 4V \setminus 2V$ . Set  $V_1 = V \cup (\mathbf{a}_1 + V)$ . Since  $\mathbf{a}_1 \notin 2V$ , we have  $V \cap (\mathbf{a}_1 + V) = \emptyset$  and  $|V_1| = 2|V|$  as before. Now  $2V_1 = 2V \cup (\mathbf{a}_1 + 2V)$ , and since  $\mathbf{a}_1 \in 4V$  it follows that  $2V \cap (\mathbf{a}_1 + 2V) \neq \emptyset$ . Thus  $|2V_1| < 2|2V| = 2|V_1|$ . Applying Theorem 16.2.1 to  $V_1$ , we conclude that there exists a linear subspace  $A_1 \subset \mathbb{F}^n$  such that  $(V_1, A_1)$  is a tiling. But then so is  $(V, A_1 + \{\mathbf{0}, \mathbf{a}_1\})$ .

$(\Rightarrow)$  If  $2V$  is linear, then  $\langle V \rangle = 2V$ , and therefore  $V$  does not tile its linear span. The claim now follows directly from Theorem 16.1.2.  $\square$

Note that  $2V$  is not linear if and only if  $\mathcal{R}(V) > 2$ . In fact, the argument of Corollary 16.2.2 may be pushed a little further, provided that  $\mathcal{R}(V)$  is large enough.

**Corollary 16.2.3** *If any of the following holds:*

- (i)  $|2V| \leq 2|V| + 2$  and  $\mathcal{R}(V) > 2$
- (ii)  $|2V| \leq 2|V| + 4$  and  $\mathcal{R}(V) > 5$
- (iii)  $|2V| \leq 2|V| + 5$  and  $\mathcal{R}(V) > 8$ ,

*then  $V$  is a linear tile.*

**Proof.** (i) If  $\mathcal{R}(V) > 2$  there exists an  $\mathbf{a}_1 \in 3V \setminus 2V$ , say  $\mathbf{a}_1 = \mathbf{v}_1 + \mathbf{v}_2 + \mathbf{v}_3$ . As before let  $V_1 = V \cup (\mathbf{a}_1 + V)$  with  $|V_1| = 2|V|$  and  $2V_1 = 2V \cup (\mathbf{a}_1 + 2V)$ . Note that  $2V \cap (\mathbf{a}_1 + 2V)$  must contain the six distinct vectors  $\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3, \mathbf{v}_1 + \mathbf{v}_2, \mathbf{v}_1 + \mathbf{v}_3, \mathbf{v}_2 + \mathbf{v}_3$ . Thus  $|2V_1| \leq 2|2V| - 6 \leq 2|V_1| - 2$ . Again, applying Theorem 16.2.1 to  $V_1$ , we conclude that  $V_1$  is a linear tile. Hence so is  $V$ .

(ii) A similar argument yields  $|2V_1| \leq 2|V_1| + 2$  in this case. Since  $\mathcal{R}(V) > 5$  it follows that  $2V_1 = 2V \cup (\mathbf{a}_1 + 2V) \neq \langle V \rangle$ , or in other words  $\mathcal{R}(V_1) > 2$ . Hence, the proof of case (i) may be used to establish that  $V_1$ , and therefore also  $V$ , is a linear tile.

(iii) Again,  $|2V_1| \leq 2|2V| - 6 \leq 2(2|V| + 5) - 6 = 2|V_1| + 4$ . Every element in  $5V_1$  is a sum of at most eight elements of  $V$ , and  $\mathcal{R}(V) > 8$ , and therefore  $\mathcal{R}(V_1) > 5$ . Now the proof of case (ii) applies.  $\square$

## 16.3 Small tiles

In this section we completely characterize all tiles of size at most eight. In addition, we also consider tilings with sets of large rank. First, we have the simple

**Theorem 16.3.1** *If  $|V| \leq 4$ , then  $V$  is a tile.*

**Proof.** Notice that  $|2V| \leq \binom{|V|}{2} + 1$ , and for  $|V| \leq 4$  we have  $\binom{|V|}{2} + 1 < 2|V|$ . Hence  $V$  is a linear tile by Theorem 16.2.1.  $\square$

Next we classify tiles of size eight. Let  $V = \{\mathbf{0}, \mathbf{v}_1, \dots, \mathbf{v}_7\} \subseteq \mathbb{F}^n$ . We distinguish between several cases according to the rank of  $V$ .

**Lemma 16.3.2** *If  $\text{rank}(V) = 7$ , then  $V$  is a tile.*

**Proof.** Consider  $\mathcal{H}_3$ , the perfect binary Hamming code of length seven. Define

$$A = \{ \mathbf{a} = c_1 \mathbf{v}_1 + c_2 \mathbf{v}_2 + \dots + c_7 \mathbf{v}_7 : (c_1, c_2, \dots, c_7) \in \mathcal{H}_3 \}.$$

We claim that  $(V, A)$  is a tiling of  $\langle V \rangle$ , which suffices by Theorem 16.1.2. Since  $|V| = 2^3$ ,  $|A| = 2^4$  and  $|\langle V \rangle| = 2^7$ , it would suffice to show that  $2V \cap 2A = \{\mathbf{0}\}$ . If  $\mathbf{a}_1 + \mathbf{a}_2 \in 2V$  for some distinct  $\mathbf{a}_1, \mathbf{a}_2 \in A$ , then there are two distinct codewords in  $\mathcal{H}_3$  at distance at most two from each other. However, since the minimum distance of  $\mathcal{H}_3$  is three, this is a contradiction.  $\square$

Note that the proof of Lemma 16.3.2 amounts to choosing the appropriate coordinates for  $\langle V \rangle$ , so that the set  $V$  of rank seven becomes the Hamming sphere  $B_1^7(\mathbf{0})$ . In general, we may always assume without loss of generality that  $B_1^r(\mathbf{0}) \subseteq V$ , where  $r = \text{rank}(V)$  (here, by a slight abuse of notation, we drop  $n - r$  zero coordinates).

Now let  $\text{rank}(V) = 6$ . Then, after a suitable choice of coordinates for  $\langle V \rangle$ , we have  $V = B_1^6(\mathbf{0}) \cup \{\mathbf{x}\}$ , where  $\mathbf{x} \in \mathbb{F}^6$  is of weight at least two.

**Lemma 16.3.3** *The set  $V$  is a tile if and only if  $w(\mathbf{x}) \neq 4, 5$ .*

**Proof.** Follows from Theorem 16.3.10 below and the remark after it.  $\square$

Let  $\text{rank}(V) = 5$ . Again, with a suitable choice of coordinates,  $V = B_1^5(\mathbf{0}) \cup \{\mathbf{x}, \mathbf{y}\}$ , where  $\mathbf{x}, \mathbf{y} \in \mathbb{F}^5$ , and  $w(\mathbf{x}) \geq w(\mathbf{y}) \geq 2$ .

**Lemma 16.3.4** *The set  $V$  is a tile if and only if one of the following holds:*

- (i)  $w(\mathbf{x}) = 2$ ,  $w(\mathbf{y}) = 2$  and  $w(\mathbf{x} + \mathbf{y}) = 2$ ;
- (ii)  $w(\mathbf{x}) = 3$ ,  $w(\mathbf{y}) = 2$  and  $w(\mathbf{x} + \mathbf{y}) = 1$ ;
- (iii)  $w(\mathbf{x}) = 3$ ,  $w(\mathbf{y}) = 2$  and  $w(\mathbf{x} + \mathbf{y}) = 5$ ;
- (iv)  $w(\mathbf{x}) = 3$ ,  $w(\mathbf{y}) = 3$  and  $w(\mathbf{x} + \mathbf{y}) = 2$ .

**Proof.** Note that  $2V$  may be written as  $B_2^5(\mathbf{0}) \cup B_1^5(\mathbf{x}) \cup B_1^5(\mathbf{y}) \cup \{\mathbf{x} + \mathbf{y}\}$ . Hence,  $V$  is a tile of  $\langle V \rangle$  if and only if there exists a set  $A \subset \mathbb{F}^5$  of cardinality four, such that

$$2A \cap B_2^5(\mathbf{0}) = \{\mathbf{0}\}, \tag{16.3.5}$$

$$2A \cap B_1^5(\mathbf{x}) = 2A \cap B_1^5(\mathbf{y}) = 2A \cap \{\mathbf{x} + \mathbf{y}\} = \emptyset. \tag{16.3.6}$$

Condition (16.3.5) means that the Hamming distance between any two vectors in  $A$  is at least three. Since the  $(5, 4, 3)$  binary code is clearly unique, we have that

$$A = \{00000, 11100, 10011, 01111\} \tag{16.3.7}$$

up to a permutation of coordinates. Note that  $A$  is linear, and therefore  $2A = A$ . Hence, condition (16.3.6) translates into

$$d(\mathbf{x}, A) \geq 2, \quad d(\mathbf{y}, A) \geq 2, \quad \mathbf{x} + \mathbf{y} \notin A. \quad (16.3.8)$$

The cases (i), (ii), (iii), (iv) may be now derived by inspection from (16.3.7) and (16.3.8).  $\square$

For  $\text{rank}(V) = 4$  we have  $V = B_1^4(\mathbf{0}) \cup \{\mathbf{x}, \mathbf{y}, \mathbf{z}\}$ . In this case it is obvious (from Corollary 16.2.2) that  $V$  is a tile if and only if  $2V \neq \langle V \rangle$ .

**Lemma 16.3.9** *The set  $V$  is a tile if and only if one of the following holds:*

- (i)  $w(\mathbf{x}) = w(\mathbf{y}) = w(\mathbf{z}) = 2$  and  $w(\mathbf{x} + \mathbf{y}) = w(\mathbf{x} + \mathbf{z}) = w(\mathbf{y} + \mathbf{z}) = 2$ ;
- (ii)  $w(\mathbf{x}) = w(\mathbf{y}) = 2$ ,  $w(\mathbf{z}) = 3$  and  $w(\mathbf{x} + \mathbf{y}) = 2$ ,  $w(\mathbf{x} + \mathbf{z}) = w(\mathbf{y} + \mathbf{z}) = 1$ ;
- (iii)  $w(\mathbf{x}) = 2$ ,  $w(\mathbf{y}) = w(\mathbf{z}) = 3$  and either  $w(\mathbf{x} + \mathbf{y}) = 1$  or  $w(\mathbf{x} + \mathbf{z}) = 1$ ;
- (iv)  $w(\mathbf{x}) = w(\mathbf{y}) = w(\mathbf{z}) = 3$ .

**Proof.** All we need to show is that there exists a vector in  $\mathbb{F}^4$  which is not a sum of two elements from  $B_1^4(\mathbf{0}) \cup \{\mathbf{x}, \mathbf{y}, \mathbf{z}\}$ . This is easily done by inspection. For instance, (1111) is such a vector in case (i), and so  $A = \{0000, 1111\}$ . In all other cases  $A$  has the form  $\{0000, 1110\}$ .  $\square$

Finally, if  $\text{rank}(V) = 3$  then  $V$  is linear, and hence is a trivial tile. Note that the foregoing classification shows that in all cases where  $|V| \leq 8$  and  $V$  is a tile, it is also a linear tile. This also follows directly from Corollary 16.6.4.

We now consider tiles of large rank, that is, those tiles for which  $r = \text{rank}(V)$  is close to the upper bound  $|V| - 1$ . For instance, if  $\text{rank}(V) = |V| - 1$ , then, without loss of generality,  $V = B_1^r(\mathbf{0})$  and is therefore a tile. If  $\text{rank}(V) = |V| - 2$ , then without loss of generality,  $V = B_1^r(\mathbf{0}) \cup \{\mathbf{x}\}$  for some  $\mathbf{x} \in \mathbb{F}^r$  of weight  $\geq 2$ .

**Theorem 16.3.10** *If  $V = B_1^r(\mathbf{0}) \cup \{\mathbf{x}\}$ , then  $V$  is a linear tile, provided  $w(\mathbf{x}) \neq r - 2, r - 1$ .*

**Proof.** We have  $2V = B_2^r(\mathbf{0}) \cup B_1^r(\mathbf{x})$  with  $r = 2^k - 2$ . Thus, we may take  $A$  to be an  $[r, r - k, 3]$  linear code, obtained by shortening the  $[r + 1, r - k + 1, 3]$  Hamming code  $\mathcal{H}_k$ , provided  $d(\mathbf{x}, 2A) = d(\mathbf{x}, A) \geq 2$ . For any  $3 \leq w \leq r - 2$  or  $w = r + 1$  it is known that there exists a codeword  $\mathbf{c} \in \mathcal{H}_k$  of weight  $w$ . Hence, if  $w(\mathbf{x}) \neq r - 2, r - 1$ , we may always find a permutation of the coordinates of  $\mathcal{H}_k$  such that  $\mathbf{c}$  coincides with  $\mathbf{x}$  in the first  $r$  coordinates and

has a 1 in the last coordinate. Again, shortening in the last coordinate, we obtain  $A$  with  $d(\mathbf{x}, A) \geq 2$ .  $\square$

It follows from the proof of Theorem 16.3.10 that if a tiling  $(V, A)$  exists, then  $A$  must have the parameters  $(n, K, d)$  of a shortened Hamming code. Further, it is easy to show that there cannot be a vector of weight  $n - 2$  or  $n - 1$  at distance at least two from any shortened perfect code  $C$  of length  $n = 2^k - 2$  (either linear or nonlinear): indeed, let  $\mathbf{x}$  be such a vector, and  $D = C_0 \cup C_1$  be a perfect code of length  $n + 1$ , where  $C_0 = \{(\mathbf{c}|0) : \mathbf{c} \in C\}$  and  $C_1 = \{(\mathbf{c}|1) : \mathbf{c} \in C'\}$  for some  $C'$ . Since  $d((\mathbf{x}|0), D) \leq 1$  while  $d((\mathbf{x}|0), C_0) \geq 2$ , it follows that  $d((\mathbf{x}|0), C_1) \leq 1$ . Therefore  $\mathbf{x} \in C'$  and hence  $D$  contains a codeword of weight  $n - 1$  or  $n$ , which is impossible. Thus, if all codes with the parameters  $(2^k - 2, 2^{2^k-k-2}, 3)$  can be obtained by shortening a perfect code, then no tiling is possible for  $w(\mathbf{x}) = r - 2$  or  $w(\mathbf{x}) = r - 1$ . This is certainly true for  $k = 3$ , since the  $(6, 8, 3)$  code is, as easily checked, unique. This establishes the “only if” part of the statement in Lemma 16.3.3.

The idea of constructing tilings from shortened Hamming codes may be employed to show the existence of certain tiles.

**Theorem 16.3.11** *Let  $V = B_1^n(\mathbf{0}) \cup S$  with  $n = 2^k - |S| - 1$ . Then  $V$  is a linear tile, provided  $\text{supp}(S) = \bigcup_{\mathbf{x} \in S} \text{supp}(\mathbf{x})$  has size at most  $k$ .*

**Proof.** Consider the parity check matrix  $\mathbf{H}$  of the Hamming code of length  $2^k - 1$ . Without loss of generality, let the columns of weight 1 in  $\mathbf{H}$  correspond to positions in  $\text{supp}(S)$ , and denote  $\mathbf{s}(\mathbf{x}) = \mathbf{Hx}^T$ . Then, for all distinct  $\mathbf{x}, \mathbf{y} \in S$ ,  $w(\mathbf{s}(\mathbf{x})) \geq 2$  and  $\mathbf{s}(\mathbf{x}) \neq \mathbf{s}(\mathbf{y})$ . Shorten the Hamming code  $|S|$  times by deleting those columns of  $\mathbf{H}$  that correspond to  $\mathbf{s}(\mathbf{x})$  for  $\mathbf{x} \in S$ . The resulting code  $A$  satisfies  $d(\mathbf{x}, A) \geq 2$  for all  $\mathbf{x} \in S$  and  $2S \cap A = \{\mathbf{0}\}$ . Hence  $(V, A)$  is a tiling.  $\square$

For example,

$$V = B_1^{28}(\mathbf{0}) \cup \{(110^{26}), (10110^{24}), (010110^{23})\}$$

is a linear tile by Theorem 16.3.11.

## 16.4 Periodicity of tilings

A tile  $V$  of  $\mathbb{F}^n$  is *periodic* if there exists a nonzero  $\mathbf{v} \in \mathbb{F}^n$ , such that  $\mathbf{v} + V = V$ . Note that since  $\mathbf{0} \in V$  by assumption, we must have  $\mathbf{v} \in V$ . We call  $\mathbf{v}$  a *periodic point* or *stabilizer* of  $V$ . Given a tiling  $(V, A)$  of  $\mathbb{F}^n$ , we say that it is *nonperiodic* if both  $V$  and  $A$  are nonperiodic.

**Theorem 16.4.1** *Let*

$$V = \{\mathbf{0}, \mathbf{v}_1, \dots, \mathbf{v}_7\} = \left\{ \begin{array}{ccccccc} 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{array} \right\}, \quad (16.4.2)$$

$$A = \{\mathbf{0}, \mathbf{a}_1, \dots, \mathbf{a}_7\} = \left\{ \begin{array}{ccccccc} 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{array} \right\}, \quad (16.4.3)$$

where the elements of  $V, A \subset \mathbb{F}^6$  are represented as column vectors. Then  $(V, A)$  is a nonperiodic tiling of  $\mathbb{F}^6$ .

**Proof.** To see that  $(V, A)$  is a tiling define  $A_0 = \{\mathbf{0}, \mathbf{a}_1, \mathbf{a}_2, \mathbf{a}_3\}$  and  $A_1 = \{\mathbf{a}_4, \mathbf{a}_5, \mathbf{a}_6, \mathbf{a}_7\}$ . Then obviously  $2V \cap (A_0 + A_1) = \emptyset$  (consider the last row in (16.4.2), (16.4.3) above), and it remains to show that  $2V \cap 2A_0 = 2V \cap 2A_1 = \{\mathbf{0}\}$ . Note that the first five rows of (16.4.2) correspond to  $B_1^5(0) \cup \{\mathbf{x}, \mathbf{y}\}$  with  $w(\mathbf{x} + \mathbf{y}) = 5$ , while the first five rows in both  $A_0$  and  $A_1$  are isomorphic to the tile set in (16.3.7). Thus,  $2V \cap 2A_0 = 2V \cap 2A_1 = \{\mathbf{0}\}$ , by the proof of Lemma 16.3.4. To see that  $(V, A)$  is nonperiodic, observe that  $\text{rank}(V) = \text{rank}(A) = 5$ . It is obvious that a set of cardinality 8 and rank 5 cannot be periodic.  $\square$

We now show that the nonperiodic tiling of Theorem 16.4.1 is the smallest possible.

**Theorem 16.4.4** *If  $(V, A)$  is a nonperiodic tiling, then  $|V| \geq 8$  and  $|A| \geq 8$ .*

**Proof.** Obviously, any tile of cardinality 2 is linear and, hence, periodic. Now let  $(V, A)$  be a tiling of  $\mathbb{F}^n$  with  $|A| = 4$ . We claim that either  $A$  is linear or  $V$  is periodic. Indeed, let  $A = \{\mathbf{0}, \mathbf{a}, \mathbf{b}, \mathbf{c}\}$  and define  $A' = \{\mathbf{0}, \mathbf{a}, \mathbf{b}, \mathbf{a} + \mathbf{b}\}$ . Then  $2A' \subseteq 2A$  which implies  $2V \cap 2A' = \{\mathbf{0}\}$ . Hence, both  $(V, A)$  and  $(V, A')$  are tilings of  $\mathbb{F}^n$ , and therefore we must have  $\mathbf{c} + V = (\mathbf{a} + \mathbf{b}) + V$ . This is only possible if  $\mathbf{c} = \mathbf{a} + \mathbf{b}$ , in which case  $A$  is linear, or if  $\mathbf{c} = (\mathbf{a} + \mathbf{b}) + \mathbf{v}$ , where  $\mathbf{v}$  is a periodic point of  $V$ .  $\square$

We now describe a general construction of tilings in  $\mathbb{F}^n$  which shows that nonperiodic tilings exist for all odd  $n \geq 7$ . Let  $\nu = 2^m - 1$ ,  $m \geq 3$ , and

let  $\mathbf{h}_1, \mathbf{h}_2, \dots, \mathbf{h}_\nu$  be the distinct nonzero elements of  $\mathbb{F}^m$ , arranged in some fixed, say lexicographical order. Fix a permutation  $\pi$  on the set  $\{1, 2, \dots, \nu\}$  and consider  $A_0, A_1, V \subset \mathbb{F}^{2m+1}$  given by

$$A_0 = \left\{ \begin{array}{cccccc} 0 & \mathbf{h}_1 & \mathbf{h}_2 & \dots & \mathbf{h}_\nu \\ 0 & 0 & 0 & \dots & 0 \\ 0 & 0 & 0 & \dots & 0 \end{array} \right\}, \quad (16.4.5)$$

$$A_1 = \left\{ \begin{array}{cccccc} 0 & 0 & 0 & \dots & 0 \\ 0 & \mathbf{h}_1 & \mathbf{h}_2 & \dots & \mathbf{h}_\nu \\ 1 & 1 & 1 & \dots & 1 \end{array} \right\}, \quad (16.4.6)$$

$$V = \left\{ \begin{array}{cccccc} 0 & \mathbf{h}_1 & \mathbf{h}_2 & \dots & \mathbf{h}_\nu \\ 0 & \mathbf{h}_{\pi(1)} & \mathbf{h}_{\pi(2)} & \dots & \mathbf{h}_{\pi(\nu)} \\ 0 & 0 & 0 & \dots & 0 \end{array} \right\}, \quad (16.4.7)$$

where the elements of  $A_0, A_1, V$  are again represented as column vectors.

**Theorem 16.4.8** *Let  $A = A_0 \cup A_1$ . If*

$$\pi = (1, 4, 2)(3, 6)(5, 7)(8, 9)(10, 11) \dots (\nu - 1, \nu)$$

for  $\nu > 7$  and

$$\pi = (1, 4, 2)(3, 6)(5, 7)$$

when  $\nu = 7$ , then  $(V, A)$  is a nonperiodic tiling of  $\mathbb{F}^{2m+1}$ , for  $m \geq 3$ .

**Proof.** Straightforward. □

To exhibit nonperiodic tilings of  $\mathbb{F}^n$  for even  $n$ ,  $n \geq 6$ , we use a variant of the same construction. As before, let  $\nu = 2^m - 1$ ,  $m \geq 2$ . Now let  $\pi$  be any derangement (a permutation with no fixed element) of the set  $\{1, 2, \dots, \nu\}$ . Define  $A, V \subset \mathbb{F}^{2m+2}$  as follows:

$$A = \left\{ \begin{array}{cccccc} 0 & \mathbf{h}_1 & \mathbf{h}_2 & \dots & \mathbf{h}_\nu \\ 0 & 0 & 0 & \dots & 0 \\ 0 & 0 & 0 & \dots & 0 \\ 0 & 0 & 0 & \dots & 0 \end{array} \right\}$$

$$\cup \left\{ \begin{array}{cccccc} 0 & 0 & 0 & \dots & 0 \\ 0 & \mathbf{h}_1 & \mathbf{h}_2 & \dots & \mathbf{h}_\nu \\ 1 & 1 & 1 & \dots & 1 \\ 0 & 0 & 0 & \dots & 0 \end{array} \right\},$$

$$V = \left\{ \begin{array}{cccccc} 0 & \mathbf{h}_1 & \mathbf{h}_2 & \dots & \mathbf{h}_\nu \\ 0 & \mathbf{h}_{\pi(1)} & \mathbf{h}_{\pi(2)} & \dots & \mathbf{h}_{\pi(\nu)} \\ 0 & 0 & 0 & \dots & 0 \\ 0 & 0 & 0 & \dots & 0 \end{array} \right\} \cup$$

$$\bigcup \left\{ \begin{array}{cccccc} \mathbf{0} & h_1 & h_2 & \dots & h_\nu \\ \mathbf{0} & h_1 & h_2 & \dots & h_\nu \\ 0 & 0 & 0 & \dots & 0 \\ 1 & 1 & 1 & \dots & 1 \end{array} \right\}.$$

**Theorem 16.4.9** *With  $V$  and  $A$  as defined above,  $(V, A)$  is a nonperiodic tiling of  $\mathbb{F}^{2m+2}$  for  $m \geq 2$ .*

**Proof.** Routine. □

We can now state the main result of this section.

**Theorem 16.4.10** *Nonperiodic tilings of  $\mathbb{F}^n$  exist if and only if  $n \geq 6$ .*

**Proof.** This follows immediately by combining Theorems 16.4.4, 16.4.8 and 16.4.9. □

## 16.5 Recursive decomposition of tilings

In this section we present a recursive decomposition (construction) of tilings, which shows that any tiling of  $\mathbb{F}^n$  may be decomposed into (constructed from) smaller tilings of certain particular type.

In view of Theorem 16.1.2, we are particularly interested in those tilings  $(V, A)$  for which  $\mathbb{F}^n = \langle V \rangle$ . Note that until now the order of the sets in the tiling pair  $(V, A)$  was of no importance, since the roles of  $V$  and  $A$  were symmetric; however, this is no longer true if we require  $\langle V \rangle = \mathbb{F}^n$ .

**Definition 16.5.1** *The ordered pair  $(V, A)$  is a proper tiling of  $\mathbb{F}^n$  if  $(V, A)$  is a tiling of  $\mathbb{F}^n$  and  $\langle V \rangle = \mathbb{F}^n$ .*

The following theorem shows that the classification of all tilings in  $\mathbb{F}^n$  may be, in principle, reduced to the study of proper tilings. Let  $V$  be a tile of  $\mathbb{F}^n$  with  $\langle V \rangle \neq \mathbb{F}^n$ , or equivalently  $\text{rank}(V) < n$ . Denote  $m = 2^{n-r} - 1$ , where  $r = \text{rank}(V)$ .

**Theorem 16.5.2** *The pair  $(V, A)$  is a tiling of  $\mathbb{F}^n$  if and only if  $A$  has the following form:*

$$A = A_0 \cup (v_1 + c_1 + A_1) \cup \dots \cup (v_m + c_m + A_m), \quad (16.5.3)$$

where

- (i) for  $i = 0, 1, \dots, m$ ,  $A_i$  is a subset of  $\langle V \rangle$ , such that  $(V, A_i)$  is a tiling of  $\langle V \rangle$ ;
- (ii)  $\{c_0 = \mathbf{0}, c_1, \dots, c_m\}$  is a set of representatives for  $\mathbb{F}^n / \langle V \rangle$ ;
- (iii) for  $i = 1, \dots, m$ ,  $v_i$  is an element of  $\langle V \rangle$ .

**Proof.** ( $\Leftarrow$ ) Let  $A$  be as in (16.5.3), and  $|V| = 2^k$ . Then  $|A_i| = 2^{r-k}$  for all  $i$ , and  $|A| = (m+1)2^{r-k} = 2^{n-k}$ . Hence, it remains to show that  $2V \cap 2A = \{\mathbf{0}\}$ . We have  $2A = \mathcal{U} \cup \mathcal{W}$ , where  $\mathcal{U} = \bigcup_{i=0}^m 2A_i$  and (set  $\mathbf{v}_0 = \mathbf{0}$ )  $\mathcal{W} = \bigcup_{0 \leq i < j \leq m} (\mathbf{v}_i + \mathbf{v}_j + \mathbf{c}_i + \mathbf{c}_j + A_i + A_j)$ .

Now,  $2V \cap \mathcal{U} = \{\mathbf{0}\}$  since  $2V \cap 2A_i = \{\mathbf{0}\}$  for all  $i$ , and  $2V \cap \mathcal{W} = \emptyset$  since  $\langle V \rangle$  and  $\mathcal{W}$  are disjoint.

( $\Rightarrow$ ) Let  $(V, A)$  be a tiling of  $\mathbb{IF}^n$ . Pick any set of representatives  $\{\mathbf{c}_0 = \mathbf{0}, \mathbf{c}_1, \mathbf{c}_2, \dots, \mathbf{c}_m\}$  for  $\mathbb{IF}^n/\langle V \rangle$  and define

$$A_i = \mathbf{v}_i + \mathbf{c}_i + (A \cap (\mathbf{c}_i + \langle V \rangle))$$

where  $\mathbf{v}_i$  is any element of  $\langle V \rangle$  such that  $\mathbf{0} \in A_i$  (set  $\mathbf{v}_0 = \mathbf{0}$ ). To see that such  $\mathbf{v}_i$  exists, note that  $\mathbf{c}_i + (A \cap (\mathbf{c}_i + \langle V \rangle)) \subseteq \langle V \rangle$ . We have  $\mathbf{v}_i + \mathbf{c}_i + A_i = A \cap (\mathbf{c}_i + \langle V \rangle)$  and, hence,

$$\bigcup_{i=0}^m (\mathbf{v}_i + \mathbf{c}_i + A_i) = \bigcup_{i=0}^m A \cap (\mathbf{c}_i + \langle V \rangle) = A. \quad (16.5.4)$$

We need to show that  $(V, A_i)$  is a tiling of  $\langle V \rangle$  for all  $i$ . Clearly  $2A_i = (A \cap (\mathbf{c}_i + \langle V \rangle)) + (A \cap (\mathbf{c}_i + \langle V \rangle)) \subseteq 2A$ , and therefore  $2V \cap 2A_i = \{\mathbf{0}\}$ . Note that  $A_i \subseteq \langle V \rangle$ , which implies  $V + A_i \subseteq \langle V \rangle$ . Thus, to establish that  $(V, A_i)$  is a tiling of  $\langle V \rangle$ , it remains to show that  $|A_i| = 2^{r-k}$ . Since  $2V \cap 2A_i = \{\mathbf{0}\}$ , we obviously have  $|A_i| \leq 2^{r-k}$ . However,  $(m+1)2^{r-k} = 2^{n-k} = |A| \leq \sum_{i=0}^m |A_i|$ , where the last inequality follows from (16.5.4). This implies that  $|A_i| = 2^{r-k}$  and completes the proof.  $\square$

The analysis of Theorem 16.5.2 shows that if all the proper tilings of  $\mathbb{IF}^r$  are known for  $r = 1, 2, \dots, n$ , we can construct all the tilings of  $\mathbb{IF}^n$ . However, the set of all the proper tilings is not the smallest class of tilings which permits complete classification of all tilings of  $\mathbb{IF}^n$ . Indeed, let  $(V, A)$  be a tiling of  $\langle V \rangle$  and consider the tiling  $(A, V)$ . Unless  $\text{rank}(A) = \text{rank}(V)$ , this tiling is not proper with respect to  $\langle V \rangle$ , and, putting  $m = 2^{\text{rank}(V) - \text{rank}(A)} - 1$  and using Theorem 16.5.2:

$$V = V_0 \cup (\mathbf{a}_1 + \mathbf{c}_1 + V_1) \cup \dots \cup (\mathbf{a}_m + \mathbf{c}_m + V_m) \quad (16.5.5)$$

where  $\mathbf{a}_1, \mathbf{a}_2, \dots, \mathbf{a}_m \in \langle A \rangle$ ,  $\mathbf{0}, \mathbf{c}_1, \dots, \mathbf{c}_m$  are representatives of  $\langle V \rangle/\langle A \rangle$  and for all  $i$ ,  $(A, V_i)$  is a proper tiling of  $\langle A \rangle$ . Thus, using (16.5.5), each of the tilings  $(V, A_i)$  of  $\langle V \rangle$  in Theorem 16.5.2 may be decomposed into yet smaller tilings, unless  $\langle A_i \rangle = \langle V \rangle$ . This process may be iterated until a complete decomposition of the original tiling  $(V, A)$  is obtained.

**Example 16.5.6** Consider the tiling of  $\mathbb{IF}^6$  given in (16.4.2) and (16.4.3). This tiling is not proper since  $\text{rank}(V) = \text{rank}(A) = 5 < 6$ . If we take

$\mathbf{c}_0 = \mathbf{0}$  and  $\mathbf{c}_1 = (000001)$  as the representatives of  $\mathbb{F}^6/\langle V \rangle$ , we can write  $A = A_0 \cup (\mathbf{c}_1 + A_1)$  with

$$A_0 = \left\{ \begin{array}{cccc} 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{array} \right\},$$

$$A_1 = \left\{ \begin{array}{cccc} 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 \end{array} \right\}.$$

Since  $\text{rank}(A_0) = \text{rank}(A_1) = 2 < \text{rank}(V)$ , we may further decompose  $(V, A_0)$  and  $(V, A_1)$  as follows. Let  $\mathbf{0}, \mathbf{c}_{0,1}, \dots, \mathbf{c}_{0,7}$  and  $\mathbf{0}, \mathbf{c}_{1,1}, \dots, \mathbf{c}_{1,7}$  be the representatives of  $\langle V \rangle/\langle A_0 \rangle$  and  $\langle V \rangle/\langle A_1 \rangle$ , respectively. We may take, for instance,

$$\{\mathbf{c}_{0,1}, \mathbf{c}_{0,2}, \dots, \mathbf{c}_{0,7}\} = \{\mathbf{c}_{1,1}, \mathbf{c}_{1,2}, \dots, \mathbf{c}_{1,7}\}$$

$$= \left\{ \begin{array}{ccccccc} 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{array} \right\}.$$

Then the corresponding decompositions of  $V$  are given by

$$V = V_{0,0} \cup (\mathbf{a}_{0,1} + \mathbf{c}_{0,1} + V_{0,1}) \cup \dots \cup (\mathbf{a}_{0,7} + \mathbf{c}_{0,7} + V_{0,7}),$$

$$V = V_{1,0} \cup (\mathbf{a}_{1,1} + \mathbf{c}_{1,1} + V_{1,1}) \cup \dots \cup (\mathbf{a}_{1,7} + \mathbf{c}_{1,7} + V_{1,7}),$$

where

$$\mathbf{a}_{0,1}, \mathbf{a}_{0,2}, \dots, \mathbf{a}_{0,7} = \mathbf{0}, \mathbf{0}, (110100), \mathbf{0}, (101010), (011110), \mathbf{0} \in \langle A_0 \rangle,$$

$$\mathbf{a}_{1,1}, \mathbf{a}_{1,2}, \dots, \mathbf{a}_{1,7} = \mathbf{0}, \mathbf{0}, (110010), \mathbf{0}, (101110), (011100), \mathbf{0} \in \langle A_1 \rangle,$$

and

$$V_{0,0} = \dots = V_{0,7} = V_{1,0} = \dots = V_{1,7} = \{\mathbf{0}\}.$$

Indeed, since  $A_0$  and  $A_1$  are linear, both  $(A_0, V_{0,i}) = (A_0, \{\mathbf{0}\})$  and  $(A_1, V_{1,i}) = (A_1, \{\mathbf{0}\})$  are trivial tilings of  $\langle A_0 \rangle = A_0$  and  $\langle A_1 \rangle = A_1$ , respectively.  $\square$

As illustrated in this example, the decomposition of (16.5.3) and (16.5.5) terminates when trivial tilings, of the form  $(V, \{0\})$  with  $V$  linear, are obtained. The only other case when the recursion of (16.5.3), (16.5.5) stops is when a tiling  $(V, A)$  with  $\langle V \rangle = \langle A \rangle$  is encountered.

A tiling  $(V, A)$  of  $\mathbb{F}^n$  is said to be of *full rank* if  $\langle V \rangle = \langle A \rangle$ .

In fact, if a tiling  $(V, A)$  of  $\mathbb{F}^n$  is of full rank, then  $\langle V \rangle = \langle A \rangle \supseteq V + A = \mathbb{F}^n$ , i.e.,  $\text{rank}(V) = \text{rank}(A) = n$ . Any tiling of  $\mathbb{F}^n$  can be constructed from the trivial tilings and tilings of full rank.

## 16.6 Tilings and perfect binary codes

In this section we show that each tiling  $(V, A)$  of  $\mathbb{F}^n$  is uniquely associated with a perfect binary code of length  $\nu = |V| - 1$ . Let  $\mathbf{H}(V^*)$  be an  $n \times \nu$  matrix having the elements of  $V \setminus \{0\}$ , arranged in some fixed order, as its columns. For  $\mathbf{x} \in \mathbb{F}^\nu$  let  $\mathbf{s}(\mathbf{x}) = \mathbf{H}(V^*)\mathbf{x}^T$  denote the syndrome of  $\mathbf{x}$  with respect to  $\mathbf{H}(V^*)$ .

**Theorem 16.6.1** *Let*

$$C = \{ \mathbf{c} \in \mathbb{F}^\nu : \mathbf{s}(\mathbf{c}) = \mathbf{H}(V^*)\mathbf{c}^T \in A \}. \quad (16.6.2)$$

*Then  $C$  is a perfect code of length  $\nu$ .*

**Proof.** We first show that  $d(C) \geq 3$ . Denote  $\mathbf{a}_1 = \mathbf{s}(\mathbf{c}_1)$  and  $\mathbf{a}_2 = \mathbf{s}(\mathbf{c}_2)$ , where  $\mathbf{a}_1, \mathbf{a}_2 \in A$  by (16.6.2). Suppose that  $\mathbf{a}_1 = \mathbf{a}_2$ , or equivalently  $\mathbf{s}(\mathbf{c}_1 + \mathbf{c}_2) = \mathbf{0}$ . Then  $d(\mathbf{c}_1, \mathbf{c}_2) = w(\mathbf{c}_1 + \mathbf{c}_2) \geq 3$  since the columns of  $\mathbf{H}(V^*)$  are distinct. Now suppose that  $\mathbf{a}_1 \neq \mathbf{a}_2$ . Note that  $\mathbf{a}_1 + \mathbf{a}_2 = \mathbf{s}(\mathbf{c}_1 + \mathbf{c}_2) = \sum_{i \in \text{supp}(\mathbf{c}_1 + \mathbf{c}_2)} \mathbf{v}_i$ . Further note that  $\mathbf{a}_1 + \mathbf{a}_2 \notin 2V$ , since  $2V \cap 2A = \{\mathbf{0}\}$ . Hence again  $d(\mathbf{c}_1, \mathbf{c}_2) = |\text{supp}(\mathbf{c}_1 + \mathbf{c}_2)| \geq 3$ . It remains to show that  $d(\mathbf{x}, C) \leq 1$  for all  $\mathbf{x} \in \mathbb{F}^\nu$ . Since  $V + A = \mathbb{F}^n$ , we have  $\mathbf{s}(\mathbf{x}) = \mathbf{v} + \mathbf{a}$  for some  $\mathbf{v} \in V$  and  $\mathbf{a} \in A$ . If  $\mathbf{v} = \mathbf{0}$  then  $\mathbf{x} \in C$  by (16.6.2) and we are done. Otherwise, let  $\mathbf{c} \in \mathbb{F}^\nu$  be a vector which coincides with  $\mathbf{x}$  in all positions except one, which is the position corresponding to the location of  $\mathbf{v}$  in  $\mathbf{H}(V^*)$ . Then  $d(\mathbf{x}, \mathbf{c}) = 1$ , and  $\mathbf{s}(\mathbf{c}) = \mathbf{a}$  which implies that  $\mathbf{c} \in C$  by (16.6.2).  $\square$

Theorem 16.6.1 provides a means for constructing a perfect code  $C$  from any given tiling  $(V, A)$ . We say that this code  $C$  is the perfect code *associated* with  $(V, A)$ .

**Theorem 16.6.3** *If  $C$  is the perfect code associated with a proper tiling  $(V, A)$  of  $\mathbb{F}^n$ , then*

$$\text{rank}(C) = |V| - 1 - \text{rank}(V) + \text{rank}(A).$$

**Proof.** Define  $C_0 = \{\mathbf{c} \in \mathbb{F}^\nu : \mathbf{s}(\mathbf{c}) = \mathbf{0}\}$ . Clearly,  $C_0$  is a linear code and  $\dim(C_0) = \nu - \text{rank}(V)$ . Now let  $A = \{\mathbf{0}, \mathbf{a}_1, \dots, \mathbf{a}_\mu\}$  where  $\mu = |A| - 1$ . Since  $\langle V \rangle = \mathbb{F}^n$  we can always find a set  $C_1 = \{\mathbf{0}, \mathbf{c}_1, \dots, \mathbf{c}_\mu\} \subset \mathbb{F}^\nu$  such that  $\mathbf{s}(\mathbf{c}_i) = \mathbf{a}_i$  for all  $i$ ,  $\text{rank}(C_1) = \text{rank}(A)$ , and  $\langle C_1 \rangle \cap C_0 = \{\mathbf{0}\}$ . Then obviously  $C = \bigcup_{\mathbf{c} \in C_1} (\mathbf{c} + C_0)$  and  $\text{rank}(C) = \dim(C_0) + \text{rank}(C_1) = \nu - \text{rank}(V) + \text{rank}(A)$ .  $\square$

Note that if  $(V, A)$  is not a *proper tiling* of  $\mathbb{F}^n$ , then Theorem 16.6.3 does not apply. This is so because for  $\text{rank}(V) < n$  there exist elements  $\mathbf{a} \in A$  which cannot be represented in the form  $\mathbf{H}(V^*)\mathbf{x}^T$  for any  $\mathbf{x} \in \mathbb{F}^\nu$ . In this case we have

$$\text{rank}(C) = \nu - \text{rank}(V) + \text{rank}(A_0) < \nu - \text{rank}(V) + \text{rank}(A)$$

where  $A_0 = A \cap \langle V \rangle$ .

Note also that  $C_0$  is a linear subcode of  $C$  (regardless of whether  $(V, A)$  is proper or not), and  $C$  itself is linear, that is, equivalent to the Hamming code of length  $\nu$  (see Section 11.2), if and only if  $A_0 = A \cap \langle V \rangle$  is linear. The following corollary is an immediate consequence of this fact.

**Corollary 16.6.4** *If  $|V| \leq 8$  and  $(V, A)$  is a proper tiling, then  $A$  is linear.*

**Proof.** The perfect code  $C$  associated with  $(V, A)$  has length at most seven and, hence, is equivalent either to the Hamming  $[7, 4, 3]$  code, or to the  $[3, 1, 3]$  repetition code (see the remark before Theorem 11.3.4).  $\square$

We conclude this section with a construction of proper tilings from perfect binary codes. This construction is, in a sense, the converse of Theorem 16.6.1. Let  $C$  be a perfect binary code of length  $\nu$ , and let  $\Gamma$  be a linear subcode of  $C$ , such that  $\Gamma + C = C$ . For instance, we may take as  $\Gamma$  any linear subspace of the set of all the periodic points of  $C$ . Denote  $\gamma = \dim(\Gamma)$ , and let  $\mathbf{H}(\Gamma)$  be a  $(\nu - \gamma) \times \nu$  parity check matrix of  $\Gamma$ . Note that the matrix  $\mathbf{H}(\Gamma)$  is of full rank by assumption. Take  $V = \{\mathbf{0}\} \cup \{\text{the columns of } \mathbf{H}(\Gamma)\}$  and define  $A = \{\mathbf{H}(\Gamma)\mathbf{c}^T : \mathbf{c} \in C\}$ .

**Theorem 16.6.5** *With  $V$  and  $A$  as defined above,  $(V, A)$  is a proper tiling of  $\mathbb{F}^{\nu-\gamma}$ .*

**Proof.** For  $\mathbf{x} \in \mathbb{F}^\nu$  let  $\mathbf{s}(\mathbf{x}) = \mathbf{H}(\Gamma)\mathbf{x}^T$ . We claim that

$$\mathbf{s}(\mathbf{x}) \in A \Rightarrow \mathbf{x} \in C. \quad (16.6.6)$$

Consider a vector  $\mathbf{x} \in \mathbb{F}^\nu$  such that  $\mathbf{s}(\mathbf{x}) = \mathbf{a} \in A$ . By the definition of  $A$ , there exists  $\mathbf{c} \in C$  such that  $\mathbf{s}(\mathbf{c}) = \mathbf{a}$ . Hence  $\mathbf{s}(\mathbf{x} + \mathbf{c}) = \mathbf{0}$ , which implies that  $\mathbf{x} + \mathbf{c} \in \Gamma$ . But since  $\Gamma + C = C$  it follows that  $\mathbf{x} = (\mathbf{x} + \mathbf{c}) + \mathbf{c} \in C$ .

It is now easy to see that  $d(C) = 3$  implies  $2V \cap 2A = \{\mathbf{0}\}$ . Suppose to the contrary that  $\mathbf{v}_1 + \mathbf{v}_2 = \mathbf{a}_1 + \mathbf{a}_2$  for some  $\mathbf{v}_1 \neq \mathbf{v}_2 \in V$  and  $\mathbf{a}_1 \neq \mathbf{a}_2 \in A$ . By the definition of  $A$  there exists a codeword  $\mathbf{c}_1 \in C$  such that  $s(\mathbf{c}_1) = \mathbf{a}_1$ . Let  $\mathbf{c}_2 \in \mathbb{F}^{\nu}$  be a vector which coincides with  $\mathbf{c}_1$  in all but the two positions corresponding to the locations of  $\mathbf{v}_1$  and  $\mathbf{v}_2$  in  $\mathbf{H}(\Gamma)$  (if, e.g.,  $\mathbf{v}_1 = \mathbf{0}$ , then  $\mathbf{c}_1$  and  $\mathbf{c}_2$  differ in one position). Then  $s(\mathbf{c}_2) = \mathbf{a}_1 + \mathbf{v}_1 + \mathbf{v}_2 = \mathbf{a}_2 \in A$ , and therefore  $\mathbf{c}_2 \in C$  by (16.6.6). This is a contradiction, since  $d(\mathbf{c}_1, \mathbf{c}_2) \leq 2$ .

Let  $\mathbf{x}' \in \mathbb{F}^{\nu-\gamma}$ . Since  $\langle V \rangle = \mathbb{F}^{\nu-\gamma}$ , there exists  $\mathbf{y} \in \mathbb{F}^{\nu}$  such that  $\mathbf{x}' = s(\mathbf{y})$ . If  $\mathbf{y} \in C$  then  $\mathbf{x}' \in A$ , and we are done. Otherwise, there exists a codeword  $\mathbf{c} \in C$  at distance 1 from  $\mathbf{y}$ . Let  $s(\mathbf{c}) = \mathbf{a} \in A$ . Then  $\mathbf{x}' = \mathbf{a} + \mathbf{v}$ , where  $\mathbf{v}$  is the column of  $\mathbf{H}(\Gamma)$  located at the position where  $\mathbf{c}$  and  $\mathbf{y}$  differ. So  $V + A = \mathbb{F}^{\nu-\gamma}$ .  $\square$

## 16.7 Nonexistence results

In this section we derive several necessary conditions for the existence of tilings. Our main result herein is a generalization of the Lloyd theorem (see Theorems 11.2.1 and 13.2.5) to arbitrary tiles.

For any  $\mathbf{u}, \mathbf{v} \in \mathbb{F}^n$  and  $V \subseteq \mathbb{F}^n$ , the characters  $\psi_{\mathbf{u}}(\cdot)$  are defined in the standard way (see Section 2.2):

$$\psi_{\mathbf{u}}(\mathbf{v}) = (-1)^{\langle \mathbf{u}, \mathbf{v} \rangle},$$

$$\psi_{\mathbf{u}}(V) = \sum_{\mathbf{v} \in V} \psi_{\mathbf{u}}(\mathbf{v}).$$

The distance distribution of a subset  $A \subseteq \mathbb{F}^n$  is given by

$$\mathcal{B}_i(A) = \frac{1}{|A|} \sum_{\mathbf{a} \in A} \mathcal{A}_i(\mathbf{a}),$$

where  $\mathcal{A}_i(\mathbf{a})$  is the number of vectors of weight  $i$  in  $\mathbf{a} + A$ . The MacWilliams transform of  $\mathcal{B}_i(A)$  is given by

$$\mathcal{B}_i^{\perp}(A) = \frac{1}{|A|} \sum_{j=0}^n \mathcal{B}_j(A) P_i(j),$$

where  $P_i(j)$  is the Krawtchouk polynomial (see Theorem 2.2.3).

Let  $(V, A)$  be a tiling of  $\mathbb{F}^n$ . Define the sets  $D(A), D^{\perp}(A) \subseteq \{0, 1, \dots, n\}$  as follows:

$$\begin{aligned} D(A) &= \{j : j \neq 0, \mathcal{B}_j(A) \neq 0\}, \\ D^{\perp}(A) &= \{j : j \neq 0, \mathcal{B}_j^{\perp}(A) \neq 0\}. \end{aligned}$$

Thus,  $D(A)$  is the set of nonzero distances occurring in  $A$  while  $D^\perp(A)$  is the set of nonzero distances occurring in the formal dual  $A^\perp = \{\mathbf{a} \in \mathbb{F}^n : \psi_{\mathbf{a}}(A) \neq 0\}$  of  $A$ . Further, let

$$\begin{aligned} U &= \{ \mathbf{u} \in \mathbb{F}^n : \psi_{\mathbf{u}}(V) = 0 \}, \\ \mathcal{W}(U) &= \{ j \in \{1, \dots, n\} : w(\mathbf{u}) = j \text{ for some } \mathbf{u} \in U \}. \end{aligned}$$

With this notation we have the following theorem.

**Theorem 16.7.1**  $D^\perp(A) \subseteq \mathcal{W}(U)$ .

**Proof.** Since  $A + V = \mathbb{F}^n$ , by (2.2.1) and (2.2.2), we have  $\psi_{\mathbf{u}}(V) \psi_{\mathbf{u}}(A) = \psi_{\mathbf{u}}(\mathbb{F}^n) = 0$  for all  $\mathbf{u} \neq \mathbf{0}$ .

Now, we use the fact (see the proof of Theorem 2.2.7) that

$$\frac{1}{|A|^2} \sum_{w(\mathbf{u})=j} |\psi_{\mathbf{u}}(A)|^2 = \mathcal{B}_j^\perp(A) \geq 0. \quad (16.7.2)$$

Let  $j \in \{1, 2, \dots, n\}$ . By definition,  $j \in D^\perp(A)$  if and only if  $\mathcal{B}_j^\perp(A) \neq 0$ . From (16.7.2) it follows that if  $\mathcal{B}_j^\perp(A) \neq 0$ , then there exists a vector  $\mathbf{u}$  of weight  $j$ , such that  $\psi_{\mathbf{u}}(A) \neq 0$ . Since  $\psi_{\mathbf{u}}(V) \psi_{\mathbf{u}}(A) = 0$  unless  $\mathbf{u} = \mathbf{0}$ , for this vector  $\mathbf{u}$  we must have  $\psi_{\mathbf{u}}(V) = 0$ . Hence  $\mathbf{u} \in U$  and  $j \in \mathcal{W}(U)$ .  $\square$

If  $V$  is the Hamming sphere of radius  $R$  and  $\mathbf{u} \in \mathbb{F}^n$  is a vector of weight  $j$ , then

$$\psi_{\mathbf{u}}(V) = \sum_{\mathbf{v} \in V} (-1)^{\langle \mathbf{u}, \mathbf{v} \rangle} = \sum_{i=0}^R \sum_{w(\mathbf{v})=i} (-1)^{\langle \mathbf{u}, \mathbf{v} \rangle} = \sum_{i=0}^R P_i(j).$$

This is precisely the Lloyd polynomial  $L_R(x)$  (see Section 11.2) evaluated at  $x = j$ . Thus, in this case  $\mathcal{W}(U)$  is just the set of integer zeros of  $L_R(x)$ , lying between 1 and  $n$ . Furthermore, if  $A$  is a perfect binary code, then  $|D^\perp(A)| = R$  — see (13.2.10). Thus, for tilings with Hamming spheres, Theorem 16.7.1 implies that the Lloyd polynomial  $L_R(x)$  has at least  $R$  distinct zeros in the set  $\{1, 2, \dots, n\}$ . This, together with  $\deg(L_R(x)) = R$ , is precisely the Lloyd theorem.

The following three theorems give additional necessary conditions for the existence of a tiling  $(V, A)$ .

**Theorem 16.7.3**  $A^\perp \subseteq U \cup \{\mathbf{0}\}$ .

**Proof.** Recall that  $A^\perp = \{\mathbf{a} \in \mathbb{F}^n : \psi_{\mathbf{a}}(A) \neq 0\}$ . The result now follows from the fact that  $\psi_{\mathbf{u}}(V)\psi_{\mathbf{u}}(A) = 0$  for  $\mathbf{u} \neq \mathbf{0}$ .  $\square$

**Theorem 16.7.4**  $|U| \geq |V| - 1$ .

**Proof.** Evidently,  $\max_{\mathbf{u} \in \mathbb{F}^n} |\psi_{\mathbf{u}}(A)| = |A|$ . Thus, taking into account that  $\psi_{\mathbf{u}}(A + A) = |\psi_{\mathbf{u}}(A)|^2 = 0$  for  $\mathbf{u} \notin U \cup \{\mathbf{0}\}$ , we have

$$\begin{aligned} \frac{1}{|A|^2} \sum_{\mathbf{u} \in \mathbb{F}^n} \psi_{\mathbf{u}}(A + A) &= \frac{1}{|A|^2} \sum_{\mathbf{u} \in U \cup \{\mathbf{0}\}} |\psi_{\mathbf{u}}(A)|^2 \\ &\leq \frac{|U| + 1}{|A|^2} \max_{\mathbf{u} \in \mathbb{F}^n} |\psi_{\mathbf{u}}(A)|^2 \leq |U| + 1. \end{aligned}$$

On the other hand,

$$\begin{aligned} &\frac{1}{|A|^2} \sum_{\mathbf{u} \in \mathbb{F}^n} \psi_{\mathbf{u}}(A + A) \\ &= \frac{1}{|A|^2} \sum_{j=0}^n \sum_{w(\mathbf{u})=j} \psi_{\mathbf{u}}(A + A) = \sum_{j=0}^n \mathcal{B}_j^\perp(A), \end{aligned}$$

where the second equality follows from (16.7.2). But, since  $\mathcal{B}_j^\perp(A)$  is the MacWilliams transform of the distance distribution of  $A$ , we have  $\sum_{j=0}^n \mathcal{B}_j^\perp(A) = 2^n / |A| = |V|$ .  $\square$

**Theorem 16.7.5**  $|\mathcal{W}(U)| \geq r$ , where  $r$  is the smallest integer such that

$$\sum_{i=0}^r \binom{n}{i} \geq |V|.$$

**Proof.** Let  $R(A)$  be the covering radius of  $A$ . Recall that  $|D^\perp(A)|$  is the number of nonzero distances in the formal dual of  $A$ . Therefore

$$|\mathcal{W}(U)| \geq |D^\perp(A)| \geq R(A),$$

where the first inequality follows from Theorem 16.7.1 and the second from the Delsarte theorem (see Theorem 8.3.7). By the sphere-covering bound we have

$$|A| \sum_{i=0}^{R(A)} \binom{n}{i} \geq 2^n.$$

This, together with  $|A| = 2^n / |V|$ , implies that  $|V| \leq \sum_{i=0}^{R(A)} \binom{n}{i}$ .  $\square$

**Example 16.7.6** Let  $V \subset \mathbb{F}^{29}$  be the union of  $B_3^{29}(\mathbf{0})$  and some 6 arbitrarily chosen vectors of weight  $\geq 4$ . We show that  $V$  cannot be a tile. Note that  $|V| = 2^{12}$  and  $r = 4$ . Let  $\mathbf{u} \in \mathbb{F}^{29}$  and let  $x$  denote the weight of  $\mathbf{u}$ . For the set  $V$  at hand, we have  $|\psi_{\mathbf{u}}(V) - L_3(x)| \leq 6$ , where  $L_3(x) = \psi_{\mathbf{u}}(B_3^{29}(\mathbf{0})) = P_0(x) + P_1(x) + P_2(x) + P_3(x)$  is the Lloyd polynomial. Thus,  $\psi_{\mathbf{u}}(V)$  may vanish only if

$$|L_3(x)| = \left| 4090 - \frac{2618}{3}x + 60x^2 - \frac{4}{3}x^3 \right| \leq 6.$$

Direct calculation shows that only  $x = 15$  satisfies this inequality, and hence  $|\mathcal{W}(U)| \leq 1$ . It can be verified that actually  $|\mathcal{W}(U)| = 1$ . However, Theorem 16.7.5 requires  $|\mathcal{W}(U)| \geq r = 4$ , a contradiction.  $\square$

## 16.8 Notes

We follow the lines of Cohen, Litsyn, Vardy and Zémor [162].

In general, tilings of  $\mathbb{F}^n$  with arbitrary bodies correspond to perfect codes correcting an arbitrary set of errors. Conditions for the existence of codes correcting an arbitrary set of errors and estimates of their cardinality were investigated in Deza [197], Deza and Hoffman [198], Deza, Karpovsky and Milman [199], Karpovsky and Milman [364], [365]. Such codes are useful, for instance, for correcting errors at the output of logic networks — the set of errors depends on the structure of the network and a single error in an element of the network may lead to an error of greater multiplicity at the network output — see Deza, Karpovsky and Milman [199]. Another example where the problem of correcting a given set of errors arises is the case of “artificial noise” which occurs if the process of data transmission is considered as a game situation, see Deza [197]. Tilings of  $\mathbb{F}^n$  have also been found useful in Vardy and Be’ery [661] for the design of efficient soft-decision decoders for BCH codes.

In the nonbinary case, tilings by generalized “crosses” and “semicrosses” are considered by Saidi in [567].

**§16.2** Using the results of Zémor [701] it is, in principle, possible to characterize all the sets  $V$  which satisfy the condition of Theorem 16.2.1. Here we give an example of a construction that produces such a set. Fix a subspace  $S \subset \mathbb{F}^n$  and a nonzero element  $\mathbf{s} \in S$ . Partition  $S$  into cosets modulo the two-element subspace  $\{\mathbf{0}, \mathbf{s}\}$ , and construct  $V$  by choosing one and only one element from each coset. By assumption, we have  $\mathbf{0} \in V$  and therefore  $\mathbf{s} \notin V$ . But then, by construction,  $\mathbf{s}$  is not in  $V + V$  and hence  $|2V| < |S| = 2|V|$ .

We are particularly interested in those tiles  $V$  which satisfy  $\langle V \rangle = \mathbb{F}^n$  (see Section 16.5). It can be shown that for these tiles  $|2V| \geq \frac{7}{4}|V|$ . More bounds on the cardinality of  $V + V$  for a given set  $V$  may be found in Zémor [701].

**§16.4** The existence of nonperiodic tilings of  $\mathbb{R}^2$  is a well-known problem in tessellation theory (see Penrose [533], and references therein). The “kites and darts” tiling of Penrose is a notable example of a nonperiodic tiling of the plane with two distinct polygons. It is still unknown, however, whether there exists a single (nonconvex) body which tiles the plane only nonperiodically.

It can be shown that the tiling of Theorem 16.4.1 is unique. Namely, in any nonperiodic tiling of  $\mathbb{F}^6$ , both tiles must be of the form (16.4.2) and (16.4.3), up to coordinate transformations [162].

**§16.6** The correspondence between sets  $V, A$  such that  $V + A = \mathbb{F}^n$  and coverings by spheres of radius one has been initially noticed by Blokhuis and Lam in [90] (cf. matrix construction, Section 3.5).

Perfect codes of full rank were constructed by Etzion and Vardy in [224] and Heden [290] (see Sections 11.3 and 11.7).

Relations between tilings and perfect codes can be employed to establish the existence of tilings of full rank. Indeed, a perfect code of full rank (that is, a perfect code of length  $\nu$  and rank  $\nu$ ), together with the Hamming sphere  $B_1(0^\nu)$ , constitutes an example of a tiling of full rank in  $\mathbb{F}^\nu$ . Furthermore, we have shown that tilings of full rank exist if and only if there exist perfect codes of full rank, for if  $(V, A)$  is a tiling of full rank in  $\mathbb{F}^n$ , then the associated perfect code must have full rank by Theorem 16.6.3.

The following was proved by Etzion and Vardy (see Theorem 11.3.22): for all  $m \geq 4$ , there exists a perfect code of full rank with length  $2^m - 1$ .

Thus, tilings of full rank exist in  $\mathbb{F}^n$  for all  $n = 2^m - 1$  with  $m \geq 4$ . They also exist for  $n = 2^m - 2$  with  $m \geq 4$  (see [162]) and do not exist for  $n \leq 7$  (Corollary 16.6.4). It was proved by Cohen, Litsyn, Vardy and Zémor [162] that tilings of full rank exist in  $\mathbb{F}^n$  for all  $n \geq 112$ , then for  $n \geq 14$  by Etzion and Vardy [225] and for  $n \geq 10$  by Levan and Phelps [415]. The case of lengths 8 and 9 remains open.

This Page Intentionally Left Blank

# Chapter 17

## Writing on constrained memories

We start this chapter with a seemingly strange question: what are the worst coverings? More precisely, what is the worst way of shortening a linear code, as far as covering radius is concerned?

In Section 17.1, we apply the results of this study to efficient overwriting on write-once memories (WOMs), describe the so-called coset-encoding method and give examples using the Golay and Hamming codes. In Sections 17.2 and 17.3, we define a general error model for these memories and design, in Section 17.4, single-error-correcting WOM-codes based on 2- and 3-error-correcting BCH codes. A nonlinear extension is presented in Section 17.5.

### 17.1 Worst case coverings and WOMs

We consider the following question: how may a “write-once memory” (WOM) be reused? That is, we have a storage medium, called WOM or  $n$ -WOM, consisting of  $n$  memory positions, or wits, each initially at “0”. At any step, a wit can be irreversibly overwritten with a “1” (e.g., by a laser beam in some digital optical disks). We describe a method, called *coset encoding*, enabling many rewritings on a WOM.

#### The coset-encoding writing rule:

An  $[n, k, d]R$  code  $C$  is used to encode  $n - k$  bits on a WOM as follows: every message  $s \in \mathbb{F}^{n-k}$  is one-to-one associated to a coset of  $C$  in  $\mathbb{F}^n$ , say  $\mathbf{x} + C$ , having as its syndrome  $s$ . That is,  $s = \mathbf{Hx}^T = s(\mathbf{x})$ , where  $\mathbf{H}$  is a generator matrix for  $C^\perp$ , the  $[n, n - k, d^\perp]$  dual code of  $C$ . Encoding, or “writing”, involves finding a minimum weight vector  $\mathbf{y}$  with syndrome  $s$ , and

writing it on the WOM. This requires a complete decoding algorithm in the sense of error-correcting codes. Decoding, or “reading”, is simply a syndrome computation calculating  $s$  from  $\mathbf{y}$ .

We present here an algebraic treatment, giving precise estimates of the “worst-case” behaviour of these WOM-codes.

For  $I \subset \{1, 2, \dots, n\}$ , we write  $C(\bar{I})$  for the *shortening* of  $C$  on  $I$ . That is,

$$C(\bar{I}) = \{\mathbf{c} = (c_1, \dots, c_n) \in C : c_i = 0 \text{ for all } i \in I\}.$$

Upon dropping these coordinates, we get a code of length  $n - |I|$ , dimension and minimum distance at least  $k - |I|$  and  $d$ , respectively, which we also call  $C(\bar{I})$ . If  $\mathbf{H}(C) = (\mathbf{h}_1, \mathbf{h}_2, \dots, \mathbf{h}_n)$  is a parity check matrix for  $C$  where  $\mathbf{h}_i$  are column vectors of size  $n - k$ , then the set of columns

$$\{\mathbf{h}_j : j \in \{1, 2, \dots, n\} \setminus I\}$$

constitutes a parity check matrix for  $C(\bar{I})$ . Recall that a linear  $[n, k, d]$  code  $C$  is *maximal* if it is not contained in a larger code with the same minimum distance. Clearly, if  $k = a[n, d]$ , then  $C$  is maximal.

We are now ready for a few lemmas.

**Lemma 17.1.1** *Writing  $r$  bits using a linear code  $C$  and the coset-encoding scheme is possible if and only if  $C^\perp$  has dimension at least  $r$ .*  $\square$

**Lemma 17.1.2 (Supercode lemma)** *If  $C_1$  is properly included in  $C_2$ , then  $R(C_1) \geq d(C_2)$ .*

**Proof.** Pick any  $\mathbf{x} \in C_2 \setminus C_1$ . Then  $d(\mathbf{x}, C_1) \geq d(C_2)$ . See also Lemma 8.2.1.  $\square$

**Lemma 17.1.3** *If  $C$  is maximal, then  $R(C) \leq d(C) - 1$ .*

**Proof.** If  $R(C) \geq d(C)$ , take a vector  $\mathbf{x}$  such that  $d(\mathbf{x}, C) \geq d(C)$ . Then  $C \cup \{\mathbf{x}\}$  generates a linear code with minimum distance  $d(C)$ , a contradiction. This result is also a consequence of Theorem 17.2.2.  $\square$

Actually, the property  $R(C) \leq d(C) - 1$  can be used for defining a maximal code, as we did in Section 2.1.

**Lemma 17.1.4** *The largest number of bits to be written to coset-encode  $n - k$  bits with an  $[n, k]_R$  code  $C$  is  $R$ .*  $\square$

**Lemma 17.1.5** *If an  $[n, k]$  code  $C$  is shortened on a set  $I$  of positions not containing the support of any nonzero codeword in its dual, then  $C(\bar{I})$  has dimension exactly  $k - |I|$ , thus enabling the writing of  $n - k$  bits.*

**Proof.** For the dimension of  $C(\bar{I})$ , notice that its dual must still have dimension  $n - k$ , since no nontrivial linear combination of rows of the matrix  $[\mathbf{h}_j : j \in \{1, 2, \dots, n\} \setminus I]$  can be  $\mathbf{0}$ . For the writing capacity, use Lemma 17.1.1.  $\square$

**Lemma 17.1.6** *Let  $C$  be an  $[n, k, d]R$  code. Then, any  $[n - i, k - i, d]$  shortened maximal code  $C'$  satisfies  $R(C') = d - 1$ .*

**Proof.** By Lemma 17.1.3,  $R(C') \leq d - 1$ . We prove the opposite inequality for  $i = 1$ ; let us assume without loss of generality that the shortened coordinate is the first one, i.e.,

$$C' = \{\mathbf{c}' \in \mathbb{F}^{n-1} : (0|\mathbf{c}') \in C\}.$$

Let  $C_1 = \{0\} \oplus C'$ ;  $C_1$  is an  $[n, k - 1, d]$  proper subcode of  $C$ . Let  $\mathbf{x} = (1|\mathbf{y})$  be a codeword of  $C$ . Then  $d(\mathbf{x}, C_1) \geq d$ , hence  $d(\mathbf{y}, C') \geq d - 1$ . The general case follows by successive shortenings.  $\square$

### The rewriting rule:

Let us define a rule for rewriting  $n - k$  bits on the WOM. After the first writing,  $\mathbf{y}_1$  is stored in the WOM and represents  $\mathbf{s}_1$ , where

$$\mathbf{s}_1 = \sum_{i \in \text{supp}(\mathbf{y}_1)} \mathbf{h}_i.$$

Let  $I_1 = \text{supp}(\mathbf{y}_1)$ . Encoding  $\mathbf{s}_2$  at the second generation amounts to writing an  $\mathbf{y}_2$  representing  $\mathbf{s}_2 + \mathbf{s}_1$ , not using wits already written, that is,

$$\mathbf{s}_2 + \mathbf{s}_1 = \sum_{i \in \text{supp}(\mathbf{y}_2)} \mathbf{h}_i,$$

with  $\text{supp}(\mathbf{y}_2) \cap I_1 = \emptyset$ . This is clearly equivalent to encoding  $\mathbf{s}_2 + \mathbf{s}_1$  with the shortened code  $C(\bar{I}_1)$ , yielding  $\mathbf{y}_2$  in  $\mathbb{F}^n$ . Again,  $\mathbf{y}_2$  is chosen of minimum weight, and the state of the WOM,  $\mathbf{y}_1 + \mathbf{y}_2$ , represents  $\mathbf{H}(\mathbf{y}_1 + \mathbf{y}_2)^T = \mathbf{s}_2$ .

Let us illustrate the process with two examples, the first one having already been discussed in Section 1.2.

Denote by  $\{n, m, g\}$  a WOM-code allowing  $g$  successive writings of  $m$  bits on an  $n$ -WOM. We define the *efficiency*  $\phi$  of a WOM-code as the number of bits written per wit in the worst possible case, i.e.,  $\phi = mg/n$ .

**Example 17.1.7** Only 3 wits are needed to write 2 bits twice. That is, there exists a  $\{3, 2, 2\}$  WOM-code. Here  $\phi = 4/3$ .

This was proved in Section 1.2 (Example 1.2.6). Let us sketch the ideas once again with the new notations. Take for  $C$  the  $[3, 1, 3]1$  repetition code. By Lemma 17.1.4, the first writing of 2 bits with  $C$  uses at most 1 wit, i.e.,  $w(\mathbf{y}_1) \leq 1$ . Thus  $I_1 = \text{supp}(\mathbf{y}_1)$  contains no support of a nonzero codeword in the  $[3, 2, 2]$  dual code of  $C$ , and, by Lemma 17.1.5,  $C(\bar{I}_1)$  allows a second writing of 2 bits. Therefore, taking  $\mathbf{H} = \begin{pmatrix} 1 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix}$ , and, for instance,  $\mathbf{s}_1 = (1 \ 1)^T$ ,  $\mathbf{s}_1$  is encoded by  $\mathbf{y}_1 = (1 \ 0 \ 0) : \mathbf{H}\mathbf{y}_1^T = \mathbf{s}_1$ . Now,  $\mathbf{H}(C(\bar{I}_1)) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ , denoted by  $\mathbf{H}'$ , is used for the second writing. To encode, for example,  $\mathbf{s}_2 = (1 \ 0)^T$ , one encodes  $\mathbf{s}_1 + \mathbf{s}_2 = (0 \ 1)^T$  with  $\mathbf{H}'$ , getting  $\mathbf{y}'_2 = (1 \ 0)$  and  $\mathbf{y}_2 = (0 \ 1 \ 0)$ . Finally,  $\mathbf{y}_1 + \mathbf{y}_2 = (1 \ 1 \ 0)$  is the state of the WOM, representing  $\mathbf{H}(\mathbf{y}_1 + \mathbf{y}_2)^T = \mathbf{s}_2$ .  $\square$

**Example 17.1.8** (The Golay  $\{23, 11, 3\}$  WOM-code.)

We recall a few facts about the  $[23, 12, 7]3$  Golay code  $C$  (cf. Section 11.1). The set of the weights of its codewords is  $W = \{0, 7, 8, 11, 12, 15, 16, 23\}$ . It contains its  $[23, 11, 8]$  dual code and possesses a four-fold transitive automorphism group  $M_{23}$ . Thus, arbitrarily assigning binary values to at most 4 positions among the 23, there exists in  $C$  a codeword of any weight in  $W \setminus \{0, 23\}$ , taking the chosen values on these positions. This property will be referred to as “transitivity”. Now let us write on the WOM.

The first generation uses at most 3 wits (by Lemma 17.1.4). By writing additional wits just before the second writing we can always assume that exactly 3 wits have been written; we can further assume, by transitivity, that they lie in the first 3 positions. Thus we are left with a  $[20, 9, 7]$  shortened Golay code which is maximal. Hence, by Lemmas 17.1.6, 17.1.4 and 17.1.1, we get

**Theorem 17.1.9** Any three times shortened Golay code allows writing 11 bits, using at most 6 wits.  $\square$

Hence, for the first 2 generations, we need at most 9 wits. We now prove that the first 2 writings do not contain the support of any nonzero codeword of  $C^\perp$ , and thus a third writing is possible, by Lemma 17.1.5. This is guaranteed for  $|I| \leq d^\perp - 1 = 7$ , hence only cases when  $|I| = 8$  or 9 must be considered.

Case  $|I| = 9$ . For this case to occur, the only possibility is to write 3 wits ( $\mathbf{y}_1$ ) at the first generation and 6 wits ( $\mathbf{y}_2$ ) at the second. By transitivity, one can assume that  $I = I_1 \cup I_2$ , with  $I_1 = \{1, 2, 3\} = \text{supp}(\mathbf{y}_1)$  and  $4 \in I_2 = \text{supp}(\mathbf{y}_2)$ . Now suppose that there exists  $\mathbf{c}^\perp \in C^\perp \setminus \{0\}$  such that  $\text{supp}(\mathbf{c}^\perp) \subseteq I$ . The only possible weights in  $C^\perp$  are 0, 8, 12, 16, so  $\mathbf{c}^\perp$  has weight 8 and  $I = \text{supp}(\mathbf{c}^\perp) \cup \{j\}$  for some position  $j$ . From  $C^\perp \subset C$  follows that  $\mathbf{c}^\perp \in C$ . Defining  $\mathbf{e}_j$  by  $\text{supp}(\mathbf{e}_j) = \{j\}$ , it follows that, with  $\mathbf{y} = \mathbf{y}_1 + \mathbf{y}_2$ ,  $\mathbf{s}(\mathbf{y}) = \mathbf{s}(\mathbf{c}^\perp + \mathbf{e}_j) = \mathbf{s}(\mathbf{e}_j)$ . Now, we should distinguish between two possibilities for  $j$ :

- 1) If  $j \in I_1$ , one can assume  $j = 1$  and then find  $\mathbf{c} \in C$ ,  $w(\mathbf{c}) = 7$ ,  $\mathbf{c} = 011\dots$
- 2) Similarly, if  $j \in I_2$ , assume  $j = 4$  and find  $\mathbf{c} \in C$ ,  $w(\mathbf{c}) = 7$ ,  $\mathbf{c} = 1110\dots$

The previous expressions of  $\mathbf{c}$  are valid by transitivity. Now the vector  $\mathbf{x} = \mathbf{c} + \mathbf{e}_j$  has the same syndrome as  $\mathbf{y}$ , is writable after the first generation — because it starts with 3 ones — and  $w(\mathbf{x}) = w(\mathbf{y}) - 1$ , contradicting the minimum weight writing hypothesis.

Case  $|I| = 8$ . It is simpler and can be dealt with along the same lines; we skip it. This completes the proof of the following.

**Theorem 17.1.10** *Coset-encoding with the Golay code, 3 writings of 11 bits are possible on a 23-WOM.*  $\square$

The efficiency of this WOM-code is  $\phi = 33/23 \approx 1.435$ .  $\square$

The previous analysis can be straightforwardly extended to other codes, yielding

**Theorem 17.1.11** *Let  $C$  be an  $[n, k, d]_R$  maximal code. If for some  $i$ ,  $i \leq d^\perp - 1$ , its shortened versions of lengths at least  $n - i$  remain maximal and of minimum distance  $d$ , then at least  $g$  writings of  $n - k$  bits are guaranteed, with  $g = 2 + \lfloor (i - R)/(d - 1) \rfloor$ .*  $\square$

**Corollary 17.1.12** *A Hamming code of length  $2^r - 1$  yields a  $\{2^r - 1, r, 2^{r-2} + 1\}$  WOM-code.*

**Proof.** Use the known fact that Hamming codes of length  $2^r - 1$  remain maximal when shortened at most  $2^{r-1} - 1$  times.  $\square$

The efficiency of this WOM-code is asymptotically  $0.25r$ . In fact,  $g$  can be increased to

$$g = 2^{r-2} + 2^{r-4} + 1 \quad (17.1.13)$$

(for  $r \geq 4$ ), by use of geometric arguments (see Notes), and the efficiency is then asymptotically improved to  $5r/16 = 0.3125r$ .

## 17.2 The error case

We adapt the previous methods in order to answer the following question: how can error-correcting WOM-codes be constructed?

Let us describe the general principles underlying the encoding schemes we use (the following is a reformulation of the “coset-encoding” technique of the previous section in a more general setting):

Let  $\Pi$  denote the set of wits of the WOM, identified with  $\{1, 2, \dots, n\}$ . The set of messages we wish to write is identified with a subset  $M$  of a finite abelian group  $G$  (in practice  $G = \mathbb{F}^m$ ). We also index the wits of  $\Pi$  by a subset  $P$  of  $G$  with a one-to-one mapping  $\sigma$  of  $\Pi$  onto  $P$ .

Let  $\epsilon$  be the function  $\Pi \rightarrow \{0, 1\}$  describing the state of the WOM, i.e.,  $\epsilon(\pi) = 0$  when  $\pi$  is unused, and  $\epsilon(\pi) = 1$  when  $\pi$  is used,  $\pi$  ranging over  $\Pi$ ; the function  $\epsilon$  is identified with its image  $\epsilon(\Pi) \in \mathbb{F}^n$ .

**Reading a message:** The last message  $c \in M$  written on the WOM is read by computing  $c(\epsilon) = \sum_{\pi: \epsilon(\pi)=1} \sigma(\pi)$ .

**Writing a message:** Given a state  $\epsilon$  of the WOM, writing a message  $c \in M$  is done by finding a set  $W \subset \Pi$  of unused wits such that

$$\sum_{\pi \in W} \sigma(\pi) + \sum_{\pi: \epsilon(\pi)=1} \sigma(\pi) = c. \quad (17.2.1)$$

Let  $C$  be a given  $[i, k, d]$  code. We denote by  $a[i, d, C]$  the maximal dimension of a linear code of length  $i$  and minimum distance  $d$  containing  $C$ . We set  $a[i, d] = a[i, d, \{\mathbf{0}\}]$  (for  $i < d$ , one has  $a[i, d] = 0$ ). Recall that an  $[i, k, d]$  code  $C$  for which  $k = a[i, d, C]$  is called maximal, see Section 17.1. Clearly,

$$k \leq a[i, d, C] \leq a[i, d].$$

**Theorem 17.2.2** *Any  $[n, k, d]_R$  code  $C$  satisfies*

$$a[R, d] + k \leq a[n, d, C]. \quad (17.2.3)$$

**Proof.** Let  $C$  be an  $[n, k, d]_R$  code, and  $\mathbf{z}$  a deep hole with respect to  $\mathbf{0}^n$ , i.e., such that  $d(\mathbf{z}, C) = w(\mathbf{z}) = R$ , with support, say,  $[1, R]$ . Define  $B$ , an  $[R, a[R, d], d]$  code, and consider a nonzero  $\mathbf{c}' = \mathbf{b}0^{n-R} \in C' := B \oplus \mathbf{0}^{n-R}$ . Since  $\text{supp}(\mathbf{c}') \subseteq \text{supp}(\mathbf{z})$ , then  $d(\mathbf{c}', C) = w(\mathbf{c}')$  clearly holds. But  $w(\mathbf{c}') = w(\mathbf{b}) \geq d$ , thus  $C + C'$  is an  $[n, k + a[R, d], d]$  code containing  $C$ .  $\square$

This theorem is used in Section 17.4 for providing upper bounds on  $R$  for shortened codes.

### 17.3 A model for correcting single errors

Suppose the group we use to construct our WOM-code is  $G = \mathbb{F}^m$ ; to every state  $\epsilon$  of the WOM, we associate the set  $S(\epsilon) \subseteq P$  corresponding to the unused wits, i.e.,  $S(\epsilon) = \{\sigma(\pi) : \epsilon(\pi) = 0\}$ . So, in the initial state  $S(0) = P$ . We write simply  $S$  when no confusion can arise.

Let  $\mathbf{H}(S)$  be any  $m \times |S|$  matrix the columns of which are the elements of  $S$  ( $\mathbf{H}(S)$  is defined modulo permutations of its columns). Then  $\mathbf{H}(S)$  is the parity check matrix of a code that we denote by  $C(S)$  (cf. Section 16.1).

We wish to correct Hamming type errors; more precisely, we say that a (single) error has occurred when the state  $\epsilon(\pi)$  of a single position  $\pi$  is either written or read incorrectly. This means that the state of the WOM which is actually read, differs from the desired state by an  $n$ -tuple of weight 1.

Let  $E \subseteq \mathbb{F}^n$  be the set of all the authorized states of the WOM (with no errors) that may occur during the history of the memory. Clearly, if we are to distinguish between two states  $\epsilon_1 \in E$  and  $\epsilon_2 \in E$ , given that a single error may occur, then we must have, as in classical coding problems,

$$d(\epsilon_1, \epsilon_2) \geq 3.$$

In other words,  $E$  must be a (not necessarily linear) code of length  $n$  and minimum distance at least 3.

We will display error-correcting WOM-codes that make full use of the capacity of the WOM, in the sense that the set  $E$  will be a Hamming code (for a WOM-length  $n = 2^r - 1$ ).

Let us now describe the scheme. When the desired message is  $c \in M$  and an error has occurred on position  $\pi$ , then the word actually read is  $c + \sigma(\pi)$ . So the sets  $M$  and  $P$  should be such that any two ordered pairs  $(c, p) \in M \times P$  and  $(c', p') \in M \times P$  satisfy the condition

$$c + p \neq c' + p'.$$

To achieve this when the size of the WOM is  $n = 2^r - 1$ , we choose a group  $G = G_1 \times G_2$ , where  $G_1 = \mathbb{F}^r$ .

The set  $P \subseteq G$  should verify:

(P) the projection on the first coordinate,  $pr_1 : P \rightarrow G_1$  is a one-to-one mapping between  $P$  and  $G_1 \setminus \{0\}$ .

The set  $M \subseteq G$  of messages should verify:

(M)  $M \subseteq \{0\} \times G_2$ .

When a single error occurs, the message read on the WOM is  $c + p$  instead of  $c$ ; property (M) ensures that  $pr_1(c + p) = pr_1(p)$ , and property (P) ensures that  $pr_1(p)$  uniquely determines  $p$ , and hence  $c$ .

Note that conditions (M) and (P) imply that the authorized states of the WOM are all the words of the Hamming code of length  $n$  (cf. Example 17.4.9).

Next, we want to maximize the number of times the WOM can be reused. To do this, we must find sets  $P$  and  $M$  satisfying (P) and (M) such that any reasonably “large” subset  $S$  of  $P$  generates  $M$ , and furthermore such that only “few” elements of  $S$  are required to generate an arbitrary message  $c \in M$ .

This is the object of the next section.

## 17.4 Single-error-correcting WOM-codes

Consider, for  $r \geq 4$ ,  $C = \mathcal{BCH}(2, r)$  the 2-error-correcting  $[n = 2^r - 1, n - 2r, 5]$  BCH code (see Section 10.1). If  $\alpha$  is a primitive element in  $\mathbb{F}_{2^r}$ , then a parity check matrix of  $C$  is given by

$$\mathbf{H} = \begin{pmatrix} 1 & \alpha & \alpha^2 & \dots & \alpha^{n-1} \\ 1 & \alpha^3 & \alpha^6 & \dots & \alpha^{3(n-1)} \end{pmatrix} = [\mathbf{h}_1, \mathbf{h}_2, \dots, \mathbf{h}_n],$$

where every element in  $\mathbf{H}$  must be thought of as an  $r$ -tuple (column) of elements in  $\mathbb{F}$ .

Now take  $G_1 = G_2 = \mathbb{F}^r$ ,  $P = \{\mathbf{h}_i : 1 \leq i \leq n\}$ ,  $M = \{0\} \times \mathbb{F}^r$ . Then conditions (P) and (M) are fulfilled.

We use the following properties of  $C$ :

$$R(C) = 3. \tag{17.4.1}$$

$$d(C^\perp) \geq 2^{r-1} - 2^{r/2}. \tag{17.4.2}$$

Combining (17.4.2) and Lemma 17.1.5, we see that any  $S \subseteq P$  with  $|S| \geq 2^{r-1} + 2^{r/2}$  generates  $G$ .

Now we use Theorem 17.2.2 to upperbound the covering radius of  $C(S)$ .

**Theorem 17.4.3** (i) If  $|S| \geq (n+1)/2 + (n+1)^{1/2}$ , then  $R(C(S)) \leq 9$ .

(ii) If, moreover,  $|S| > (\sqrt{2}/2)(n+1)$ , then  $R(C(S)) \leq 7$ .

**Proof.** Let  $s = |S|$ . If  $D$  is any linear code with length  $s$  and minimum distance at least 5, the sphere-packing bound reads:  $|D|(1+s+s(s-1)/2) \leq 2^s$ . This implies

$$|D|s^2/2 \leq 2^s,$$

hence

$$a[s, 5] \leq s - 2 \log s + 1. \tag{17.4.4}$$

Suppose  $S$  satisfies  $|S| \geq (n+1)/2 + (n+1)^{1/2}$ ; then  $C(S)$  is an  $[s, s-2r, \geq 5]$  code (its parity check matrix  $\mathbf{H}(S)$  has full rank).

Set  $R = R(C(S))$ . Applying Theorem 17.2.2 to  $C(S)$  and using (17.4.4), we obtain:

$$a[R, 5] \leq 2r - 2 \log s + 1. \quad (17.4.5)$$

We have  $s > 2^{r-1}$ , so:

$$a[R, 5] < 3. \quad (17.4.6)$$

But  $a[10, 5] = 3$  (see Table 2.3), so (17.4.6) implies  $R \leq 9$ ; this proves (i). If, besides,  $S$  verifies  $s > (\sqrt{2}/2)(n+1)$ , then  $\log s > -1/2 + r$ , and (17.4.5) yields  $a[R, 5] < 2$ . Since  $a[8, 5] = 2$  (see Table 2.3), this implies  $R \leq 7$ . This proves (ii).  $\square$

Theorem 17.4.3 means that the above scheme yields single-error-correcting WOM-codes, with parameters  $\{2^r - 1, r, g\}$ , where, applying Lemmas 17.1.4 and 17.1.5 and straightforward averaging:

$$g = \left( \frac{1 - \sqrt{2}/2}{7} + \frac{\sqrt{2}/2 - 0.5}{9} \right) n + o(n) \approx n/15.42 + o(n).$$

An estimate of their efficiency is:  $\phi \approx r/15.42$ .

We now use 3-error-correcting BCH codes; for  $r \geq 4$ , let  $C = \mathcal{BCH}(3, r)$  be a 3-error-correcting  $[n = 2^r - 1, n - 3r, 7]$  BCH code. For the sake of brevity, we only sketch this case, very similar to the previous one; the parity check matrix of  $C$  is now

$$\mathbf{H} = \begin{pmatrix} 1 & \alpha & \alpha^2 & \dots & \alpha^{n-1} \\ 1 & \alpha^3 & \alpha^6 & \dots & \alpha^{3(n-1)} \\ 1 & \alpha^5 & \alpha^{10} & \dots & \alpha^{5(n-1)} \end{pmatrix} = [\mathbf{h}_1, \mathbf{h}_2, \dots, \mathbf{h}_n].$$

We set  $G_1 = \mathbb{F}^r$ ,  $G_2 = \mathbb{F}^r \times \mathbb{F}^r$ ,  $P = \{\mathbf{h}_i : 1 \leq i \leq n\}$ ,  $M = \{0\} \times G_2$ , thus again fulfilling conditions (P) and (M).

**Theorem 17.4.7** (i) If  $|S| \geq (n+1)/2 + 2(n+1)^{1/2}$ , then  $R(C(S)) \leq 16$ .

(ii) If, moreover,  $|S| > 1.145(n+1)/2$ , then  $R(C(S)) \leq 14$ .

(iii) If, moreover,  $|S| > 1.443(n+1)/2$ , then  $R(C(S)) \leq 13$ .

(iv) If, moreover,  $|S| > 1.818(n+1)/2$ , then  $R(C(S)) \leq 12$ .

**Proof.** Proceed as in Theorem 17.4.3. Note that now, if  $|S| \geq (n+1)/2 + 2(n+1)^{1/2}$ , then  $C(S)$  is an  $[s, s - 3r, \geq 7]$  code, so that instead of (17.4.5) we obtain:

$$a[R, 7] \leq 3r - 3 \log s + \log 6. \quad (17.4.8)$$

Since  $s > 2^{r-1}$ ,  $a[R, 7] < 6$  and (i) follows from  $a[17, 7] = 6$  (see Table 2.3). If  $s > (\sqrt[3]{3/16})(n+1) \approx 1.145(n+1)/2$ , then  $a[R, 7] < 5$  and (ii) follows

from  $a[15, 7] = 5$  (see Table 2.3). If  $s > (\sqrt[3]{3/8})(n+1) \approx 1.443(n+1)/2$ , then  $a[R, 7] < 4$  and (iii) follows from  $a[14, 7] = 4$  (see Table 2.3). If  $s > (\sqrt[3]{3/4})(n+1) \approx 1.818(n+1)/2$ , then  $a[R, 7] < 3$  and (iv) follows from  $a[13, 7] = 3$  (see Table 2.3).  $\square$

We get  $\{2^r - 1, 2r, g\}$  WOM-codes with  $g = n/26.9 + o(n)$  and an estimated efficiency:  $\phi \approx r/13.45$ .

The following example is too small for the previous methods to display real efficiency, but is intended to be illustrative.

**Example 17.4.9** Set  $C = \mathcal{BCH}(2, 4)$ . We are thus dealing with 4-bit messages, which we write on a 15-WOM using the lower part  $\mathbf{H}_2$  of the parity check matrix

$$\mathbf{H} = \begin{pmatrix} \mathbf{H}_1 \\ \mathbf{H}_2 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 \\ \hline - & - & - & - & - & - & - & - & - & - & - & - & - & - & - \\ 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}.$$

Let  $\Pi = \{1, 2, \dots, 15\}$ . We know by (17.4.1) that  $R(C) = 3$ , hence writing any  $\sigma$  requires at most 3 wits. Suppose  $\mathbf{c} = (0110)^T$  is to be written; then  $\mathbf{c}$  is associated to

$$\sigma = (0000\ 0110)^T,$$

and we have

$$\sigma = \mathbf{h}_1 + \mathbf{h}_2 + \mathbf{h}_5,$$

so that  $\mathbf{c}$  is represented by writing on positions 1, 2 and 5. The state of the memory is now

$$\epsilon = (110010000000000).$$

Note that  $\mathbf{H}_1 \epsilon^T = \mathbf{0}$  so that  $\epsilon$  is a codeword of the Hamming code. At that stage, we are left with a set  $S$  with size 12 yielding a  $[12, 4, 5]$  code by (17.4.2). Thus any new message can be written on the memory using at most 7 wits, by Theorem 17.4.3-(ii).

Now suppose we wish to read the last message written on the WOM; say the state of the memory is

$$\epsilon = (011011110000100).$$

We evaluate

$$\sigma = \begin{pmatrix} \sigma' \\ \sigma'' \end{pmatrix} = \mathbf{h}_2 + \mathbf{h}_3 + \mathbf{h}_5 + \mathbf{h}_6 + \mathbf{h}_7 + \mathbf{h}_8 + \mathbf{h}_{13} = (11010100)^T.$$

Vector  $\sigma'$  being nonzero means that an error has been made. Moreover, we see that  $(1101)^T$  is the first part of  $\mathbf{h}_8$ , so that the error is on position 8. Evaluating:  $\sigma + \mathbf{h}_8 = (00000111)^T$ , we read the message as  $(0111)^T$ .  $\square$

## 17.5 Nonlinear WOM-codes

We survey briefly nonlinear WOM-codes. Let us use the notation  $\omega(< v >^g)$  for the minimum length  $n$  of a WOM needed to update one of  $v$  possible values  $g$  times.

The conjecture

$$\omega(< v >^g) = (1 + o(1)) \max\{g, g \frac{\log v}{\log g}\} \quad (17.5.1)$$

is disproved with an easy counterexample. Observe that for every fixed positive  $\alpha < 0.5$ ,

$$\omega(< v >^{\alpha v}) \geq 2\alpha v.$$

Indeed, if  $n \leq v - 1$ , then every updating requires at least 2 wits in the worst case.

The group  $\mathbb{Z}_p$  can be used for coset encoding.

**Theorem 17.5.2** *Let  $p$  be a prime and  $S$  a nonempty subset of  $\mathbb{Z}_p$ . Then*

$$|S^{\neq t}| \geq \min\{p, t|S| - t^2 + 1\},$$

where  $S^{\neq t}$  denotes the set of sums of  $t$  distinct elements of  $S$  and  $S^{\neq 0} = \{0\}$  by convention.  $\square$

In particular

$$s_{\mathbb{Z}_p}(t) \leq (p + t^2 - 1)/t,$$

where, for an abelian group  $G$ , the function  $s_G(t)$  — studied in the next chapter — denotes the smallest integer  $s$  such that, for any generating set  $S$

of  $G$ ,  $\sum_{0 \leq i \leq t} S^{\neq i} = G$  for  $|S| \geq s$ . Hence the  $\mathbb{Z}_p$ -scheme allows  $g$  updatings with asymptotically:

$$\begin{aligned} g &\geq (1 + o(1))p \left( (1 - \frac{1}{2})\frac{1}{2} + (\frac{1}{2} - \frac{1}{3})\frac{1}{3} + \dots + (\frac{1}{i-1} - \frac{1}{i})\frac{1}{i} + \dots \right) \\ &= (1 + o(1))p(2 - \frac{\pi^2}{6}), \end{aligned}$$

i.e.,

$$g > (1 + o(1))0.35p. \quad (17.5.3)$$

Note that, for large enough  $p$  and  $t$ , Theorem 17.5.2 only guarantees:

$$s_{\mathbb{Z}_p}(t) \leq \frac{p}{t} \left( 1 + \frac{t^2 - 1}{p} \right) \approx \frac{|\mathbb{Z}_p|}{t}.$$

Whereas, for large  $t$  and  $r$ , by Theorem 18.2.6,

$$s_{\mathbb{F}^r}(t) \leq \frac{|\mathbb{F}^r|(t+1)}{2^t},$$

so linear WOM-codes should be asymptotically more efficient than  $\mathbb{Z}_p$ -codes. The main problem is that the set of columns of  $\mathbf{H}$  we are left with while updating is not guaranteed to generate  $\mathbb{F}^r$  when  $|S| \leq 2^{r-1}$ , so, starting from the parity check matrix of a Hamming code, we could have to settle to writing fewer bits after  $g = 2^{r-2} + 1$  generations. This has been improved to

$$g = 2^{r-2} + 2^{r-4} + 1, \quad (17.5.4)$$

by use of geometric considerations: remember (see Lemma 17.1.5) that  $\mathbf{H}(C)$ , the parity check matrix of a code  $C$ , remains of full rank if and only if the written wits do not contain the support of a nonzero codeword of  $C^\perp$  (here, codewords of  $C$  are just complements of hyperplanes in  $PG(r-2, 2)$ ). In fact, from the point of view of the writing efficiency, a decrease of the rank is good, since the covering radius then drops (the code dimension increases). Of course, to implement such a system, one would need a few extra wits used as flags to warn the reader and future writer of the surviving rank.

If we are ready to relax the assumption that the writing rate be kept constant, then the WOM can be overwritten more. Namely, in Lemma 17.1.5, we have seen that  $C(\bar{I})$  has dimension  $k - |I|$  when  $I$  does not contain a support of a nonzero codeword in  $C^\perp$ . This is guaranteed if

$$|I| \leq d^\perp - 1.$$

However, if  $|I| \geq d^\perp$  and  $|I|$  is not too large, one can hope that the support of only one nonzero codeword of  $C^\perp$  is contained in  $I$ , and thus  $r - 1$  bits can still be written. The idea is captured by the following definition and result.

**Definition 17.5.5** The  $i$ -th distance of  $C$ , denoted by  $d_i(C)$  or  $d_i$ , is the minimum size of the union of the supports of  $i$  linearly independent codewords.

**Theorem 17.5.6** Shortening an  $[n, k, d]$  code  $C$  on at most  $s = d_i^\perp - 1$  positions gives a code

$$C' [n - s, k' \leq k - s + i - 1, \geq d]$$

enabling to write at least  $n - k - (i - 1)$  bits by coset encoding.  $\square$

Let us not pursue further but conclude by noting that our knowledge of  $s_{\mathbb{F}^r}(t)$  for small  $t$ 's (see next chapter) already gives

$$\begin{aligned} g &\geq 2^r (1 + o(1)) \sum_{i=2}^{\infty} \frac{1}{i} (s_{\mathbb{F}^r}(i-1) - s_{\mathbb{F}^r}(i)) \\ &\geq \sum_{i=2}^6 \frac{1}{i} (s_{\mathbb{F}^r}(i-1) - s_{\mathbb{F}^r}(i)) \\ &= 2^r (1 + o(1)) \left( \frac{1}{2} \left(1 - \frac{1}{2}\right) + \frac{1}{3} \left(\frac{1}{2} - \frac{1}{3}\right) + \frac{1}{4} \left(\frac{1}{3} - \frac{1}{4}\right) + \frac{1}{5} \left(\frac{1}{4} - \frac{1}{8}\right) + \frac{1}{6} \left(\frac{1}{8} - \frac{1}{16}\right) \right). \end{aligned}$$

This leads to an improvement on (17.5.3):

$$g > 0.36 \cdot 2^r (1 + o(1)).$$

**The case  $g = 2$ .**

The following was first proved nonconstructively:

$$\omega(< v >^2) \approx 1.29 \log v. \quad (17.5.7)$$

Let us show how to achieve this value semi-constructively (cf. Section 20.3), using linear codes. One can obtain, through a greedy algorithm, an  $[n, \kappa n] R$  code  $C$ , with  $R = \kappa n$ , on the Gilbert-Varshamov bound with rate satisfying

$$\kappa = H^{-1}(1 - \kappa),$$

i.e.,  $\kappa \approx 0.227$ .

After coset-encoding  $n(1 - \kappa)$  bits with  $C$ , we can always assume that exactly  $n\kappa$  wits have been used. For the second writing, we consider these used wits as defects: we now want to write  $n(1 - \kappa)$  bits on a memory of size  $n$  with  $s = n\kappa$  defects (in fact  $s$  asymmetric defects). We know that this is possible (cf. Notes on Section 18.7). The efficiency of this WOM-code is

$$\phi = 2(1 - \kappa) \approx 1.546. \quad (17.5.8)$$

Table 17.1: Parameters of a few WOM-codes, linear or not.

$g$	$r$	$n$	$\phi$	$\phi(g, r)$	$\phi(g)$	Comments
2	2	3	1.33	1.33	1.54	Ex. 17.1.7
2	$0.77n$	$n$	1.55	1.55	1.55	(17.5.8)
3	11	23	1.43	1.65	1.94	Th. 17.1.10
4	3	8	1.50	1.50	2.24	[153]
6	4	15	1.60	1.71	2.5	(17.1.13)
7	4	16	1.75	1.87	2.8	[153]
$5 \cdot 2^{r-4} + 1$	$r$	$2^r - 1$	$\approx 5r/16$	$< r$		(17.1.13)
4	$\log 7$	7	1.60			[553]
5	$\log 11$	11	1.57			[76]
7	$\log 15$	15	1.82			[483]

$\phi = rg/n$  - achieved efficiency through WOM-codes;

$\phi(g, r)$  - upper bound on the efficiency as a function of  $g$  and  $r$  [553];

$\phi(g)$  - estimated upper bound on the efficiency as a function of  $g$  [553].

## 17.6 Notes

§17.1 WOMs have been introduced by Rivest and Shamir [553]. Section 17.1 follows Cohen, Godlewski and Merkx [153], where the coset-encoding writing rule is introduced.

The supercode lemma is folklore. Example 17.1.7 is by Rivest and Shamir [553]. The properties of the  $[23, 12, 7]_3$  Golay code can be found in, e.g., MacWilliams and Sloane [464]. The case  $|I| = 8$  in the proof of Theorem 17.1.10 is treated in [153].

§17.2 The treatment of the error case, presented in Sections 17.2, 17.3 and 17.4, follows Zémor and Cohen [702]. Writing on the WOM requires a complete decoding algorithm for shortened BCH codes, which is simple for 2- and 3-error-correcting BCH codes.

Reading and correcting errors is straightforward (it amounts to syndrome computation).

Note that we have only estimated the efficiency of the BCH WOM-codes (it could be higher). It is not clear to us whether increasing the minimum distance can further raise the efficiency of the error-correcting WOM-code.

§17.5 The notation  $\omega(< v >^g)$  is introduced by Rivest and Shamir [553]. Their conjectured (17.5.1) is disproved by Alon, Nathanson and Ruzsa [19], who also prove Theorem 17.5.2. The construction yielding (17.5.4) is due to Godlewski [252]. See Wei [682] and Cohen, Litsyn and Zémor [163] for bounds

on the  $i$ -th distance. The nonconstructive proof of (17.5.7) is by Rivest and Shamir [553].

Finally, let us mention that some cryptographic aspects of WOMs are studied by Cohen and Godlewski [152], [253].

This Page Intentionally Left Blank

# Chapter 18

## Subset sums and constrained memories

We begin this chapter by recalling some basic facts on Cayley graphs and their relation to coding. We then consider in Section 18.2 two extremal problems in combinatorial group theory with a distinct coding flavour. Section 18.3 is devoted to maximal sum-free sets and to the codes they yield. We then turn to connections with constrained memories (Section 18.4); when the constraints are translation-invariant (this is the case for, e.g., write-isolated, reluctant and defective memories), we show in Section 18.5 that a coding strategy based on packing by coverings applies. In Section 18.6, a special type of memories (reluctant memories) is linked to the domatic number of a graph. Section 18.7 deals with defective memories. The chapter ends with a few words on the error case.

### 18.1 Cayley graphs

Network theory deals with the estimation of graph parameters such as diameter, maximal degree, robustness, ... These concepts have coding-theoretical counterparts in several situations: for instance, Cayley graphs can be associated with codes to yield the following correspondences:

$$\begin{array}{lll} \text{diameter} & \leftrightarrow & \text{covering radius} \\ \text{degree} & \leftrightarrow & \text{length} \\ \text{robustness} & \leftrightarrow & \text{dual distance.} \end{array}$$

Given an abelian group  $G$ , and a generating subset  $S$  of  $G$ , let us denote by  $(G, S)$  the associated Cayley graph. Recall that  $(G, S)$  is a graph having the elements of  $G$  for vertices and that there is an edge from  $g$  to  $g'$  if and

only if  $g' = g + s$  where  $s \in S$ . If  $S = -S$ , then  $(G, S)$  is an undirected graph. Having chosen for  $S$  a generating subset makes  $(G, S)$  a connected graph.

From the purely degree and diameter point of view, one should turn to Cayley graphs on noncommutative groups. However, to emphasize the links with coding theory, we restrict our attention to the commutative case, and more precisely to  $(\mathbb{Z}/2\mathbb{Z})^r$ , the additive group of  $\mathbb{F}^r$ , which we still denote by  $\mathbb{F}^r$ . Note that  $(G, S)$  is undirected in this instance. Our approach is the following: what can coding theory tell us about the graph-theoretical properties of  $(G, S)$ ?

Now we introduce the main tool coding theory can provide for the study of  $(G, S)$ . Let  $S = \{s_1, \dots, s_n\}$ ,  $\mathbf{0} \notin S$  (so there are no loops) and  $|S| = n$ .

We have the following obvious

**Fact 1.** The degree of every vertex in the graph  $(G, S)$  is  $n$ .

Taking the elements  $s_i$  of  $S$  as column vectors, we can form an  $r \times n$  matrix  $\mathbf{H} = (s_1, \dots, s_n)$ , which we use as a parity check matrix to define an  $[n, n-r, d \geq 3]$  code  $C(S)$ .

**Fact 2.** There is a one-to-one correspondence between the words of weight  $m$  of  $C(S)$  and the subsets  $T$  of  $S$  such that

$$|T| = m \text{ and } \sum_{s \in T} s = \mathbf{0}.$$

The quantity  $d(\mathbf{y}, C)$  can be interpreted in terms of the set  $S$ :

**Fact 3.**  $d(\mathbf{y}, C) = \min\{t : \sum_{s \in T} s = \sum_{i \in \text{supp}(\mathbf{y})} s_i \text{ for some } T \subseteq S, |T| = t\}$ .

Denote by  $D(G, S)$  the diameter of the graph  $(G, S)$ , i.e.,

$$D(G, S) = \max_{g, g' \in G} \delta(g, g'),$$

where  $\delta$  denotes the *graphic distance*, that is, the length of the shortest connecting path. Since  $(G, S)$  is a Cayley graph, its diameter is simply the maximum distance between  $\mathbf{0}$  and an arbitrary element  $\mathbf{x}$  of  $G$ , i.e.,

$$D(G, S) = \max_{\mathbf{x} \in \mathbb{F}^r} \delta(\mathbf{0}, \mathbf{x}).$$

Now  $\delta(\mathbf{0}, \mathbf{x})$  is, by definition of  $(G, S)$ , given by

$$\delta(\mathbf{0}, \mathbf{x}) = \min\{t : \sum_{s \in T} s = \mathbf{x} \text{ for some } T \subseteq S, |T| = t\}.$$

So, Fact 3 tells us that

$$d(\mathbf{y}, C) = \delta(\mathbf{0}, \sum_{i \in \text{supp}(\mathbf{y})} \mathbf{s}_i). \quad (18.1.1)$$

Since  $S$  generates  $\mathbb{F}^r$ ,  $\sum_{i \in \text{supp}(\mathbf{y})} \mathbf{s}_i$  ranges over all of  $\mathbb{F}^r$ , when  $\mathbf{y}$  ranges over  $\mathbb{F}^n$ . Hence

$$\max_{\mathbf{y} \in \mathbb{F}^n} d(\mathbf{y}, C) = \max_{\mathbf{x} \in \mathbb{F}^r} \delta(\mathbf{0}, \mathbf{x}).$$

In other words, we have proved:

**Fact 4.** The diameter of  $(G, S)$  equals the covering radius of  $C(S)$ :

$$D(G, S) = R(C(S)).$$

## 18.2 Subset sums

As before, let  $G$  denote the group  $\mathbb{F}^r$  and  $S$  be a generating set of  $G$  not containing  $\mathbf{0}$ . For any positive integer  $i$ , recall from Section 17.5 that  $S^{\neq i}$  stands for the set of sums of  $i$  distinct elements of  $S$ . Set  $S^{\neq 0} = S^0 = \{\mathbf{0}\}$  and for any nonempty set  $I$  of nonnegative integers, let  $S^I = \cup_{i \in I} S^{\neq i}$ . Denote by  $R(S)$  the smallest integer  $t$  such that any nonzero element of  $G$  can be expressed as a sum of  $t$  or fewer elements of  $S$ , i.e., such that

$$G^* \subseteq S^{[1,t]} \text{ (or } G = S^{[0,t]}).$$

We wish to focus on the following additive problems on  $\mathbb{F}^r$ :

**Problem 1.** For given  $r$  and  $t$ , find the smallest  $s$  such that  $|S| \geq s$  implies  $R(S) \leq t$ , i.e.,  $G = S^{[0,t]}$ .

**Problem 2.** Given  $r$ ,  $L \subseteq [0, n]$ , find the smallest  $s$  such that  $|S| \geq s$  implies  $G = S^L$ .

Problem 2 is obviously a generalization of Problem 1. The following is readily checked.

**Theorem 18.2.1** *The correspondence  $S \rightarrow C(S)$  is such that*

$$R(S) = R(C(S)).$$

□

This correspondence transforms problems of an additive nature into covering problems.

We now focus on Problem 1, asking for those sets  $S$ , and their cardinalities, such that  $S^{[1,R]} = S \cup S^{\neq 2} \cup \dots \cup S^{\neq R}$  grows as slowly as possible.

## Problem 1

Recall from Section 17.5 that  $s_G(R)$  denotes the smallest integer  $s$  such that, for any generating set  $S$  of  $G$ ,  $R(S) \leq R$  whenever  $|S| \geq s$ . In other words,  $s_G(R) - 1$  is the largest possible cardinality of a generating set  $S$  of  $G$  such that  $R(S) > R$ . Problem 1 asks for the determination of  $s_G(R)$ . In view of the discussion of the preceding section, this can be understood as asking for the largest possible covering radius of a linear code  $C(S)$  of given length and dimension, and with minimum distance at least three. This pursues the study initiated in Section 8.1 in relation with  $T(n, k, 3)$ .

### A lower bound on $s_G(R)$

We consider the following sets.

**Definition 18.2.2** Call a  $\mu$ -cylinder of  $\mathbb{F}^r$ , a subset isomorphic to  $S \cup \{0^r\} = B_1(0^\mu) \oplus \mathbb{F}^{r-\mu}$ . In other words,  $S$  is the subset of all the nonzero vectors of  $\mathbb{F}^r$  whose first  $\mu$  coordinates make up a vector of weight at most one. If  $S \cup \{0\}$  is a  $\mu$ -cylinder of  $\mathbb{F}^r$ , then  $R(S) = \mu$  and  $|S| = (\mu + 1)2^{r-\mu} - 1$ .

Since  $s_G(R) + 1$  must be larger than the cardinality of an  $(R + 1)$ -cylinder, we have:

**Theorem 18.2.3** Whenever  $r \geq R + 1$ ,

$$s_G(R) \geq \frac{R + 2}{2^{R+1}} |G|.$$

□

### Upperbounding $s_G(R)$

It is possible to prove that the above lower bound is the best possible for some values of  $r$  by a coding argument. The idea is to say, broadly speaking, that a code cannot have too large a covering radius, otherwise, without changing the minimum distance, one would use it to construct a code with an impossibly large dimension.

Recall that  $a[n, d]$  stands for the maximum dimension of a binary linear code of length  $n$  and minimum distance at least  $d$ .

**Theorem 18.2.4** Let  $C$  be an  $[n, k, d]_R$  code. Then

$$k + a[R, d] \leq a[n, d].$$

**Proof.** See Theorem 17.2.2 for the proof of a slightly more general result, and Theorem 8.1.18 for a nonlinear version.  $\square$

**Lemma 18.2.5**  $a[n, 3] = n - 1 - \lfloor \log_2 n \rfloor$ .

**Proof.** One just needs to find the smallest  $r = n - k$  such that there exists an  $r \times n$  matrix with distinct nonzero columns. See also the end of Section 8.1.

$\square$

Applying Theorem 18.2.4 and Lemma 18.2.5 to an  $[n = |S|, k = n - r, 3]R + 1$  code shows that  $\log_2 n < r - R + \lfloor \log_2(R + 1) \rfloor$  and we obtain the following upper bound on  $s_G(R)$ .

**Theorem 18.2.6**

$$s_G(R) \leq \frac{|G|}{2^{R - \lfloor \log_2(R + 1) \rfloor}}.$$

$\square$

For small  $R$ , refinements are possible: see Table 18.1 in the Notes.

Remarkably, the two bounds in Theorems 18.2.3 and 18.2.6 coincide for  $R$  of the form  $2^m - 2$ .

**Corollary 18.2.7** For  $m \geq 2$ ,  $r \geq 2^m - 1$ ,

$$s_G(2^m - 2) = \frac{|G|}{2^{2^m - m - 1}}.$$

$\square$

## Problem 2

For  $n > 0$ , and for  $w > 0$  or  $w = 0$  and  $n$  even, let  $K^\pm(n, w)$  be the minimal  $K$  for which there exists a code  $V$  of size  $K$ ,  $V = \{\mathbf{v}_1, \dots, \mathbf{v}_K\}$  with the property that for any  $\mathbf{x} \in \mathbb{F}^n$  there exists a  $\mathbf{v}_i \in V$  such that

$$|n - 2d(\mathbf{v}_i, \mathbf{x})| \leq w, \tag{18.2.8}$$

where (18.2.8) is a rewriting of  $|\langle \mathbf{v}_i^\pm, \mathbf{x}^\pm \rangle| \leq w$ .

Notice that if  $w > 0$  and  $w \equiv n + 1 \pmod{2}$ , then  $K^\pm(n, w - 1) = K^\pm(n, w)$ . So in the following we consider only the case  $w \equiv n \pmod{2}$ .

**Theorem 18.2.9** If  $n > 0$ ,  $w \geq 0$  and  $w \equiv n \pmod{2}$ , then

$$K^\pm(n, w) = b(n, w) := \lceil \frac{n}{w+1} \rceil.$$

**Proof.** Set

$$\mathbf{v}_1 = 1^n;$$

$$\mathbf{v}_2 = 0^{w+1}1^{n-(w+1)};$$

.....;

$$\mathbf{v}_i = 0^{(i-1)(w+1)}1^{n-(i-1)(w+1)};$$

.....;

$$\mathbf{v}_{b(n,w)} = 0^{(b(n,w)-1)(w+1)}1^{n-(b(n,w)-1)(w+1)}.$$

Now for all  $i$ ,  $n - 2d(\mathbf{v}_i, \mathbf{x}) \not\equiv w+1 \pmod{2}$  and combining

$$n - 2d(\mathbf{v}_1, \mathbf{x}) = 2w(\mathbf{x}) - n,$$

with

$$n - 2w(\mathbf{x}) - 2(w+1) \leq n - 2d(\mathbf{v}_{b(n,w)}, \mathbf{x}) \leq n - 2w(\mathbf{x}) + 2(w+1),$$

and noticing that

$$|(n - 2d(\mathbf{v}_i, \mathbf{x})) - (n - 2d(\mathbf{v}_{i+1}, \mathbf{x}))| =$$

$$2|d(\mathbf{v}_{i+1}, \mathbf{x}) - d(\mathbf{v}_i, \mathbf{x})| \leq 2d(\mathbf{v}_i, \mathbf{v}_{i+1}) = 2(w+1),$$

one concludes by a “discrete intermediate-value theorem” that (18.2.8) holds for some  $i$ .

Now we prove the lower bound, with the help of the following lemma.

**Lemma 18.2.10** Let  $P(\mathbf{y}^\pm) = P(y_1^\pm, y_2^\pm, \dots, y_n^\pm)$  be a multilinear polynomial over the reals, different from 0. If  $P(\mathbf{y}^\pm) = 0$  for every  $\mathbf{y}$  having even (odd) weight, then  $\deg P \geq n/2$ .

**Proof.** We prove the even case (the odd case is analogous).

We construct a  $2^n \times 2^{n-1}$  matrix  $\mathbf{A}$  with rows labelled with the vectors in  $\mathbb{F}^n$  and columns labelled with the even vectors in  $\mathbb{F}^n$ :

$$\mathbf{A} = (a(\mathbf{x}, \mathbf{z})) = \left( (-1)^{\langle \mathbf{x}, \mathbf{z} \rangle} \right).$$

It is easy to see that  $(-1)^{\langle \mathbf{x}, \mathbf{z} \rangle}$  is actually the value of the one-term multilinear polynomial  $\prod_{i: x_i=1} y_i$ , at  $y_i = z_i^\pm$ . Let  $\mathbf{B}$  be a submatrix of  $\mathbf{A}$  consisting of a subset of the rows of  $\mathbf{A}$ , such that if the row corresponding to  $\mathbf{x}$  is in  $\mathbf{B}$  then the row corresponding to  $\bar{\mathbf{x}}$ , the complement of  $\mathbf{x}$ , is not in  $\mathbf{B}$ . Let us

compute the scalar product of two rows of  $\mathbf{B}$ . If the rows are different they are orthogonal since

$$(-1)^{\langle \mathbf{x}_1, \mathbf{z} \rangle} (-1)^{\langle \mathbf{x}_2, \mathbf{z} \rangle} = (-1)^{\langle \mathbf{x}_1 + \mathbf{x}_2, \mathbf{z} \rangle},$$

and by assumption  $\mathbf{x}_1 + \mathbf{x}_2 \neq \mathbf{1}$ . So,  $\mathbf{x}_1 + \mathbf{x}_2$  is a binary vector different from  $\mathbf{0}$  and  $\mathbf{1}$ , and on the set of even vectors  $\mathbf{z}$  the scalar products  $\langle \mathbf{x}_1 + \mathbf{x}_2, \mathbf{z} \rangle$  take even and odd values an equal number of times. The scalar product of a row with itself is  $2^{n-1}$ , so

$$\mathbf{B}\mathbf{B}^T = 2^{n-1} \mathbf{I}_{2^{n-1}},$$

$\mathbf{B}\mathbf{B}^T$  is nonsingular and the rows of  $\mathbf{B}$  are linearly independent over the reals. Hence, no sum of the columns equals  $\mathbf{0}$ . This means that no multilinear polynomial vanishes on all even vectors if it does not contain at least one pair of complementary terms, say,  $\prod_{i \in I} y_i$  and  $\prod_{i \in N \setminus I} y_i$ , where  $N = \{1, 2, \dots, n\}$  and  $I \subseteq N$  is an arbitrary subset. Clearly, either  $|I|$  or  $|N \setminus I|$  is at least  $n/2$ , which concludes the proof of the lemma.  $\square$

**End of the proof of Theorem 18.2.9.** Let  $n \equiv 0 \pmod{4}$  and  $w \equiv 0 \pmod{4}$  (for other cases the proof is similar). Let  $V = \{\mathbf{v}_1, \dots, \mathbf{v}_K\}$  be a code such that for every vector  $\mathbf{x} \in \mathbb{F}^n$  there exists an  $i$  such that (18.2.8) holds. Let  $V_e$  ( $V_o$ ) be the set of all even (odd) vectors of  $V$ .

Consider the following polynomial in  $\mathbf{y}^\pm = (y_1^\pm, \dots, y_n^\pm)$ :

$$\begin{aligned} P(\mathbf{y}^\pm) = \prod_{\mathbf{v} \in V_e} \langle \mathbf{v}^\pm, \mathbf{y}^\pm \rangle \prod_{\mathbf{v} \in V_o} (2^2 - \langle \mathbf{v}^\pm, \mathbf{y}^\pm \rangle^2) \prod_{\mathbf{v} \in V_e} (4^2 - \langle \mathbf{v}^\pm, \mathbf{y}^\pm \rangle^2) \dots \\ \prod_{\mathbf{v} \in V_e} (w^2 - \langle \mathbf{v}^\pm, \mathbf{y}^\pm \rangle^2). \end{aligned}$$

It is easy to check that for every even  $\mathbf{y}$ ,  $P(\mathbf{y}^\pm) = 0$ . Let  $\widehat{P}(\mathbf{y}^\pm)$  be the multilinear polynomial obtained from  $P(\mathbf{y}^\pm)$  by replacing repeatedly each occurrence of  $(y_i^\pm)^2$  by 1 in the standard representation of  $P$  as a sum of monomials. Clearly,  $\widehat{P}(\mathbf{y}^\pm) = P(\mathbf{y}^\pm)$  for all  $\mathbf{y}^\pm$ . Moreover,  $\widehat{P}(\mathbf{y}^\pm)$  is not 0 since it does not vanish at odd vectors. Therefore, by Lemma 18.2.10

$$|V_e| + \frac{w}{2}(|V_e| + |V_o|) = \deg P \geq \deg \widehat{P} \geq n/2. \quad (18.2.11)$$

Repeating the above process for odd vectors  $\mathbf{y}$  and the polynomial obtained from  $P$  by changing the ranges of multiplication to complementary, namely,  $V_e$  to  $V_o$  and vice versa, we get

$$|V_o| + \frac{w}{2}(|V_e| + |V_o|) \geq n/2. \quad (18.2.12)$$

The summation of (18.2.11) and (18.2.12) completes the proof of the theorem.  $\square$

Rewriting (18.2.8) as

$$(n - w)/2 \leq d(\mathbf{v}_i, \mathbf{x}) \leq (n + w)/2,$$

we see that  $V$  is in fact a covering with “shells”  $S_{[(n-w)/2, (n+w)/2]}(\mathbf{v}_i)$ , where

$$S_L(\mathbf{v}) := \{\mathbf{x} \in \mathbb{F}^n : d(\mathbf{x}, \mathbf{v}) \in L\}$$

is an  $L$ -sphere for  $L \subseteq [0, n]$  (see Section 19.1). In this case, the sphere-covering bound gives

$$|V| \geq \frac{2^n}{\sum_{i \in L} \binom{n}{i}}. \quad (18.2.13)$$

For  $L = [(n - w)/2, (n + w)/2]$  we get that the right hand side of (18.2.13) is in  $O(n^{1/2})$ , but we know that this lower bound is not tight, since  $b(n, w)$  turns out to be the exact value of  $K^\pm(n, w)$ . For any set  $L \subseteq [0, n]$ , the method used to prove the lower bound of Theorem 18.2.9 can be applied, providing the following result.

**Theorem 18.2.14** *Let  $L \subseteq [0, n]$  and  $C$  be an  $L$ -covering, i.e., a code such that for all  $\mathbf{x} \in \mathbb{F}^n$ , there exists a  $\mathbf{c} \in C$  with  $d(\mathbf{x}, \mathbf{c}) \in L$ . Then*

$$|C| \geq \frac{n}{|L|}.$$

$\square$

This bound is weaker than the sphere-covering bound for  $L = [0, t]$ , but tight for  $L = [(n - w)/2, (n + w)/2]$ .

**Corollary 18.2.15** *There is no perfect  $L$ -covering with  $L = [(n - w)/2, (n + w)/2]$ .*

**Proof.** Combine (18.2.13) and Theorem 18.2.14.  $\square$

### 18.3 Maximal sum-free sets

**Definition 18.3.1** *A subset  $S = \{s_1, s_2, \dots, s_n\}$  of  $\mathbb{F}^r$  is called sum-free (SF) if*

$$s_i, s_j \in S \Rightarrow s_i + s_j \notin S. \quad (18.3.2)$$

*The set  $S$  is said to be maximal sum-free (MSF) if it is maximal for inclusion with the SF property.*

Setting  $\mathbf{H} = [s_1, \dots, s_n]$ , the SF property is equivalent to  $C(S)$ , the code with parity check matrix  $\mathbf{H}$ , having minimum distance at least four.

Maximality means that for all  $\mathbf{y}$  not in  $S$  there exist two elements in  $S$  with sum equal to  $\mathbf{y}$ , i.e.,  $R(C(S)) = 2$ . A (*complete*) *cap* in a projective geometry is a (maximal) collection of points no three of which are collinear. Elements of  $S$  are identified with points in  $PG(r-1, 2)$ , the  $(r-1)$ -dimensional binary projective geometry.

Summarizing:

**Theorem 18.3.3** *The following properties are equivalent.*

- (i) *A subset  $S$  of  $\mathbb{F}^r$  with size  $n$  is maximal sum-free.*
- (ii) *Its associated code  $C(S)$  is an  $[n, n-r, 4]_2$  code or the  $[5, 1, 5]_2$  code.*
- (iii)  *$S \cap (S + S) = \emptyset$  and  $S \cup (S + S) = \mathbb{F}^r$ , i.e.,  $(S, 2S)$  is a partition of  $\mathbb{F}^r$ .*
- (iv)  *$S$  is a complete cap in  $PG(r-1, 2)$ .* □

The notion of SF set immediately carries over to any abelian group  $G$ . If  $S$  is any subset of a coset  $H + x$ ,  $x \notin H$ , where  $H$  is a subgroup of  $G$ , then clearly  $S$  is SF. Such a subset is called *trivial*.

**Lemma 18.3.4** *Any subset  $S$  of an abelian group  $G$  with  $|S| \geq \lceil |G|/2 \rceil$  and  $0 \notin S$  satisfies  $S \cup 2S = G$ .*

**Proof.** Let  $g$  be a nonzero element of  $G$ . If  $g \notin S$ , then, by the pigeon-hole principle,  $\{g - s : s \in S\} \cap S \neq \emptyset$ . Hence there exist  $s_1$  and  $s_2$  in  $S$  such that  $g = s_1 + s_2$ . □

**Lemma 18.3.5** *If  $G$  contains a subgroup  $G_0$  of index two, then there exists  $S \subset G$ , with size  $(|G|/2) - 1$  and  $S \cup 2S \neq G$ .*

**Proof.** Pick  $h \in G \setminus G_0$  and set  $S = (G_0 + h) \setminus \{h\}$ . Then  $h \notin S \cup 2S$ . □

Combining Lemmas 18.3.4 and 18.3.5, we get the exact value of  $s_G(2)$  for a wider class of groups than  $\mathbb{F}^r$  (Corollary 18.2.7):

**Theorem 18.3.6** *If  $G$  is an abelian group containing a subgroup of index two, then*

$$s_G(2) = |G|/2.$$

□

From the preceding discussion, it is clear that, if  $G$  contains a subgroup  $G_0$  of index two, then an MSF subset is precisely the coset of  $G_0$ .

The current record for the minimum length of an MSF set is established for even  $r$ ,  $r \geq 10$ :

$$|S| = \frac{15}{8}2^{r/2} - 3. \quad (18.3.7)$$

**Theorem 18.3.8** *A lower bound for the size of an MSF set in  $\mathbb{F}^r$  is  $\sqrt{2} \cdot 2^{r/2}(1 + o(1))$ .*

**Proof.** Combine

$$|2S| \leq 1 + \binom{n}{2}$$

with

$$|S| + |2S| = 2^r.$$

□

**Conjecture 18.3.9** *The previous lower bound is asymptotically tight.*

## 18.4 Constrained memories ( $\mathbf{W^*Ms}$ )

We now consider a binary storage medium consisting of  $n$  cells on which we want to store and update information. These operations must be performed under some constraints, dictated by technology, cost, efficiency, speed, ... In the past few years, many models have been studied, which we list here in more or less chronological order: write-once memory or WOM, write-unidirectional memory or WUM and write-isolated memory or WIM.

We also consider the related problems of reluctant memories (WRM) and defective memories (WDM). The reasons for this blossoming of acronyms are evolving technology, fashion, ... and existing letters!

The initial model (WOM) representing the first generation of optical disks differs fundamentally from the others in that writing is irreversible. It is dealt with separately in Chapter 17. Thus here, \* stands for U, I, R or D.

The memory is in a given *state*  $\mathbf{y}$ , that is,  $\mathbf{y} \in \mathbb{F}^n$  is stored in it. Due to the constraints, only a subset  $A(\mathbf{y})$  of  $\mathbb{F}^n$  is reachable from  $\mathbf{y}$ . Let us write  $\mathbf{y} A \mathbf{y}'$  if and only if  $\mathbf{y}'$  is reachable from  $\mathbf{y}$  and call the constraint *symmetric* if  $A$  — viewed as a binary relation — is. Define the (directed) *constraint graph*  $(\mathbb{F}^n, A)$  as a digraph with vertex set  $\mathbb{F}^n$  and an arc from  $\mathbf{y}$  to  $\mathbf{y}'$  if and only if  $\mathbf{y} A \mathbf{y}'$ .

The state  $\mathbf{y}$  can be updated to  $v(\mathbf{y})$  states, where  $v(\mathbf{y})$  is the *outdegree* of  $\mathbf{y}$ . To store one among  $M$  messages on the memory, the following must clearly hold:

**Theorem 18.4.1**  $M \leq \max_{\mathbf{y} \in \mathbb{F}^n} v(\mathbf{y})$ . □

Although very simple, we shall see that this bound is tight in some cases. We want to continue the writing process indefinitely, under a specific constraint depending on  $*$ .

The problem is: what is asymptotically the maximum achievable rate  $\kappa$  of the  $W^*M$ , defined as

$$\kappa = (1/n) \log_2 M ?$$

Let us now describe one first type of constraint.

## WUM

A write-unidirectional memory is constrained, during the updating, to either writing 1's in selected bit positions or 0's in selected bit positions and no combinations of 0's and 1's. Such a constraint arises when the mechanism that chooses to write 0's or 1's operates much more slowly than the means of accessing and scanning a word. The subset  $A(\mathbf{y})$  depends on the weight  $w$  of the state  $\mathbf{y}$ :

$$|A(\mathbf{y})| = 2^w + 2^{n-w} - 1.$$

Notice that the WUM constraint is not symmetric. Next section describes  $W^*Ms$  satisfying an even stronger requirement than symmetry.

## 18.5 Translation-invariant constraints

We say that the constraints are *translation-invariant* if

$$A(\mathbf{y}) = \mathbf{y} + A(\mathbf{0}) = \{\mathbf{y} + \mathbf{x} : \mathbf{x} \in A(\mathbf{0})\}.$$

We set  $A(\mathbf{0}) = A$ ,  $|A| = a_n$ , to emphasize dependency on  $n$ , and call  $A(\mathbf{x})$  the *A-set centred at x*.

Obviously, translation-invariance is a stronger requirement than symmetry. It also implies that the constraint graph is regular: for all  $\mathbf{y} \in \mathbb{F}^n$ ,  $|A(\mathbf{y})| = a_n$ . So we may assume that we are in the state  $\mathbf{0}$ , and by Theorem 18.4.1,  $M \leq a_n$ .

Let us now describe the main types of translation-invariant constraints.

## WIM

On a write-isolated memory no change of two consecutive positions is allowed when updating:

$$a_n = |\{\mathbf{x} = (x_1, x_2, \dots, x_n) \in \mathbb{F}^n : x_j x_{j+1} = 0 \text{ for } j = 0, 1, \dots, n-1\}|.$$

It is well known that  $a_n$  is  $\phi(n)$ , the  $n$ -th Fibonacci number, with

$$\phi(0) = 1, \phi(1) = 2, \phi(i+2) = \phi(i+1) + \phi(i), i \geq 0.$$

Asymptotically

$$n^{-1} \log_2 \phi(n) \approx \log_2 \frac{1 + \sqrt{5}}{2} \approx 0.69$$

and

$$\kappa \leq 0.69.$$

## WRM

Suppose our storage media allows only a limited number, say  $R$ , of bit changes when updating:

$$a_n = |\{\mathbf{x} \in \mathbb{F}^n : w(\mathbf{x}) \leq R\}| = V(n, R).$$

If only a fraction  $R = \lambda n$ ,  $0 \leq \lambda \leq 1/2$ , of the total number  $n$  of positions may change when updating, then an upper bound on the capacity is

$$\kappa \leq H(\lambda).$$

For more on reluctant memories, see Section 18.6.

## WDM

The model is the following: a set  $S_0$  of positions of the memory are stuck at “0”, a set  $S_1$  at “1”. For an  $s$ -defective memory, the sets  $S_0$  and  $S_1$  are known to the encoder only and satisfy  $|S_0| + |S_1| = s$ ; although the state 0 is not reachable when  $S_1 \neq \emptyset$ , upon translating on the positions corresponding to  $S_1$  we can consider that we are in a translation-invariant model, where

$$A = \{\mathbf{x} \in \mathbb{F}^n : x_j = 0 \text{ for } j \in S_0 \cup S_1\}.$$

That is,  $A$  is a *subcube* of dimension  $n - s$ :

$$a_n = 2^{n-s}$$

and

$$\kappa \leq 1 - s/n.$$

For more on defective memories, see Section 18.7.

## Cloud encoding — packings by coverings

We now present a coding strategy based on the notion of  $A$ -coverings which applies whenever the constraints are translation-invariant.

A subset  $B = \{\mathbf{b}_i\}$  of  $\mathbb{F}^n$  is called an  $A$ -covering or *cloud* if

$$\bigcup_{\mathbf{b}_i \in B} A(\mathbf{b}_i) = \mathbb{F}^n.$$

That is,  $\mathbb{F}^n$  is covered by the  $A$ -sets centred at the elements of  $B$ . Clearly, if a cloud  $B$  is an  $A$ -covering, so is any translate  $B + \mathbf{x}$ ,  $\mathbf{x} \in \mathbb{F}^n$ .

If  $B$  is a an  $A$ -covering, then

$$\text{for all } \mathbf{x} \in \mathbb{F}^n, \text{ there exists } \mathbf{b} \in B \text{ such that } \mathbf{b} A \mathbf{x}. \quad (18.5.1)$$

Using symmetry,  $\mathbf{x} A \mathbf{b}$  holds as well. In other words, starting from any state  $\mathbf{x}$  of the memory, there exists an allowed transition which transforms  $\mathbf{x}$  into an element of  $B$ .

To write on a  $W^*M$ , use the following strategy: define an encoding function which associates to a message  $m_i$  an  $A$ -covering  $C_i$  of  $\mathbb{F}^n$ :

$$m_i \leftrightarrow C_i = \{\mathbf{c}_{i,1}, \mathbf{c}_{i,2}, \dots\},$$

where, for all  $i$

$$\bigcup_{\mathbf{c}_{i,j} \in C_i} A(\mathbf{c}_{i,j}) = \mathbb{F}^n.$$

In that way, whatever the state  $\mathbf{y}$  of the memory is,  $\mathbf{y}$  can be updated to one of the  $\mathbf{c}_{i,j}$ 's encoding  $m_i$ , while satisfying the constraints.

**Theorem 18.5.2** *If  $B_1, B_2, \dots, B_M$  are pairwise disjoint  $A$ -coverings, they yield a  $W^*M$ -code of size  $M$ .*

**Proof.** Put the  $M$  messages in one-to-one correspondence with the  $M$  clouds. By (18.5.1), whatever the state of the  $W^*M$  is, updating is possible to any message. Note that from the strict point of view of using the memory, each  $B_i$  need not be an  $A$ -covering of  $\mathbb{F}^n$  but should satisfy a weaker condition, namely that it is an  $A$ -covering of the union of the  $B_j$ 's.  $\square$

We now address the following problem: what is the maximum number of  $A$ -coverings of  $\mathbb{F}^n$  that can be packed in  $\mathbb{F}^n$ , i.e., have void pairwise intersection?

We show that the upper bound in Theorem 18.4.1 is asymptotically tight. We first establish the existence of small  $A$ -group coverings of  $\mathbb{F}^n$  (i.e., clouds which are groups). Then the second step, finding pairwise disjoint clouds,

becomes simple: if  $G$  is a group  $A$ -covering with  $|G| = 2^k$ , then there are  $2^{n-k}$  pairwise disjoint  $A$ -coverings, namely the cosets of  $G$ . To that end, we use a greedy algorithm (see Section 20.3), in a group version.

**Theorem 18.5.3** *There exists a group covering  $G$  of  $\mathbb{F}^n$  of size  $2^k$ , with*

$$k = n - \log_2 a_n + \log_2 n + O(1).$$

□

This scheme gives

$$M = 2^{n-k} = \Omega(a_n/n),$$

and the following result.

**Theorem 18.5.4**

$$\kappa = \lim_{n \rightarrow \infty} n^{-1} \log_2 a_n.$$

□

Dropping the group condition, one can obtain still smaller  $A$ -coverings, but this of course does not improve the rate.

We now present a generalization to any graph of the problem of packing by coverings.

## 18.6 Domatic number and reluctant memories

Given a graph  $\Gamma = (V, E)$  and a vertex  $v \in V$ , we may define the sphere of radius  $r$  centred at  $v$  as the set of all vertices of the graph being at graphic distance at most  $r$  from  $v$ . Clearly, the sphere  $B_1(v)$  of radius one consists of  $v$  and all vertices adjacent to it. The *domatic number*  $\alpha(\Gamma)$  of a graph  $\Gamma$  is the maximum number of colours in a vertex-colouring of  $\Gamma$  such that any sphere of radius one contains  $\alpha(\Gamma)$  of them. In other words, it is the maximum number of vertex-disjoint coverings of  $\Gamma$ .

Let  $K(\Gamma)$  be the *covering number* of  $\Gamma$ , i.e., the minimal number of vertices such that the spheres of radius one centred at these vertices cover  $V$ . Then clearly

$$\alpha(\Gamma) \leq \frac{|V|}{K(\Gamma)}. \quad (18.6.1)$$

In the case of translation-invariant constraints,  $V$  is the constraint graph  $(\mathbb{F}^n, A(\mathbf{0}))$ . Reverting to the hypergraph with set of vertices  $\mathbb{F}^n$  and set of

hyperedges  $\{A(\mathbf{x}) : \mathbf{x} \in \mathbb{F}^n\}$ , we see that this hypergraph is  $|A|$ -regular and  $|A|$ -uniform. Then (see Problems 1 and 2 in Section 20.3) the Johnson-Stein-Lovász theorem yields via a greedy algorithm a covering with size

$$K(\Gamma) \leq \frac{2^n}{|A|} (1 + \ln |A|).$$

Furthermore, the greedy algorithm can again be linearized, like in Theorem 18.5.3, outputting a group covering  $C$  of size  $2^k$  with

$$k = n - \log_2 |A| + \log_2 n + O(1).$$

This gives, taking cosets of  $C$ :

**Theorem 18.6.2** *An asymptotic lower bound on the domatic number of the constraint graph  $\Gamma = (\mathbb{F}^n, A)$  is  $\Omega(|A|/n)$ .*  $\square$

Now, clearly, the number of messages that can be represented on the memory using the “cloud encoding” scheme described in the previous section is  $M = \alpha((\mathbb{F}^n, A))$ .

## Reluctant memories

Here the constraint graph is  $Q_n^R = (V, E)$ , where

$$V = \mathbb{F}^n, \quad E = \{\{\mathbf{x}, \mathbf{y}\} \in V^2 : 1 \leq d(\mathbf{x}, \mathbf{y}) \leq R\}.$$

For  $R = 1$ , this graph is the classical *hypercube*; we denote it by  $Q_n$ .

By (18.6.1), the domatic number  $\alpha_n$  of the hypercube  $Q_n$  is upperbounded by

$$\alpha_n \leq \frac{2^n}{K(n, 1)}.$$

We have seen (Theorem 12.4.11) that

$$K(n, 1) = \frac{2^n}{n+1} (1 + o(1)).$$

Recall that to the  $M$  possible messages we associate subsets  $B_1, \dots, B_M$  of  $\mathbb{F}^n$  with the following properties (cf. the proof of Theorem 18.5.2):

- (i)  $B_i \cap B_j = \emptyset$  for  $i \neq j$ .
- (ii) For any  $\mathbf{x}$  in  $\cup_{1 \leq i \leq M} B_i$  and any  $j, 1 \leq j \leq M$ , there exists  $\mathbf{y}$  in  $B_j$  with  $d(\mathbf{x}, \mathbf{y}) \leq R$ .

We denote by  $u_R(M)$  the smallest integer  $n$  for which (i) and (ii) are possible. The idea is to use a memory of size  $n = u_R(M)$  to store the  $M$  messages. When  $M$  is a power of two, say  $M = 2^m$ , the following result gives a nonconstructive asymptotic upper bound on  $u_{\lambda m}(2^m)$ ,  $\lambda$  constant:

**Theorem 18.6.3** For  $\mu$  constant,  $0 < \mu < 1/2$  and  $m$  large enough,

$$u_{\mu(H(\mu))^{-1}m}(2^m) \leq (H(\mu))^{-1}m.$$

□

In the case  $R = 1$  we have

**Theorem 18.6.4**

$$u_1(M) = M(1 + o(1)).$$

**Proof.** It is based on two lemmas giving the exact value of  $u_1(M)$  when  $M$  is a power of two and lower bounding  $u_1(M)$  in all cases. For intermediate values, rather lengthy density arguments are necessary. We do not give them here. □

**Lemma 18.6.5**

$$u_1(M) \geq M - 1.$$

**Proof.** Let  $\mathbf{x} \in B_i$  be the content of the memory. Any updating to a cloud  $B_j$ ,  $j \neq i$ , must be possible. Hence  $\mathbf{x}$  has at least  $M - 1$  neighbours in the hypercube. □

**Lemma 18.6.6**

$$u_1(2^r) = 2^r - 1.$$

**Proof.** In length  $n = M - 1 = 2^r - 1$ , choose for  $B_1$  a  $[2^r - 1, 2^r - r - 1]$  Hamming code, and for the  $B_i$ 's,  $i \neq 1$ , the  $2^r - 1$  cosets of  $B_1$ . Then  $B_i$  has covering radius one for all  $i$ , which implies  $u_1(2^r) \leq 2^r - 1$ , and equality follows from Lemma 18.6.5. □

From the definition of the domatic number  $\alpha(Q_n^R)$ , we see that

$$u_R(\alpha(Q_n^R)) \leq n.$$

In particular, for  $R = 1$ ,

$$u_1(\alpha_n) \leq n$$

and by Theorem 18.6.4

$$u_1(\alpha_n) = \alpha_n(1 + o(1))$$

when  $n$  hence  $\alpha_n$  goes to infinity.

## 18.7 Defective memories

Recall from Definition 3.7.5 that a matrix  $\mathbf{A}$  with  $n$  columns is  $s$ -surjective if for any set of  $s$  columns, say with indices  $(j_1, j_2, \dots, j_s)$ , and every binary  $s$ -tuple  $(t_1, t_2, \dots, t_s)$ , there exists a row  $\mathbf{m} = (m_1, \dots, m_n)$  in  $\mathbf{A}$  such that  $m_{j_i} = t_i$  for all  $i$ ,  $1 \leq i \leq s$ .

Suppose we have two subsets  $C$  and  $M$  of  $\mathbb{F}^n$ , with the following properties:

- P1. The matrix  $\mathbf{A} = \mathbf{A}(M)$  whose rows are the elements of  $M$  (in any order) is  $s$ -surjective.  
 P2.  $(C + C) \cap (M + M) = \{\mathbf{0}\}$ .

Then  $C$  can be used as a set of messages for storing information on an  $s$ -defective memory in the following way:

Let  $\mathbf{c} = (c_1, c_2, \dots, c_n) \in C$  be the message to be stored. Let  $j_1, j_2, \dots, j_s$  be the indices of the defective positions and  $d_1, d_2, \dots, d_s$ , the stuck-at values. Define  $t_i$ ,  $1 \leq i \leq s$ , by  $t_i = c_{j_i} + d_i$ .

Let  $\mathbf{m}$  be a row of  $\mathbf{A}$  with  $m_{j_i} = t_i$  for  $1 \leq i \leq s$  (its existence stems from P1). Write  $\mathbf{y} = \mathbf{c} + \mathbf{m}$  in the memory. This is possible since  $\mathbf{c} + \mathbf{m}$  matches the defects, i.e.,  $y_{j_i} = c_{j_i} + m_{j_i} = c_{j_i} + t_i = d_i$  for  $i \in \{1, 2, \dots, s\}$ .

Furthermore, the decoding is unambiguous because of P2.

Of course, one can take  $M = B_s(\mathbf{0})$ , which is trivially  $s$ -surjective. But then the Hamming bound implies that asymptotically, for  $s$  fixed,

$$\kappa = n^{-1} \log_2 |C| \leq 1 - sn^{-1} \log_2 n.$$

In fact, as we now show, one can do better, since defects are easier to correct than errors (this is not too surprising).

If  $M$  is an  $[n, r]$  code with its information set on the positions  $[1, r]$ , then  $C = \mathbf{0}^r \oplus \mathbb{F}^{n-r}$  is a possible choice of size  $2^{n-r}$ . Because  $M$  is linear, its dual is an  $[n, n-r, s+1]$  code (cf. last paragraph of Section 2.2), e.g., a shortened BCH code, yielding

$$\kappa = 1 - \lfloor s/2 \rfloor n^{-1} \log_2 n.$$

To further improve on this, we must turn to nonlinear codes (see Notes).

The following condition is easier to check but stronger than P2.

P'2. There exists a set of  $r$  positions, say  $[1, r]$ , such that any two rows of  $M$  differ in at least one of these positions.

If P'2 holds, then again  $\mathbf{0}^r \oplus \mathbb{F}^{n-r}$  is a possible  $C$ . By analogy with the linear case, a set fulfilling P'2 may be called an information set. Write  $r(M)$  for its size. Of course, if  $M$  is linear,  $r(M) = \dim(M)$ . In general, one has:

$$\max\{s, \log_2 |M|\} \leq r(M) \leq n.$$

## 18.8 The error case

Suppose now that  $e = \theta n$  errors may occur during the writing or reading process. Let us give an idea of the methods at hand for general  $W^*Ms$ .

**Theorem 18.8.1** *If there exist  $A$ -coverings  $B_1, B_2, \dots, B_M$  of  $\mathbb{F}^n$ , such that for all  $i \neq j$ :*

$$d(B_i, B_j) \geq 2e + 1,$$

*then there exists an  $e$ -error-correcting  $W^*M$ -code of size  $M$ .*  $\square$

So we are looking for the maximal number of  $A$ -coverings such that not only do they constitute a packing of  $\mathbb{F}^n$ , but furthermore the sets  $\cup_{b \in B_i} B_e(b)$  do not intersect. Applying Gilbert-Varshamov type techniques, one gets

**Theorem 18.8.2** *For  $n$  large enough, there exist  $e$ -error-correcting  $W^*M$ -codes with rate*

$$\kappa(\theta) \geq \kappa - H(2\theta)$$

*where  $\kappa$  is the largest achievable rate in the “noiseless” case.*  $\square$

## 18.9 Notes

§18.2 Theorem 18.2.4 is due to Godlewski [252].

An improvement over Theorem 18.2.6 is obtained by Zémor [701] using a more traditional additive approach:

$$s_G(3) \leq 2^r/3. \quad (18.9.1)$$

The known facts about  $s_G(R)$  when  $G = \mathbb{F}^r$  are summarized in Table 18.1.

The only general bound on Problem 2 is due to Alon, Bergmann, Copersmith and Odlyzko [17], where it is stated in the nonlinear case. We have explicated and rephrased it in coding terminology.

In the case when  $w = 0$  (and hence  $n$  is even), a construction due to Knuth [382] implies that  $K^\pm(n, 0)$  is at most  $n$ ; this construction is generalized in [17] to prove Theorem 18.2.9.

§18.3 For complements on geometry, see, e.g., Hirschfeld [305], and Hill [304], Wolfmann [692] for the relations between caps and codes. If  $S$  is a subset of a coset  $V + h$ , where  $V$  is a subgroup of  $\mathbb{F}^r$  and  $h \notin V$ , then  $S$  is clearly sum-free; it is called *trivial* by Clark and Pedersen in [140], where they prove, using earlier work by Clark, Dunning and Rogers [139], that any  $S$  of size  $|S| > 5 \cdot 2^{r-4}$  is trivial. Hence no MSF set exist for  $5 \cdot 2^{r-4} < |S| < 2^{r-1}$ .

Table 18.1: Values of  $s_G(R)$ .

$R$	Lower bounds	Upper bounds	$s_G(R)$
1			$2^r - 1$ d
2			$2^{r-1}$ e
3	$5 \cdot 2^{r-4}$ c	$2^r/3$ a	
4	$3 \cdot 2^{r-4}$ c	$2^{r-2}$ b	
5	$7 \cdot 2^{r-6}$ c	$2^{r-3}$ b	
$2^m - 2$			$2^{r-2^m+m+1}$ e
$R$	$(R+2)2^{r-R-1}$ c	$2^{r-R+\lfloor \log_2(R+1) \rfloor}$ b	

- a (18.9.1).
- b Theorem 18.2.6.
- c Theorem 18.2.3.
- d from Hamming codes.
- e Corollary 18.2.7.

The record (18.3.7) is due to Gabidulin, Davydov and Tombak [245] (see also the Notes of Chapter 5 on Section 5.4).

§18.4 WUMs were introduced by Borden in an unpublished manuscript [92], and developed by Simonyi [587]. Their relation with combinatorial aspects of conflict resolution in multiple access is studied by Cohen [146]. The information-theoretic approach is adopted by a few authors:

- for WOMs, by Wolf, Wyner, Ziv and Körner [691];
- for WUMs, a thorough presentation, in relation with deterministic two-way channels, is given by van Overveld (see [528] and references therein).

WIMs are studied by Robinson [554], in the context of bar codes. Bounds on the achievable rates and constructions are presented by van Eijl, Cohen and Zémor [215] for WIMs and WUMs. For a slightly different model of WIM, where both the content and the updating should satisfy the nonadjacency constraint, see Cohn [174].

§18.5 A general model, the WEM — where E stand for “efficient”— encompassing WOMs, WUMs, WIMs and WRMs, in which costs are associated to transitions, is introduced by Ahlswede and Zhang in [12]; there the maximal rate achievable with a maximal cost per letter criteria is investigated.

For “group” greedy algorithms, see Cohen [143] and Cohen and Frankl [151].

§18.6 Östergård [521] has recently shown that

$$\alpha(Q_n) = n(1 + o(1)).$$

Thus, one can store  $n + 1 + o(1)$  messages on a WRM with  $R = 1$ .

For  $\Gamma = Q_n^2$ , it is proved in Theorem 4.5.8 that, for an infinite number of values of  $n$ ,

$$K(n, 2) = \frac{2^n}{V(n, 2)} (1 + o(1)).$$

It is tempting to conjecture that, for an infinite number of  $n$ 's,

$$\alpha(Q_n^2) = V(n, 2)(1 + o(1)).$$

This would imply that one can store  $V(n, 2)$  messages on a WRM with  $R = 2$ .

Reluctant memories were introduced by Fellows [235], in the framework of categories. Theorem 18.6.3 is due to Fellows [236], based on a nonconstructive upper bound on covering radius by Cohen [143] (cf. Theorem 12.3.2). Theorem 18.6.4 is also from [236].

**§18.7** The problem of writing on a defective memory has been studied among others by Kuznetsov and Tsypakov [398], Dumer [211], Kuznetsov and Vinck [399]. Starting with a linear set  $M$ , a nonconstructive proof is given by Kuznetsov and Tsypakov in [398] that one can choose a subset  $M'$  of  $M$  such that the resulting  $C$  have rate

$$\kappa \geq 1 - sn^{-1} - n^{-1} \log_2 \ln \left( 2^s \binom{n}{s} \right). \quad (18.9.2)$$

For  $s$  fixed, Busschbach provides in [107] a recursive construction with  $\kappa = 1 - O(n^{-1} \log_2 \log_2 n)$ . This is improved by Dumer in [211]:

$$\log_2 |C| = n - \log_2 \log_2 n - (s - 1) \log_2 \log_2 \log_2 n (1 + o(1)).$$

Combined with the upper bound  $\log_2 |C| \leq n - \log_2 \log_2 n$  due to Kasami, Yamamura and Kuznetsov [370], Dumer's result closes the gap asymptotically for constant  $s$ . From a slightly different perspective, Heegard [291] and Heegard and El Gamal [292] show that the capacity of such a memory is  $1 - p$  if each memory cell has probability  $p/2$  of being stuck at 0 or at 1. Inequality (18.9.2) has been improved by Dumer [211] for *asymmetric defects*, i.e. when  $S_0$  or  $S_1$  is empty. We state his result without proof: a number  $s + 2$  of check symbols is sufficient for correcting  $s$  asymmetric defects, for  $1 < s < \lfloor n/2 \rfloor - 1$ .

Notice that  $s$  check symbols are clearly necessary. This gives for the optimal dimension of a code correcting  $s$  asymmetric defects

$$n - s - 2 \leq k \leq n - s \text{ for } 1 < s < \lfloor n/2 \rfloor - 1.$$

Let us mention yet another model, introduced by Bassalygo, Gelfand and Pinsker in [55] under the name of “channel with localized errors” (see also the work of Ahlswede, Bassalygo and Pinsker [10]); it could fit in the W\*M model,

under WSM (writing on “suspicious” memories): the writer knows the set of size  $pn$  of suspicious positions, i.e., where an error can occur with probability  $1/2$  when writing. The other positions are error-free. The capacity of such a memory is shown in [55] to be  $1 - H(p)$ .

**§18.8** The error case for W\*Ms is dealt with by van Eijl, Cohen and Zémor in [215].

This Page Intentionally Left Blank

# Chapter 19

## Heterodox coverings

In this chapter we consider a few generalizations of coverings. In Section 19.1, we consider  $L$ -spheres, i.e., we relax the definition of the sphere to allow unions of shells; in Section 19.2, we use spheres of two different radii and in Section 19.3, we restrict all the spheres to be of different radii. In the first two sections we only deal with the perfect case, whereas the third section is devoted to finding optimal coverings. In Section 19.4, we study multicoverings and Section 19.5 deals with a problem related to constant weight coverings.

Most of the issues considered here stem from communication problems (see the notes at the end of the chapter), although they are of evident intrinsic interest.

### 19.1 Perfect coverings by $L$ -spheres

Let  $L$  be a fixed subset of  $[0, n]$ . For  $\mathbf{x} \in \mathbb{F}^n$ , we set

$$L(\mathbf{x}) = \{\mathbf{y} \in \mathbb{F}^n : d(\mathbf{x}, \mathbf{y}) \in L\}.$$

We call  $L(\mathbf{x})$  the  $L$ -sphere around  $\mathbf{x}$  and we say that  $\mathbf{x}$  covers  $\mathbf{y}$  if  $\mathbf{y} \in L(\mathbf{x})$ . Observe that a vector covers itself if and only if  $0 \in L$ . A code  $C \subseteq \mathbb{F}^n$  is called an  $L$ -covering if

$$\bigcup_{\mathbf{c} \in C} L(\mathbf{c}) = \mathbb{F}^n.$$

For  $L$ -coverings, the sphere-covering bound reads — cf. (18.2.13) —

$$|C||L(\mathbf{c})| = |C| \sum_{i \in L} \binom{n}{i} \geq 2^n. \quad (19.1.1)$$

Another lower bound on  $|C|$  is given in Theorem 18.2.14. If equality holds in (19.1.1),  $C$  is called a *perfect  $L$ -covering*. Then the sets  $L(\mathbf{c})$  for  $\mathbf{c} \in C$  form a partition of  $\mathbb{F}^n$  and  $|C| = 2^k$ ,  $|L(\mathbf{c})| = 2^{n-k}$  for some  $k$ . Such a code is denoted by  $\mathcal{L}(n, k, L)$ .

Let us set  $\overline{L} = \{n - \ell : \ell \in L\}$ . We have, for all  $\mathbf{x} \in \mathbb{F}^n$ ,

$$L(\mathbf{x}) = \overline{L}(\overline{\mathbf{x}}). \quad (19.1.2)$$

Moreover,

$$L(\mathbf{x}) \cap L(\overline{\mathbf{x}}) = \emptyset \text{ if and only if } (\ell \in L \text{ implies } n - \ell \notin L). \quad (19.1.3)$$

As for  $\mathbf{c} \in C$  we have  $\mathbf{0} \in \mathbf{c} + C$ , we always assume  $\mathbf{0} \in C$ . Let  $\overline{C} = \{\mathbf{x} \in \mathbb{F}^n : \overline{\mathbf{x}} \in C\}$ ; a code  $C$  such that  $C = \overline{C}$  is called *self-complementary*. If  $C$  is not self-complementary we assume that  $\mathbf{0} \in C$  and  $\mathbf{1} \notin C$  hold. Define

$$L^* = \{\min\{\ell, n - \ell\} : \ell \in L\}.$$

Notice that  $L^* \subseteq [0, \lfloor n/2 \rfloor]$ .

**Lemma 19.1.4** *If  $C = \overline{C}$  is a perfect  $L$ -covering, then  $C$  is a perfect  $L^*$ -covering.*

**Proof.** Use (19.1.2) and (19.1.3). □

For a perfect  $L$ -covering, we have

**Lemma 19.1.5** *There is no triangle in  $\mathbb{F}^n$  with side lengths  $\ell, \ell', d(\mathbf{c}, \mathbf{c}')$ , with  $\ell, \ell'$  in  $L$  and  $\mathbf{c}, \mathbf{c}'$  in  $C$ .*

**Proof.** Otherwise, we would get a triangle  $(\mathbf{c}, \mathbf{c}', \mathbf{x})$ , with  $\mathbf{c}$  and  $\mathbf{c}'$  in  $C$ , i.e.,  $\mathbf{x} \in L(\mathbf{c}) \cap L(\mathbf{c}')$ , a contradiction. □

The following result is proved in Section 2.4 (Lemma 2.4.6).

**Lemma 19.1.6** *In  $\mathbb{F}^n$  there exists a triangle with side lengths  $a, b, c$  if and only if (i), (ii) and (iii) hold.*

(i) *The triangle inequalities are satisfied.*

(ii)  *$a + b + c$  is even.*

(iii)  *$a + b + c \leq 2n$ .* □

As an immediate consequence we deduce the following corollaries for a perfect  $L$ -covering  $C$ .

**Corollary 19.1.7** *If  $\mathbf{c}, \mathbf{c}' \in C$  and  $d(\mathbf{c}, \mathbf{c}') = 2t$  for some positive integer  $t$ , then  $t > \min\{\ell, n - \ell\}$  holds for every  $\ell \in L$ .*  $\square$

**Corollary 19.1.8** *If  $\mathbf{c} \in C \setminus \{\mathbf{0}\}$  and  $w(\mathbf{c})$  is even, then*

$$w(\mathbf{c}) > 2 \max_{\ell \in L} \min\{\ell, n - \ell\}.$$

 $\square$ 

We are now in a position to prove nonexistence results.

**Theorem 19.1.9** *For a perfect  $L$ -covering  $C$  that is not self-complementary, let  $\ell \in L$ ,  $2 \leq \ell \leq n/2$ ; then*

$$\ell - 2 \in L.$$

**Proof.** Suppose the theorem is not true and let  $\ell$  be the smallest integer for which the theorem is violated. Let  $\mathbf{x}$  be a vector of weight  $\ell - 2$  and let  $\mathbf{c}$  be the (nonzero) centre of the (unique)  $L$ -sphere containing  $\mathbf{x}$ , i.e.,  $d(\mathbf{x}, \mathbf{c}) = \ell' \in L$ . As  $\mathbf{0} \in C$ , by Lemma 19.1.5 there is no triangle in  $\mathbb{F}^n$ , with side lengths  $\ell, \ell', w(\mathbf{c})$ . In view of Lemma 19.1.6, one of the conditions (i), (ii), (iii) must be violated. By  $\mathbf{x} \in L(\mathbf{c})$  we know the existence of a triangle with side lengths  $\ell - 2, \ell', w(\mathbf{c})$ . Hence there are only two possibilities:

- a) either  $\ell - 2 = \ell' + w(\mathbf{c})$  and consequently  $(\mathbf{0}, \mathbf{c}, \mathbf{x})$  is a flat triangle;
- b) or  $\ell - 2 + \ell' + w(\mathbf{c}) = 2n$ , i.e.,  $\ell - 2 = (n - \ell') + (n - w(\mathbf{c}))$  and consequently  $(\mathbf{0}, \bar{\mathbf{c}}, \mathbf{x})$  is a flat triangle.

(Note that if  $\ell = 2$ , then  $\mathbf{x} = \mathbf{0}$ ,  $\ell' = w(\mathbf{c})$ , so there must be no triangle with side lengths  $\ell = 2, \ell', w(\mathbf{c}) = \ell'$ . This is possible only if  $\ell + \ell' + w(\mathbf{c}) = 2n + 2$  and we are in case b). If  $\ell' = 0$ , i.e.,  $\mathbf{c} = \mathbf{x}$ , then  $w(\mathbf{c}) = \ell - 2 = \ell - 2 - \ell'$  and we are in case a). Finally  $\ell = 2$  and  $\ell' = 0$  is impossible, since  $\ell$  is assumed to violate the theorem.)

Let  $\mathcal{C}$  be the set of codewords covering all the vectors  $\mathbf{x}$  of weight  $\ell - 2$  in  $\mathbb{F}^n$ ;  $\mathcal{C}$  can be partitioned into three classes  $\mathcal{C}_1 = \{\mathbf{c} \in \mathcal{C} : w(\mathbf{c}) \leq n/2\}$ ,  $\mathcal{C}_e = \{\mathbf{c} \in \mathcal{C} : w(\mathbf{c}) \text{ even, } w(\mathbf{c}) > n/2\}$  and  $\mathcal{C}_o = \{\mathbf{c} \in \mathcal{C} : w(\mathbf{c}) \text{ odd, } w(\mathbf{c}) > n/2\}$ . Then  $\mathcal{C}_1$  corresponds to case a),  $\mathcal{C}_e$  and  $\mathcal{C}_o$  to case b). We assert that each class contains at most one element. Suppose the contrary; then for the corresponding  $\mathbf{c}_1, \mathbf{c}_2$  we have  $d(\mathbf{c}_1, \mathbf{c}_2) = 2t < 2\ell$ , in contradiction with Corollary 19.1.7. Indeed, for the first class,  $w(\mathbf{c}_1) = \ell - 2 - \ell'_1, w(\mathbf{c}_2) = \ell - 2 - \ell'_2$ , so by Corollary 19.1.8,  $w(\mathbf{c}_1)$  and  $w(\mathbf{c}_2)$  are odd. This shows that  $d(\mathbf{c}_1, \mathbf{c}_2)$  is even and  $d(\mathbf{c}_1, \mathbf{c}_2) < 2\ell$ . For  $\mathcal{C}_e$  or  $\mathcal{C}_o$ , we would have  $w(\bar{\mathbf{c}}_1) = \ell + \ell'_1 - 2 - n$ ,  $w(\bar{\mathbf{c}}_2) = \ell + \ell'_2 - 2 - n$ , with the same conclusion for  $\mathbf{c}_1$  and  $\mathbf{c}_2$ .

If  $\mathbf{c} \in \mathcal{C}_1$ , then  $(\mathbf{0}, \mathbf{c}, \mathbf{x})$  is a flat triangle and  $\mathbf{c}$  can cover at most

$$\binom{n - w(\mathbf{c})}{\ell - 2 - w(\mathbf{c})}$$

vectors of weight  $\ell - 2$ . Moreover,  $0 < w(\mathbf{c}) \leq \ell - 2$  and  $w(\mathbf{c})$  is odd by Corollary 19.1.8.

If  $\mathbf{c} \in \mathcal{C}_e$  or  $\mathcal{C}_o$ , then  $(\mathbf{0}, \bar{\mathbf{c}}, \mathbf{x})$  is a flat triangle and  $\mathbf{c}$  can cover at most

$$\binom{n - w(\bar{\mathbf{c}})}{\ell - 2 - w(\bar{\mathbf{c}})}$$

vectors of weight  $\ell - 2$ , with  $0 < w(\bar{\mathbf{c}}) \leq \ell - 2$ . Hence we are led to the following inequality:

$$\binom{n}{\ell - 2} \leq \binom{n - w(\mathbf{c}_1)}{\ell - 2 - w(\mathbf{c}_1)} + \binom{n - w(\bar{\mathbf{c}}_e)}{\ell - 2 - w(\bar{\mathbf{c}}_e)} + \binom{n - w(\bar{\mathbf{c}}_o)}{\ell - 2 - w(\bar{\mathbf{c}}_o)}, \quad (19.1.10)$$

where  $0 < w(\mathbf{c}_1) \leq \ell - 2$  is odd and  $n - (\ell - 2) \leq w(\mathbf{c}_i) < n$ , for  $\mathbf{c}_i = \mathbf{c}_e$  and  $\mathbf{c}_i = \mathbf{c}_o$ .

The right hand side of (19.1.10) is too small unless  $\ell \geq 4$ ,  $w(\mathbf{c}_1) = 1$ ,  $w(\mathbf{c}_2) = n - 1$  for some  $\mathbf{c}_1, \mathbf{c}_2 \in \mathcal{C}$ , in which case  $d(\mathbf{c}_1, \mathbf{c}_2) = n$  or  $n - 2$ ; furthermore, it is easy to check that, for the same reason, none of the three classes  $\mathcal{C}_1, \mathcal{C}_e, \mathcal{C}_o$ , can be empty.

Now this implies that there exists a vector  $\mathbf{x}$  of weight  $\ell - 2$  which has distance  $\ell - 3$  to  $\mathbf{c}_1$ , i.e.,  $\ell - 3 \in L$  and similarly  $n - (\ell - 3) \in L$ ; this leads to a contradiction: a triangle with side lengths  $d(\mathbf{c}_1, \mathbf{c}_2) = n - 2$  or  $n, \ell - 3, n - (\ell - 3)$  cannot exist by Lemma 19.1.5, however it satisfies conditions (i), (ii) and (iii) of Lemma 19.1.6.  $\square$

Note that if  $C = \bar{C}$ , either the unique  $\mathbf{c}$  covering  $\mathbf{x}$  is not  $\mathbf{1}$  and the previous proof carries over *mutatis mutandis*, or  $\mathbf{c} = \mathbf{1}$ , in which case  $\ell' = n - (\ell - 2) \in L$ .

**Corollary 19.1.11** *Let  $C$  be a perfect self-complementary  $L^*$ -covering,  $\ell \in L^*$ ,  $2 \leq \ell$ . Then  $\ell - 2 \in L^*$ .*  $\square$

**Theorem 19.1.12** *For a perfect  $L$ -covering  $C$  that is not self-complementary, let  $\ell \in L$ ,  $n/2 \leq \ell \leq n - 2$ . Then  $\ell + 2 \in L$ .*

**Proof.** If  $C$  is a perfect  $L$ -covering, then  $\bar{C}$  is a perfect  $\bar{L}$ -covering. If  $C$  is not self-complementary, then  $\bar{C}$  is not self-complementary. Hence Theorem 19.1.9 implies Theorem 19.1.12.  $\square$

By the previous two theorems, the set  $L$  for perfect  $L$ -coverings which are not self-complementary is determined by four integers  $-2 \leq a_1, a_2, b_1, b_2 \leq n/2$ , with  $a_1, b_1$  odd,  $a_2, b_2$  even, in the following way:

$$L = \{2s_1 + 1 : 0 < 2s_1 + 1 \leq a_1\} \cup \{2s_2 : 0 \leq 2s_2 \leq a_2\} \cup$$

$$\cup \{n - 2s_3 - 1 : 0 < 2s_3 + 1 \leq b_1\} \cup \{n - 2s_4 : 0 \leq 2s_4 \leq b_2\},$$

which we write  $L = L_1 \cup L_2 \cup L_3 \cup L_4$ . By the previous two corollaries, the same is true for self-complementary codes and  $L^*$ . From now on, we assume rather naturally that  $L \subseteq [0, n/2]$ , i.e.,  $L_3 = L_4 = \emptyset$ . By the previous corollary, for perfect self-complementary  $L^*$ -coverings,  $L^*$  is of the form  $L_1 \cup L_2$ .

**Theorem 19.1.13** *If  $C$  is a perfect  $L$ -covering, with  $L \subseteq [0, n/2]$ ,  $a_1 \geq 1$  and  $a_2 \geq 0$ , then  $|a_1 - a_2| = 1$ , that is,  $L$  is the interval  $[0, \max\{a_1, a_2\}]$ .  $\square$*

In other words, when both  $L_1$  and  $L_2$  are nonempty,  $L(\mathbf{x})$  is the “usual sphere”. We omit the proof (see [148]).

Consequently, the following theorem, which deals with the case when one of the two sets  $L_1$  or  $L_2$  is empty, enables us to classify the perfect  $L$ -coverings, when  $L \subseteq [0, n/2]$ .

**Theorem 19.1.14** *Let  $\epsilon = R - 2\lfloor R/2 \rfloor$ . Then there exists an  $\mathcal{L}(n, k, L = \{0, 1, 2, \dots, R\})$  if and only if there exists an  $\mathcal{L}(n + 1, k + 1, L' = \{R, R - 2, R - 4, \dots, \epsilon\})$ .*

**Proof.** Let  $C$  be an  $\mathcal{L}(n, k, L = \{0, 1, 2, \dots, R\})$ , i.e., a perfect code with covering radius  $R$ . For any distinct  $\mathbf{c}_1$  and  $\mathbf{c}_2$  in  $C$ ,  $d(\mathbf{c}_1, \mathbf{c}_2) \geq 2R + 1$ . Now let  $C' = C \oplus \mathbb{F}$  (cf. Section 3.2). Obviously, for any distinct  $\mathbf{c}'_1$  and  $\mathbf{c}'_2$  in  $C'$ ,  $d(\mathbf{c}'_1, \mathbf{c}'_2)$  equals 1 or is at least  $2R + 1$ . Thus  $L'(\mathbf{c}'_1)$  and  $L'(\mathbf{c}'_2)$  have an empty intersection. Furthermore the sphere-covering equality for  $C$  can be rewritten as

$$2^{k+1} \sum_{i \in L'} \binom{n+1}{i} = 2^{n+1},$$

hence  $C'$  is a perfect  $L'$ -covering.

Conversely, let  $C'$  be an  $\mathcal{L}(n + 1, k + 1, L')$  with  $\epsilon = 0$  (respectively, 1). Then the  $2^n$  even vectors in  $\mathbb{F}^{n+1}$  are covered by the even (respectively, odd) codewords in  $C'$ . Deleting the last component in  $\mathbb{F}^{n+1}$  we get an  $\mathcal{L}(n, k, L)$ .  $\square$

**Corollary 19.1.15** *The only perfect  $L$ -coverings with  $L \subseteq [0, n/2]$  are the classical perfect codes and those with the following parameters:*

$$\mathcal{L}(2R + 2, 2, \{R, R - 2, \dots, R - 2\lfloor R/2 \rfloor\}),$$

$$\mathcal{L}(2^m, 2^m - m, \{1\}),$$

$$\mathcal{L}(24, 13, \{1, 3\}),$$

derived from binary repetition, Hamming and Golay codes, respectively.  $\square$

So, either when  $L$  is included in  $[0, n/2]$  (or, by (19.1.2), in  $[n/2, n]$ ) or when the code is self-complementary, we know all the parameters of perfect  $L$ -coverings (note that for a given self-complementary code, various sets  $L$  are possible).

We now study a case when  $L$  is not included in  $[0, n/2]$ , to give a flavour of methods that can be used (first note that the construction of Theorem 19.1.14 yields an  $\mathcal{L}(n+1, 1, L' = \{n, n-2, \dots, n-2\lfloor n/2 \rfloor\}) = \{0^{n+1}, 0^n 1\}$  obtained from the trivial perfect code  $\{0^n\}$ ).

### The case $L = [0, \ell] \cup \{n\}$

Let us first give an easy existence result.

**Theorem 19.1.16** *For  $m \geq 2$ , there exists an  $\mathcal{L}(2^m-2, 2^m-2-m, \{0, 1, 2^m-2\})$ .*

**Proof.** Shorten a Hamming code of length  $2^m - 1$ . □

On the other hand, as we now prove, for  $\ell = 2$  there is no such perfect code:

**Theorem 19.1.17** *There is no nontrivial  $\mathcal{L}(n, k, \{0, 1, 2, n\})$ .*

**Proof.** The sphere-covering equality would give, setting  $n - k = r$  :

$$n^2 + n - 2(2^r - 2) = 0.$$

The discriminant  $2^{r+3} - 15$  can be a nonzero square only if

$$2^{r+3} \equiv x^2 \pmod{3},$$

which implies  $x^2 \equiv 1 \pmod{3}$ ,  $r+3 = 2\gamma$  and

$$15 = 2^{r+3} - x^2 = (2^\gamma - x)(2^\gamma + x).$$

Solving for  $\gamma$  and  $x$  gives only the trivial  $\mathcal{L}(3, 0, [0, 3])$  code. □

We conclude with a conjecture.

**Conjecture 19.1.18** *Let  $L = L_1 \cup L_2 \cup L_3 \cup L_4$  be the decomposition of  $L$  as before. If  $L_i \neq \emptyset$ , for  $i = 1, 2, 3, 4$ , then  $L_1 \cup L_2$  and  $L_3 \cup L_4$  are intervals containing 0 and  $n$ , respectively.*

Before giving some results in the nonbinary case, we remind the reader that Corollary 18.2.15 states that no perfect  $L$ -covering exists for  $L = [(n-w)/2, (n+w)/2]$ .

## The nonbinary case

Here, the situation is simpler and perfect  $L$ -coverings are classified as follows.

**Theorem 19.1.19** *For  $q > 2$ , the only possible perfect  $L$ -coverings occur for  $L = [0, R]$ , i.e., are the classical ones.*

The proof follows from two easy lemmas (cf. Lemmas 19.1.5 and 19.1.6).

**Lemma 19.1.20** *If  $C$  is a perfect  $L$ -covering, there is no triangle in  $\mathbb{Z}_q^n$  with side lengths  $\ell, \ell', d(\mathbf{c}, \mathbf{c}')$ , with  $\ell, \ell'$  in  $L$  and  $\mathbf{c}, \mathbf{c}'$  in  $C$ .  $\square$*

**Lemma 19.1.21** *In  $\mathbb{Z}_q^n$ ,  $q > 2$ , there exists a triangle with side lengths  $a, b, c$  if and only if the triangle inequalities are satisfied.  $\square$*

**Proof of Theorem 19.1.19** First note that there is no  $\ell$  in  $L$  with  $\ell > n/2$ , because a triangle with side lengths  $\ell, \ell, w(\mathbf{c})$  (with  $\mathbf{c} \in C$ ), possible by Lemma 19.1.21, would violate Lemma 19.1.20; hence  $L \subseteq [0, n/2]$ . Suppose that  $L$  is not an interval  $[0, R]$ . Let  $\mathbf{x}$  be such that  $w(\mathbf{x}) = \min\{i : i \notin L\}$  and  $m = \max\{i : i \in L\}$ . Then  $\mathbf{x} \notin L(0)$  and there is a  $\mathbf{c}$  in  $C$  for which  $\mathbf{x} \in L(\mathbf{c})$ . Now  $w(\mathbf{c}) \leq m + w(\mathbf{x}) < 2m$ , so there is a triangle with side lengths  $m, m, w(\mathbf{c})$  (by Lemma 19.1.21), which is impossible, by Lemma 19.1.20.  $\square$

## 19.2 Perfect coverings by spheres of two radii

Let us consider another generalization of perfect codes, where the spheres have different radii. Let  $C = \cup_{1 \leq i \leq p} C_i \subseteq \mathbb{F}^n$ , with  $|C_i| = K_i$ , and let  $R_1, \dots, R_p$  be  $p$  distinct integers between 1 and  $n$ . If the  $p$  sets  $\cup_{\mathbf{c} \in C_i} B_{R_i}(\mathbf{c})$  partition  $\mathbb{F}^n$ , this partition is denoted by  $P(n, \{R_i\}, \{K_i\})$  and  $C$  is called a *perfect p-radius code*. In what follows we consider the case  $p = 2$ , except for the last two lines of the section, and give a few sporadic examples of perfect codes with two radii.

**Theorem 19.2.1** *For any even  $m, m \geq 4$ , there exists a*

$$P(2^m, \{2, 1\}, \{2^{2^m-2m}, 2^{2^m-m-1} - 2^{2^m-2m}\}).$$

**Proof.** For  $m$  even,  $m \geq 4$ , there exists a punctured Preparata code  $\mathcal{P}_m^*$  with parameters  $(2^m-1, 2^{2^m-2m}, 5)3$ , which is a subcode of the  $[2^m-1, 2^m-m-1, 3]$  Hamming code  $\mathcal{H}_m$  (cf. Theorem 2.6.5). Furthermore,

$$d(\mathbf{x}, \mathcal{P}_m^*) = 3 \text{ if and only if } \mathbf{x} \in \mathcal{H}_m \setminus \mathcal{P}_m^*,$$

since

$$|\mathcal{P}_m^*| \cdot V(2^m - 1, 2) + |\mathcal{H}_m| - |\mathcal{P}_m^*| = 2^{2^m - 1}.$$

Setting  $C_2 = \mathcal{P}_m^* \oplus \{0\}$ ,  $R_2 = 2$ ,  $C_1 = (\mathcal{H}_m \setminus \mathcal{P}_m^*) \oplus \{1\}$ ,  $R_1 = 1$ , it is again easily checked by counting that we obtain a partition of  $\mathbb{F}^{2^m}$  with the announced parameters.  $\square$

**Theorem 19.2.2** *There exists a  $P(15, \{3, 1\}, \{32, 896\})$ .*

**Proof.** Take for  $C_1$  the  $[15, 5, 7]5$  punctured Reed-Muller code  $\mathcal{RM}^*(1, 4)$  with  $R_1 = 3$ . There are  $28 \cdot 2^5$  vectors at distance 5 from  $\mathcal{RM}^*(1, 4)$ , the so-called “bent” functions (see Notes on Section 9.2), and they form a  $(15, 896, 3)$  code  $C_2$ . Set  $R_2 = 1$  and conclude by noticing that

$$2^5 \sum_{i=0}^3 \binom{15}{i} + 28 \cdot 2^5 \sum_{i=0}^1 \binom{15}{i} = 2^{15}.$$

$\square$

**Theorem 19.2.3** *There exists a  $P(11, \{3, 1\}, \{2, 132\})$ .*

**Proof.** There exists a Steiner system  $S(4, 5, 11)$  (see Example 3.3.3 where it is used to prove that  $K(11, 1) \leq 192$ ). Together with its complement  $\overline{S}$ , this gives an  $(11, 132, 3)$  code  $C_1$  with the property that for all  $\mathbf{x} \in \mathbb{F}^{11}$  such that  $4 \leq w(\mathbf{x}) \leq 7$ , there exists a unique codeword  $\mathbf{c} \in C_1$  with  $d(\mathbf{x}, \mathbf{c}) \leq 1$ . Take  $C_2 = \{0^{11}, 1^{11}\}$ ,  $R_2 = 3$  to obtain the existence of  $P(11, \{3, 1\}, \{2, 132\})$ .  $\square$

**Theorem 19.2.4** *For  $s > 4$ , a  $P(2s+3, \{s-1, 1\}, \{K_1, K_2\})$  exists only if  $K_1 = 2$ ,  $K_2 = 2 \binom{2s+3}{s} / (s+1)$ .*

**Proof.** Suppose there exists a  $P(2s+3, \{s-1, 1\}, \{K_1, K_2\})$ . One can always centre a sphere of radius  $s-1$  at  $\mathbf{0}$ . Suppose  $K_1 \geq 3$ . Then there would be at least two other spheres  $B_{s-1}(\mathbf{x})$  and  $B_{s-1}(\mathbf{y})$ . Now  $B_{s-1}(\mathbf{0}) \cap B_{s-1}(\mathbf{x}) = \emptyset$ ,  $B_{s-1}(\mathbf{0}) \cap B_{s-1}(\mathbf{y}) = \emptyset$ , implies  $w(\mathbf{x}) \geq 2s-1$ ,  $w(\mathbf{y}) \geq 2s-1$ . For  $s > 4$ ,  $B_{s-1}(\mathbf{x})$  and  $B_{s-1}(\mathbf{y})$  would intersect in  $\mathbf{1}$ , the all-one vector of length  $2s+3$ , which is impossible. Hence  $K_1 \leq 2$ . Suppose now  $K_1 = 1$ , so the only sphere of radius  $s-1$  is centred at  $\mathbf{0}$ . Call  $\mathcal{A}_i$  the number of spheres whose centres have weight  $i$ . Elements of weight  $s$  in  $\mathbb{F}^{2s+3}$  are contained in spheres with centres of weight  $s+1$ . Every such sphere contains  $s+1$  elements of weight  $s$ , so  $\mathcal{A}_{s+1} = \binom{2s+3}{s} / (s+1)$ . The same method then shows that  $\mathcal{A}_{s+2} = \mathcal{A}_{s+1}$ ,  $\mathcal{A}_{s+3} = \mathcal{A}_{s+4} = 0$ .

Now spheres with centres of weight  $s + 5$  must contain all elements of weight  $s + 4$  and at most the total number of elements of weight  $s + 6$ , hence

$$A_{s+5} = \binom{2s+3}{s-1} / (s+5)$$

and

$$A_{s+5} \leq \binom{2s+3}{s-3} / (s-2) = \frac{s-1}{s+6} \binom{2s+3}{s-1} / (s+5),$$

a contradiction. Finally  $K_1 = 2$ . Now the sphere-covering equality

$$K_1 V(2s+3, s-1) + K_2 V(2s+3, 1) = 2^{2s+3}$$

gives  $K_2 = 2 \binom{2s+3}{s} / (s+1)$ .  $\square$

Puncturing sometimes allows to obtain new perfect codes from existing ones. Let us mention the following constructions:

**Theorem 19.2.5** *Let  $P(n, \{R_1, R_2\}, \{K_1, K_2\})$  be such that*

$$K_1 \binom{n-1}{R_1} = K_2 \binom{n-1}{R_2};$$

*if moreover any two adjacent spheres of the same radius have the same  $i$ -th component, then puncturing on the  $i$ -th position yields two perfect 2-radius codes:*

$$P(n-1, \{R_1-1, R_2\}, \{K_1, K_2\}),$$

$$P(n-1, \{R_1, R_2-1\}, \{K_1, K_2\})$$

*(two spheres of radius  $R_j$  are adjacent if the distance between their centres is  $2R_j + 1$ ).*

**Proof.** Straightforward.  $\square$

**Example 19.2.6** Viewing the Golay code as a  $P(23, \{3, 3\}, \{2^{11}, 2^{11}\})$  gives rise to a  $P(22, \{3, 2\}, \{2^{11}, 2^{11}\})$ . In fact a further puncturing gives a perfect 3-radius code  $P(21, \{3, 2, 1\}, \{2^{10}, 2^{11}, 2^{10}\})$ .  $\square$

### 19.3 Coverings by spheres all of different radii

In this section we consider the problem of coverings by spheres when no two equal radii are allowed. Namely, we allow the occurrence in a covering of at most one sphere of each of the radii  $1, 2, \dots, n$ . The problem is to find a covering minimizing the maximum radius of a sphere used in the covering. Evidently, one sphere of radius  $n$  is enough to cover all the space. As well, two spheres of radii  $\lceil n/2 \rceil - 1$  and  $\lceil n/2 \rceil$  centred at two complementary vectors suffice. Thus, an evident upperbound on the maximum radius of a sphere involved in the covering is  $\lceil n/2 \rceil$ . Surprisingly enough we cannot do better.

Let us rephrase the problem more precisely. Let  $I = \{R_1, \dots, R_m\}$ ,  $R_1 < R_2 < \dots < R_m$ , be a subset of  $\{1, \dots, n\}$ ,  $m \leq n$  and  $C = \{c_1, \dots, c_m\}$ , be a collection of centres. Assume that

$$\bigcup_{j=1}^m B_{R_j}(c_j) = \mathbb{F}^n.$$

Given  $n$  we want to construct a covering  $C$  with minimal  $R_m$ . The minimum of  $R_m$  over all possible  $C$  is denoted by  $\rho(n)$ .

**Lemma 19.3.1** *Let  $\mathbf{A} = (\mathbf{a}_i) = (a_{i,j})$ ,  $i = 1, \dots, n$ ,  $j = 1, \dots, n$ , be a matrix with entries  $\pm 1$ . Then there exists a  $\pm 1$ -vector  $\mathbf{y}^\pm = (y_j^\pm)$  such that*

$$\left| \sum_{1 \leq j \leq n} y_j^\pm a_{i,j} \right| < 2i$$

for  $i = 1, \dots, n$ .

**Proof.** For each  $i$ , consider the homogenous system of  $n$  equations  $z_i = \sum_{j=1}^n a_{i,j} x_j$  in the  $n$  real variables  $x_1, \dots, x_n$ .

Set  $\mathbf{x} = (x_1, \dots, x_n)$  and  $\mathbf{y} = (y_1, \dots, y_n)$ , where the  $y_i$ 's belong to  $\{-1, 0, +1\}$ . A trivial solution to  $\mathbf{A}\mathbf{x}^T = 0^n$  is  $\mathbf{y} = 0^n$ . At step one, relax, say, the last equation: delete the last row of  $\mathbf{A}$  and denote by  $\mathbf{A}_1$  the resulting matrix; then the set of solutions to  $\mathbf{A}_1\mathbf{x}^T = 0^{n-1}$  is a vector space of dimension at least one, thus containing a line through the origin. This line hits the real cube  $[-1, 1]^n$  on a face; after possible reordering, we can assume that it is the  $n$ -th face, of equation  $x_n$  equal to, say,  $-1$ . Set  $\mathbf{y} = (0^{n-1}, -1)$  and repeat this procedure  $n-1$  times. That is, before step  $t+1$ ,  $\mathbf{y} = (0^{n-t} | y_{n-t+1}, \dots, y_n)$  where  $y_{n-t+1}, \dots, y_n$  are  $t \pm 1$  elements determined by the previous moves; at step  $t+1$ , relax the  $(n-t)$ -th equation, determine the space of solutions to the system of  $n-t-1$  equations in  $n-t$  unknowns, find a face where it intersects the cube  $[-1, 1]^{n-t}$ . This fixes a new component of  $\mathbf{y}$ , say  $y_{n-t}$ , and defines  $\mathbf{y} = (0^{n-t-1} | y_{n-t}, \dots, y_n)$ . Denote the final  $\pm 1$  result, obtained after step  $n$ , by  $\mathbf{y}^\pm$  and consider the sum  $\sum_{1 \leq j \leq n} y_j^\pm a_{i,j}$ . From the description of the

process, this sum remains 0 until we reach step  $n - i + 1$ . During step  $n - i + 1$ , the absolute value of this sum increases by at most one, and by at most two during the  $i - 1$  remaining steps. So  $|\sum_{1 \leq j \leq n} y_j^\pm a_{i,j}| \leq 1 + 2(i - 1) < 2i$ .  $\square$

Now we are in position to prove

**Theorem 19.3.2**

$$\rho(n) = \lceil n/2 \rceil.$$

**Proof.** Assume the contrary, i.e., that we have a covering  $C = \{c_1, \dots, c_m\}$ , with  $R_m \leq \lceil n/2 \rceil - 1$ . Without loss of generality, we can assume that  $R_1 = 1$ ,  $R_2 = 2, \dots, R_m = m$ , with  $m = \lceil n/2 \rceil - 1$ . Let  $c^\pm$  be the vector obtained from  $c$  by changing 0's to 1's and 1's to  $-1$ 's, and let  $\bar{c}$  be the complement of  $c$ . Construct a matrix  $A$  having as first rows the words  $c_{m-1}^\pm, \dots, c_1^\pm$ , the remaining rows being arbitrary. By Lemma 19.3.1, there is a  $\pm 1$ -vector  $y^\pm$  such that

$$\left| \sum_{1 \leq j \leq n} y_j^\pm c_{i,j}^\pm \right| < 2m - 2i,$$

$i = 1, \dots, m - 1$ . Since  $\sum_{1 \leq j \leq n} y_j^\pm c_{i,j}^\pm = n - 2d(c_i, y)$  and  $d(c_i, y) = n - d(c_i, \bar{y})$ , there exists a binary vector  $y$  such that  $d(c_i, y) > n/2 - m + i$  and  $d(c_i, \bar{y}) > n/2 - m + i$ . Since  $n/2 - m + i \geq i = R_i$ , neither  $y$  nor  $\bar{y}$  belong to  $B_{R_i}(c_i)$ , for  $i = 1, \dots, m - 1$ .

Evidently, one of the two distances  $d(c_m, y)$  or  $d(c_m, \bar{y})$  is strictly greater than  $\lceil n/2 \rceil - 1$ . Let it be  $d(c, \bar{y})$ : this means that  $\bar{y}$  is not covered by  $C$ .

On the other hand,  $B_{\lceil n/2 \rceil}(\mathbf{0})$  and  $B_{\lceil n/2 \rceil - 1}(\mathbf{1})$  provide such a covering.  $\square$

This problem has an application to broadcasting in the  $n$ -dimensional cube. Let  $2^n$  processors be connected as in the  $n$ -dimensional cube, i.e., each processor is assigned a different binary  $n$ -tuple and two processors are connected if the corresponding binary vectors are at Hamming distance one. Now, to broadcast a message in the  $n$ -cube, it is allowed at each round to provide it to exactly one of the processors; in parallel, a processor that already received the message sends it to its neighbours. Thus, after the first round, one processor, say  $p_1$ , knows the message; after the second round,  $p_1$ , its neighbours and some other processor  $p_2$  know the message, and so on. The question is: how many rounds are needed to deliver the message to all processors? Theorem 19.3.2 gives the answer, namely  $\lceil n/2 \rceil + 1$ , and the strategy is very easy: just send the message to two antipodal nodes during the first two rounds and after this, ... relax.

## 19.4 Multicovering radius

In this section we study codes with the property that for every  $s$ -tuple of vectors in the Hamming space there is a codeword which is close to *all* of them. This leads to the concept of *multicovering radius*.

**Definition 19.4.1** *Let  $s \geq 1$  be fixed. The multicovering radius of a code  $C \subseteq \mathbb{F}^n$  is the smallest integer  $R_s = R_s(C)$  such that for every  $s$ -tuple  $(\mathbf{x}_1, \mathbf{x}_2, \dots, \mathbf{x}_s)$ , where  $\mathbf{x}_1, \mathbf{x}_2, \dots, \mathbf{x}_s \in \mathbb{F}^n$ , there is a codeword  $\mathbf{c} \in C$  such that  $d(\mathbf{c}, \mathbf{x}_i) \leq R_s$  for all  $i = 1, 2, \dots, s$ .*

When  $s = 1$ , the definition of course reduces to that of covering radius.

**Theorem 19.4.2** *If  $C$  is an  $(n, K)$  code, then  $R_s(C) \geq n - t(n, s)$ .*

**Proof.** Recall that  $t(n, s)$  is the smallest covering radius among all  $(n, s)$  codes. Take as the vectors  $\mathbf{x}_1, \mathbf{x}_2, \dots, \mathbf{x}_s$  the codewords of a binary code of length  $n$  with covering radius  $t(n, s)$ . If  $\mathbf{y} \in \mathbb{F}^n$ , then  $\bar{\mathbf{y}}$  is within distance  $t(n, s)$  from at least one of these  $s$  vectors, say  $\mathbf{x}_i$ , and therefore  $d(\mathbf{y}, \mathbf{x}_i) \geq n - t(n, s)$ . In particular, any codeword in  $C$  is at distance at least  $n - t(n, s)$  from at least one  $\mathbf{x}_j$ .  $\square$

**Corollary 19.4.3** *If  $s \geq 2$ , then the multicovering radius  $R_s$  of any code of length  $n$  is at least  $\lceil n/2 \rceil$ .*  $\square$

The following theorem shows that determining  $R_s(\mathbb{F}^n)$  for all  $s$  and  $n$  is equivalent to determining the values of  $K(n, R)$  for all  $n$  and  $R$ .

**Theorem 19.4.4** *The quantity  $R_s(\mathbb{F}^n)$  equals the smallest integer  $t$  such that  $K(n, n - t - 1) > s$ .*

**Proof.** We see that  $R_s(\mathbb{F}^n) \leq t$  if and only if for every  $s$ -tuple of vectors, say  $\mathbf{x}_1, \mathbf{x}_2, \dots, \mathbf{x}_s$ , there is a point  $\mathbf{c} \in \mathbb{F}^n$  such that  $d(\mathbf{x}_i, \mathbf{c}) \leq t$  for all  $i$ ; or equivalently that for every  $s$  vectors  $\mathbf{x}_1, \dots, \mathbf{x}_s$  there is a vector  $\mathbf{c} \in \mathbb{F}^n$  such that  $d(\mathbf{x}_i, \bar{\mathbf{c}}) \geq n - t$ . But this is equivalent to saying that  $K(n, n - t - 1) > s$ .  $\square$

Determining  $R_s(\mathbb{F}^n)$  is an essential problem also from the point of view of studying the multicovering radius of other codes as can be seen from the following immediate result.

**Theorem 19.4.5** For every code  $C$ ,  $R_s(\mathbb{F}^n) \leq R_s(C) \leq R_s(\mathbb{F}^n) + R(C)$ .  $\square$

**Theorem 19.4.6**  $R_2(\mathcal{H}_m) = 2^{m-1}$ .

**Proof.** Let  $n = 2^m - 1$ . By Corollary 19.4.3,  $R_2(\mathcal{H}_m) \geq \lceil n/2 \rceil = 2^{m-1}$ . It remains to show that  $R_2(\mathcal{H}_m) \leq (n+1)/2$ .

Let  $\mathbf{x}, \mathbf{y} \in \mathbb{F}^n$  be arbitrary. If  $d(\mathbf{x}, \mathbf{y}) \leq n-1$ , then let  $\mathbf{z} \in \mathbb{F}^n$  be any vector such that  $d(\mathbf{z}, \mathbf{x}) \leq (n-1)/2$  and  $d(\mathbf{z}, \mathbf{y}) \leq (n-1)/2$ . Because  $\mathcal{H}_m$  has covering radius one, there is a codeword  $\mathbf{c} \in \mathcal{H}_m$  such that  $d(\mathbf{c}, \mathbf{z}) \leq 1$ . Then  $d(\mathbf{c}, \mathbf{x}) \leq (n+1)/2$  and  $d(\mathbf{c}, \mathbf{y}) \leq (n+1)/2$ .

Second, assume that  $d(\mathbf{x}, \mathbf{y}) = n$ , i.e.,  $\mathbf{y} = \bar{\mathbf{x}}$ , and show that there is a codeword  $\mathbf{c} \in \mathcal{H}_m$  such that  $d(\mathbf{x}, \mathbf{c}) \in \{(n-1)/2, (n+1)/2\}$ . Then also  $d(\mathbf{y}, \mathbf{c}) = n - d(\mathbf{x}, \mathbf{c}) \in \{(n-1)/2, (n+1)/2\}$ . Let  $\mathbf{H}$  be a parity check matrix of  $\mathcal{H}_m$  and denote  $\mathbf{s} = \mathbf{H}\mathbf{x}^T$ . It is sufficient to show that there is a vector  $\mathbf{u} \in \mathbb{F}^n$  of weight  $(n-1)/2$  or  $(n+1)/2$  such that  $\mathbf{H}\mathbf{u}^T = \mathbf{s}$ , because then  $\mathbf{x} + \mathbf{u} \in C$ . Take

$$\mathbf{H} = \left( \begin{array}{cccc|cccc} 0 & 0 & \dots & 0 & 1 & 1 & 1 & \dots & 1 \\ \mathbf{v}_1 & \mathbf{v}_2 & \dots & \mathbf{v}_{(n-1)/2} & \mathbf{0} & \mathbf{v}_1 & \mathbf{v}_2 & \dots & \mathbf{v}_{(n-1)/2} \end{array} \right)$$

where the vectors  $\mathbf{v}_i$  run through all the nonzero binary  $(m-1)$ -tuples. Clearly, the columns on the left hand side add up to  $\mathbf{0}$ , and the same is true for the right hand side. If the column  $\mathbf{s}$  occurs on the right hand side, then all the columns on the right hand side except  $\mathbf{s}$  add up to  $\mathbf{s}$ , and we are done. If  $\mathbf{s}$  appears on the left hand side, then all the columns on the left hand side except  $\mathbf{s}$  add up to  $\mathbf{s}$ , but now there are just  $(n-3)/2$  columns, so we have to replace one of them, say  $(0, \mathbf{v}_i)^T$ , by the two columns  $(1, \mathbf{v}_i)^T$  and  $(1, \mathbf{0})^T$  from the right hand side, and we are done.  $\square$

## 19.5 Perfect coverings of a sphere and constant weight coverings

Consider now the sphere  $B_r(\mathbf{0})$  of radius  $r$  centred at  $\mathbf{0}$  in  $\mathbb{F}^n$ . We search for the minimum number of spheres necessary to partition  $B_r(\mathbf{0})$  into smaller spheres. In other words, we are looking for the minimum number of elements  $\mathbf{c}_i \in B_r(\mathbf{0})$  which cover  $B_r(\mathbf{0})$ , where each  $\mathbf{c}_i$  covers the sphere  $B_{r_i}(\mathbf{c}_i)$  ( $r_i \leq r - w(\mathbf{c}_i)$ ).

Consider  $S_r(\mathbf{0})$ , the surface of  $B_r(\mathbf{0})$ . Then a partition of  $B_r(\mathbf{0})$  contains a covering  $C$  of  $S_r(\mathbf{0})$ , whose elements are the centres of the spheres tangent

to  $S_r(\mathbf{0})$ . Let  $C_w$  be the set of elements of  $C$  of weight  $w$ ,  $r \geq w > 0$ . Then  $C_w$  is a constant weight code and, unless it has only one element, its minimum distance  $d$  is even, with  $d/2 \geq r - w + 1$  (note also that  $2w \geq d$ , i.e.,  $w \geq (r + 1)/2$ ). Using the notation of Section 2.7, we see that  $|C_w| \geq K(n, w, r, r - w)$ . On the other hand, by Lemma 12.6.8,

$$|C_w| \leq \frac{n}{w} \left( \frac{n-1}{w-1} \cdots \left( \frac{n-w+d/2}{d/2} \right) \cdots \right). \quad (19.5.1)$$

Since  $C_w$  covers  $A_w$  points of  $S_r(\mathbf{0})$ , where

$$A_w = \binom{n-w}{r-w} |C_w|,$$

inequality (19.5.1) implies that

$$\frac{A_w}{\binom{n}{r}} \leq \frac{r(r-1)\dots(r-(r-w)+1)}{(n-2w+r)\dots(n-2w+r-(r-w)+1)}.$$

Asymptotically, for  $r$  fixed:  $A_w = O(n^w)$ . That is,  $A_w = O(n^{r-1})$  for  $w = r - 1$  and  $A_w = O(n^{r-2})$  for  $0 < w < r - 1$ . So  $\sum_{i=1}^{r-1} A_i = O(n^{r-1})$  and there are  $\Omega(n^r)$  isolated points (spheres of radius zero) in  $S_r(\mathbf{0}) \cap C$ .

Non-asymptotically, supposing that  $r \leq n/3$ :

$$\frac{A_w}{\binom{n}{r}} \leq \mu^{r-w},$$

where  $\mu = r/(n-r)$ . The sum of the above for  $0 < w < r$  is at most  $\mu/(1-\mu)$ . So the proportion of isolated points in a covering of  $S_r(\mathbf{0})$  is at least

$$\frac{1-2\mu}{1-\mu} = \frac{n-3r}{n-2r}.$$

In other words,  $C$  contains at least

$$\binom{n}{r} \frac{n-3r}{n-2r}$$

isolated points.

Loosely speaking: If you want to partition a sphere into smaller ones, you have to take a lot of spheres of radius 0 (isolated points). The nontrivial ones cover only a negligible amount of the total volume. Notice that this problem is related to that of perfect  $p$ -radius codes dealt with in Section 19.2: namely, by adding the sphere  $B_{n-r-1}(1)$  to a perfect covering of  $B_r(\mathbf{0})$ , we get a perfect covering of  $\mathbb{F}^n$  by spheres with different radii.

The following classical theorem in graph theory now solves the problem of covering  $S_3$  with elements of  $S_2$ .

**Theorem 19.5.2** *If the graph  $G$  has  $n$  vertices and  $m$  edges, where  $m > n^2/4$ , then  $G$  contains a triangle.*

**Proof.** Let  $G = (V, E)$  be a graph with no triangle, and let  $d(u)$  denote the degree (i.e., the number of adjacent vertices) of a vertex  $u \in V$ . Then two adjacent vertices have disjoint sets of neighbours, and  $d(u) + d(v) \leq n$  for every edge  $\{u, v\} \in E$ . Trivially  $\sum_{v \in V} d(v) = 2m$  and therefore summing over all edges, we get

$$mn \geq \sum_{\{u, v\} \in E} (d(u) + d(v)) = \sum_{v \in V} d(v)^2 \geq \frac{1}{n} \left( \sum_{v \in V} d(v) \right)^2 = \frac{4m^2}{n},$$

proving our claim.  $\square$

On the other hand, a bipartite graph  $G = (V, E)$  with  $V = V_1 \cup V_2$ ,  $|V_1| = \lfloor |V|/2 \rfloor$ ,  $|V_2| = \lceil |V|/2 \rceil$  and  $E = V_1 \times V_2$  shows that there exist graphs with  $n$  vertices,  $\lfloor n/2 \rfloor \lceil n/2 \rceil$  edges and no triangle.

Now let  $C \subseteq S_2$  be a 1-covering of  $S_3$  in  $\mathbb{F}^n$ . We consider the graph  $G(C) = (V, E)$  with  $V = \{1, 2, \dots, n\}$  and  $E = \{\{i, j\} : \mathbf{e}_i + \mathbf{e}_j \in C\}$ . This graph has the following property:  $G(C)$  contains at least one edge of any triangle  $T$  in the complete graph on  $V$ . Indeed, otherwise the element of  $S_3$  corresponding to  $T$  would not be covered by  $C$ . In other words, the complementary graph of  $G(C)$  is triangle-free, i.e., contains at most  $n^2/4$  edges by Theorem 19.5.2. Hence  $C$  has size at least  $\binom{n}{2} - n^2/4$  and this lower bound can be achieved:

**Corollary 19.5.3** *For all  $n$ ,  $K(n, 2, 3, 1) = \lceil \frac{n(n-2)}{4} \rceil$ .*  $\square$

More generally,

**Theorem 19.5.4** *If  $n = t(r-1) + r_0$  with  $0 \leq r_0 < r-1$ ,  $r > 2$ , then  $K(n, 2, r, r-2) = (r-1)\binom{t}{2} + tr_0$ .*  $\square$

## 19.6 Notes

§19.1 *L*-packings were introduced by Karpovsky [363], where their practical significance – correction or detection of physical failures in networks – is described. In [363] some perfect *L*-codes are given, as well as an analogue of Lloyd’s theorem (cf. Theorem 11.2.1). See also Deza, Karpovsky and Milman [199].

Corollaries 19.1.7, 19.1.8 and 19.1.15, Theorems 19.1.9, 19.1.12, 19.1.13 and 19.1.14 are by Cohen and Frankl [148]. Theorem 19.1.16 is due to Karlovsky [363]. Theorem 19.1.17 is by Laurent (unpublished).

Reliquet (unpublished) has used methods similar to those of Cohen and Frankl [148] to rule out the existence of nontrivial  $\mathcal{L}(n, k, L)$  for  $L = [0, 2t + 1] \cup \{n\}$  and  $L = \{1, 3, 5, \dots, 2t + 1, n\}$  when  $3 \leq 2t + 1 \leq n/2$ .

Using earlier results proved by Laurent (unpublished), we get that nontrivial perfect  $L$ -coverings with  $L = [0, \ell] \cup \{n\}$  can only exist if  $\ell = 1$  or  $\ell \geq 6$ .

The nonbinary case is treated by Cohen and Frankl [149].

§19.2 Applications of perfect  $p$ -radius codes to source coding and unequal protection of messages are described by Montaron and Cohen [495].

Theorems 19.2.1, 19.2.2, 19.2.3 and 19.2.5 as well as Example 19.2.6 are by Cohen and Montaron [167] [495]. Theorem 19.2.4 is due to Cohen and Frankl [150].

More can be said about Theorem 19.2.1; first, another construction, with the same parameters as, but nonisomorphic to, that of Theorem 19.2.1, was obtained by van den Akker, Koolen and Vaessens [13], by letting  $C_2 = \mathcal{P}_m$ ,  $R_2 = 2$ ,  $C_1 = \widehat{\mathcal{H}}_m \setminus \mathcal{P}_m$ ,  $R_1 = 1$ , where  $\widehat{\cdot}$  denotes extension.

Now let us call two codewords  $\mathbf{c} \in C_i$ ,  $\mathbf{c}' \in C_j$  adjacent if  $d(\mathbf{c}, \mathbf{c}') = R_i + R_j + 1$ . Then to a code  $C$  one can associate in an obvious way a graph  $\Gamma(C)$  whose set of vertices is  $C$ ,  $C$  being called bipartite if  $\Gamma(C)$  is, with  $C_1$  and  $C_2$  being independent sets (i.e., there are no edges within  $C_1$  and  $C_2$ ). For example, the code  $C = (\widehat{\mathcal{H}}_m \setminus \mathcal{P}_m) \cup \mathcal{P}_m$  is bipartite, since  $d(\mathbf{c}, \mathbf{c}') \geq 6$ , (respectively, 4) if  $\mathbf{c}, \mathbf{c}' \in C_2$  (respectively,  $C_1$ ). But the code of Theorem 19.2.1 is not bipartite.

Based on the fact that a nearly perfect code which is not perfect and has covering radius at least 3, has the same parameters as a punctured Preparata code (see Theorem 11.6.3), it is proved in [13] that a bipartite 2-radius  $(R, 1)$ -perfect code with  $R \geq 2$  necessarily has parameters given by Theorem 19.2.1.

On this topic, see also Zinoviev and Katsman [711].

§19.3. Lemma 19.3.1 is due to Beck and Spencer [63]. Its use for finding the best strategy for transmitting in the  $n$ -cube is by Alon [15].

§19.4 The problem discussed in this section is due to Klapper [377] and arose from investigations concerning the cryptanalysis of stream ciphers [376]. Corollary 19.4.3 and Theorem 19.4.6 are from [377], where a more detailed discussion about the multicovering radius and, e.g., its behaviour in various constructions, can be found.

§19.5 Theorem 19.5.2 is due to Mantel [468]. A result by Turán [656] settles the more general case of covering  $S_r$  with a subset of  $S_2$ . On the

subject of perfectly covering a sphere, see Fachini and Körner [227] for a proof that no sphere can be partitioned into two spheres, i.e., there is no perfect code in  $\mathbb{F}^n$  with three spheres of any, not necessarily equal, radii.

See Etzion, Wei and Zhang [226] for a survey on constant weight coverings.

This Page Intentionally Left Blank

# Chapter 20

## Complexity

Several works deal with complexity issues related to error-correcting codes (problem of linear decoding, with or without preprocessing, problem of computing the minimum distance of a linear code, ...), mainly from an NP-completeness viewpoint, that is, a worst-case approach.

In the first two sections of this chapter, we also use the framework of the theory of NP-completeness, for covering problems, and determine the complexity of upperbounding the covering radius of a given binary code, linear or not. We first give in Section 20.1 the necessary background concerning the polynomial hierarchy, by describing different classes of complexity. Then in Section 20.2 we show that computing an upper bound on the covering radius of a nonlinear code is co-NP-complete and that the same problem for linear codes is  $\Pi_2$ -complete. This means that it is unlikely that there are polynomial-time algorithms that solve these problems for all instances.

What can be done when facing an NP-complete (or worse) problem? One can use heuristics (see Section 3.8), approximations, ... or a brute-force attack. If only an existential result is required, then random methods often work. Recently a promising method has emerged: derandomization. The idea, roughly speaking, is to perform an exhaustive search on a suitably chosen small subset of the original set of possible solutions. We illustrate the method in Section 20.3 on a problem akin to classical covering, namely that of covering by union of subcubes.

### 20.1 Basic facts about the polynomial hierarchy

Our intention here is to give an intuitive approach of the notion of *completeness* in the *polynomial hierarchy*.

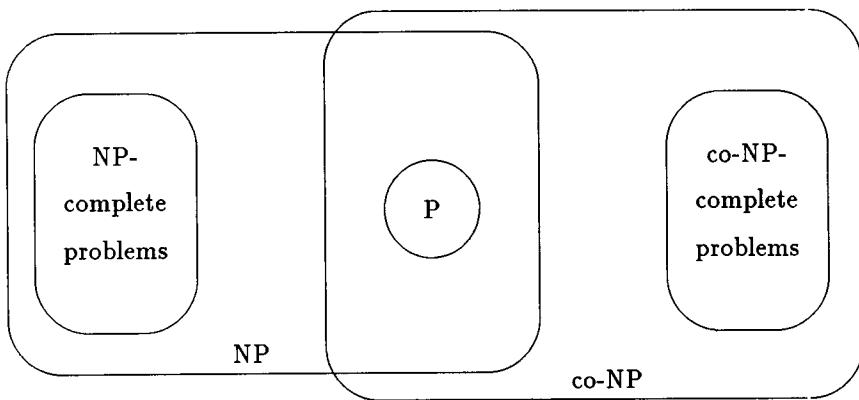
We deal only with *decision problems*, that is, problems consisting of a question whose answer is either YES or NO. An algorithm  $A$  solves a problem  $\pi$  if, applied to any instance  $I$  of  $\pi$ , it gives the correct answer to that instance  $I$ . An estimation of the *size* of an instance  $I$  of  $\pi$  is given by any “reasonable” encoding of  $I$  (for instance, a reasonable encoding of an integer  $m$  requires  $\log m$  bits). The *time complexity function* of an algorithm  $A$  that solves  $\pi$  is, for each possible instance size, the *maximal* time required by  $A$  to solve an instance of that size. A *polynomial-time* algorithm is one whose time complexity function can be bounded by a polynomial  $p(n)$ , where  $n$  is the size of the instance we consider. The class of polynomial-time solvable problems is denoted by  $P$ .

A *polynomial reduction* from a problem  $\pi_1$  to another problem  $\pi_2$  is a polynomial constructive transformation that maps any instance of  $\pi_1$  into an equivalent instance of  $\pi_2$  (the answer is the same for both instances): thus, such a transformation provides the means for converting any polynomial-time algorithm that solves  $\pi_2$  into a corresponding polynomial-time algorithm for solving  $\pi_1$ .

Next, we introduce the class  $NP$ : a decision problem belongs to  $NP$  if it can be solved by a *polynomial-time nondeterministic algorithm*, i.e., an algorithm consisting of two stages: a *guessing stage* and a polynomial-time *checking stage*. The first stage provides some structure  $s$ . The second stage proceeds in a deterministic way and correctly answers YES or NO. For example, consider the well-known Travelling Salesman (TS) problem, for which the instance is a set of cities, the set of integer distances between the cities and an upper bound  $B$ , and the question is whether there exists a Hamiltonian cycle with length at most  $B$ ; the guessing stage provides a sequence  $s$  of the cities and the checking stage checks in polynomial time if  $s$  is a Hamiltonian cycle of length no more than  $B$  or not.

For a set  $S$  of problems, let  $co-S$  be the set of problems that are complementary to those in  $S$  (i.e., their answers are reversed). We have  $P = co-P \subseteq NP \cap co-NP$ , but membership in  $NP$  does not seem to imply membership in  $co-NP$  (see Figure 20.1). For instance, the complement of TS is to determine whether *all* Hamiltonian cycles have length at least  $B + 1$  and there is no known way to verify a YES answer short of examining a very large proportion of all possible Hamiltonian cycles, which is not known to be achievable in polynomial time.

Among problems in  $NP$ , some have the property that all other problems in  $NP$  can be polynomially reduced to them. This particular class of problems is denoted by  $NP\text{-C}$  and its members are called *NP-complete* problems. If one problem in  $NP\text{-C}$  could be solved in polynomial time, then so could every problem in  $NP$  and  $P$  would be equal to  $NP$ . The question “ $P = NP?$ ” is still open and is one of the most challenging in the theory of complexity. Thus,

Figure 20.1: If  $NP \neq co\text{-}NP$ .

the NP-complete problems can be seen as the most difficult problems in NP. For example, TS is NP-complete and so is 3-satisfiability (3-SAT), for which the instance is a set of variables and a set of clauses containing exactly three different literals (a literal is either a variable  $x_i$  or a negated variable  $\bar{x}_j$ ), and the question is whether there exists a truth assignment to the variables such that each clause has at least one true literal. In other words, can the boolean formula  $E$  be satisfied, where  $E = C_1 \wedge C_2 \wedge \dots \wedge C_m$ , each clause  $C_i = x_{i_1} \vee x_{i_2} \vee x_{i_3}$ , for  $i = 1, 2, \dots, m$  and  $x_{i_1}, x_{i_2}, x_{i_3}$  are three different literals? Such an expression for  $E$  is called its *conjunctive normal form*.

Some problems might be harder than the NP-complete problems and classes of problems of increasing *apparent* difficulty, all containing NP, can be defined, which form the *polynomial hierarchy*. For these classes, the notion of completeness can be extended: a problem  $\pi$  belonging to a class  $S$  of the polynomial hierarchy is *S-complete* if every problem in  $S$  can be polynomially reduced to  $\pi$ .

In particular, the polynomial hierarchy contains classes denoted by  $\Pi_0, \Pi_1, \dots, \Pi_k, \dots$  and  $\Sigma_0, \Sigma_1, \dots, \Sigma_k, \dots$ , with the following properties:  $\Pi_0 = \Sigma_0 = P$ ,  $\Sigma_1 = NP$ ,  $\Pi_1 = co\text{-}NP$ ,  $\Pi_k = co\text{-}\Sigma_k$ ,  $\Sigma_k \cup \Pi_k \subseteq \Sigma_{k+1} \cap \Pi_{k+1}$  (see Figure 20.2).

Roughly speaking, a problem is in  $\Sigma_k$  if it can be solved by a polynomial-time nondeterministic algorithm with access to an *oracle* (a subroutine) that provides, *in one step of computation*, solutions for a problem in  $\Sigma_{k-1}$ . Another rather informal characterization of  $\Sigma_k$  is to represent the instance of a problem  $\pi$  by a string  $z$ ; now  $\pi \in \Sigma_k$  if and only if  $\pi = \{z : \exists y_1 \forall y_2 \dots$

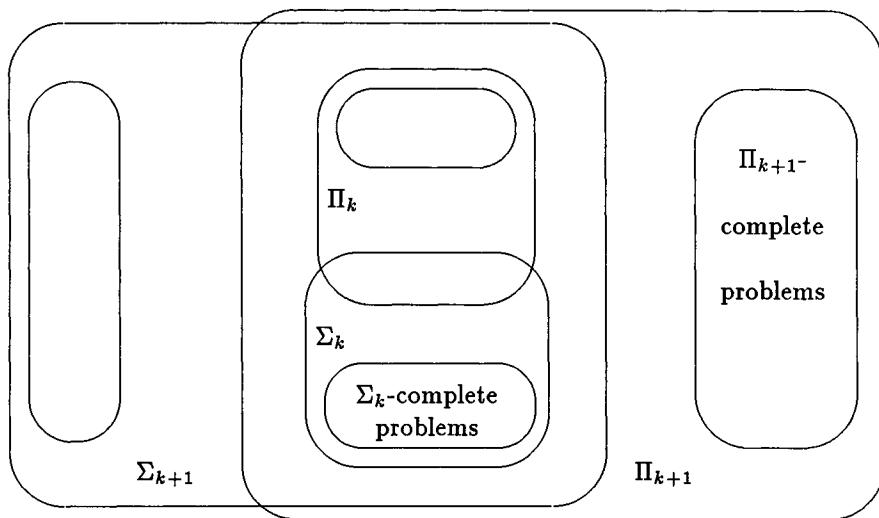


Figure 20.2: If  $\Sigma_{k+1} \neq \Pi_{k+1}$ , for  $k \geq 1$ .

$Qy_k R(z, y_1, y_2, \dots, y_k)\}$ , where the quantifiers alternate,  $Q$  stands for  $\forall$  if  $k$  is even and  $\exists$  if  $k$  is odd,  $R$  is a polynomial-time recognizable relation and the lengths of the strings  $y_1, y_2, \dots, y_k$  are polynomially bounded by the length of the string  $z$ . The same characterization holds for  $\Pi_k$ , with the alternating quantifiers  $\forall \exists \forall \dots$ . Thus, the following problem is in  $\Pi_k$  and moreover it is  $\Pi_k$ -complete.

**NAME:**  $\forall_1 \exists_2 \forall_3 \dots Q_k$ -3-satisfiability ( $\forall_1 \exists_2 \forall_3 \dots Q_k$ -3-SAT), where the quantifiers alternate and  $Q$  stands for  $\forall$  if  $k$  is odd and  $\exists$  if  $k$  is even.

**INSTANCE:**  $k$  integers  $m_1, \dots, m_k$ , a quantified Boolean expression  $\forall u_{1,1} \dots \forall u_{1,m_1} \exists u_{2,1} \dots \exists u_{2,m_2} \forall u_{3,1} \dots \forall u_{3,m_3} \dots Q u_{k,1} \dots Q u_{k,m_k} E$ , where  $E$  is in conjunctive normal form, there are three distinct literals in each clause and the quantified variables are all the variables of  $E$ .

**QUESTION:** Is it true that for every truth assignment to  $u_{1,1}, \dots, u_{1,m_1}$ , there exists a truth assignment to  $u_{2,1}, \dots, u_{2,m_2}$ , such that for every truth assignment to  $u_{3,1}, \dots, u_{3,m_3}, \dots, E$  is satisfied?

To prove that a problem  $\pi$  is  $S$ -complete, we have to check that it belongs

to  $S$  and that every problem in  $S$  can be polynomially reduced to  $\pi$ . For the second step, it is sufficient to prove that some known  $S$ -complete problem  $\pi_0$  is polynomially reducible to  $\pi$ , since all problems in  $S$  are polynomially reducible to  $\pi_0$  and the reduction process is transitive.

Completeness results are *conditional*; for example, the NP-completeness of a problem  $\pi$  means that a polynomial-time algorithm solving  $\pi$  exists if and only if  $P = NP$ ; analogously, for  $k \geq 1$ , the  $\Sigma_k$ -completeness of  $\pi$  implies that  $\pi \in \Sigma_k \setminus \Sigma_{k-1}$ , unless  $\Sigma_k = \Sigma_{k-1}$ . It is not known whether the polynomial hierarchy is finite or infinite. The first alternative occurs if  $P = NP$ ; it also occurs if for some  $k_0 \geq 1$ ,  $\Sigma_{k_0} = \Pi_{k_0}$ , since it can be shown that this would imply that for all  $k \geq k_0$ ,  $\Sigma_k = \Pi_k = \Sigma_{k_0}$ .

It is widely believed that  $P$  is not equal to  $NP$ , i.e., that no polynomial-time algorithm exists for  $NP$ -complete problems.

## 20.2 The complexity of computing the covering radius of a binary code

The complexity of computing bounds on the covering radius of a binary code has been studied first in the linear case then in the general unrestricted case. The seemingly rather paradoxical result is that the problem of upperbounding the covering radius of a linear code is  $\Pi_2$ -complete, whereas the problem of upperbounding the covering radius of a nonlinear code is “only” co-NP-complete. This fact can be explained by the more compact representation of a linear code: the size of a problem involving an  $[n, k]$  (respectively,  $(n, K)$ ) code is  $n \times k$  (respectively,  $n \times K$ ), but the latter representation provides, explicitly but uneconomically, all the elements of the code.

Co-NP-completeness and  $\Pi_2$ -completeness results mean that it is unlikely that the covering radius problem may be solved by a polynomial-time algorithm.

We first show the  $\Pi_2$ -completeness of the linear version, then the co-NP-completeness of the unrestricted version (whose proof is much shorter and simpler).

The problem of deriving an upper bound on the covering radius of a binary linear code can be stated (as a decision problem) as follows:

NAME: Upper bound on the covering radius of a binary linear code (UB-LIN).

INSTANCE: A binary linear code  $C$ , given by a parity check matrix  $\mathbf{H}$  of dimensions  $m \times n$ , an integer  $w$ .

QUESTION: Is it true that  $\forall \mathbf{y} \in \mathbb{F}^m, \exists \mathbf{x} \in \mathbb{F}^n$ , such that  $\mathbf{Hx}^T = \mathbf{y}$  and  $w(\mathbf{x}) \leq w$ ?

Indeed, since the covering radius of  $C$  is the smallest positive integer  $R$  such that any  $m$ -tuple is the sum of at most  $R$  columns of  $\mathbf{H}$  (see Theorem 2.1.9), we get a YES answer to the question if and only if  $R \leq w$ .

**Theorem 20.2.1** *The decision problem UB-LIN is  $\Pi_2$ -complete.*

**Proof.** We see that the problem UB-LIN presents the pattern  $\forall\exists$ . Thus it belongs to  $\Pi_2$ . We reduce, in two steps, the problem  $\forall\exists$ -3-satisfiability, which is, as we already mentioned,  $\Pi_2$ -complete, to UB-LIN.

NAME:  $\forall\exists$ -3-satisfiability ( $\forall\exists$ -3-SAT).

INSTANCE: A quantified Boolean expression  $\forall u_1 \dots \forall u_{m_1} \exists v_{m_1+1} \dots \exists v_{m_1+m_2} E$ , where  $E$  is in conjunctive normal form, there are three distinct literals in each clause and the quantified variables are all the variables of  $E$ .

QUESTION: Is it true that for every truth assignment to  $u_1, \dots, u_{m_1}$ , there exists a truth assignment to  $v_{m_1+1}, \dots, v_{m_1+m_2}$  that satisfies  $E$ ?

We first reduce  $\forall\exists$ -3-SAT to  $\forall\exists$ -3-dimensional matching ( $\forall\exists$ -3-DM), then we reduce  $\forall\exists$ -3-DM to UB-LIN.

NAME:  $\forall\exists$ -3-dimensional matching ( $\forall\exists$ -3-DM).

INSTANCE: Two disjoint subsets  $M_1$  and  $M_2$  of  $X_1 \times X_2 \times X_3$ , where  $X_1, X_2$  and  $X_3$  are three disjoint sets of the same cardinality.

QUESTION: Is it true that  $\forall S_1 \subseteq M_1, \exists S_2 \subseteq M_2$ , such that  $S_1 \cup S_2$  is a matching?

Recall that a *matching*  $S$  is a subset of  $M_1 \cup M_2$  with  $|X_1|$  elements such that no two triples in  $S$  agree in any coordinate.

Starting from any instance of  $\forall\exists$ -3-SAT, we have to construct, in polynomial time, an instance of  $\forall\exists$ -3-DM in such a way that positive and negative instances correspond in  $\forall\exists$ -3-DM and  $\forall\exists$ -3-SAT.

Let  $\forall u_1 \dots \forall u_{m_1} \exists v_{m_1+1} \dots \exists v_{m_1+m_2} E$  be an instance of  $\forall\exists$ -3-SAT, with  $E = C_1 \wedge C_2 \wedge \dots \wedge C_m$ . Let  $n$  be the number of variables in  $E$ .

For each variable  $w_i$  that occurs in  $E$ , let  $T_i = T_i^t \cup T_i^f$ , where

$$T_i^t = \{(\bar{w}_i[j], a_i[j], b_i[j]) : 1 \leq j \leq m\}$$

and

$$T_i^f = \{(w_i[j], a_i[j+1], b_i[j]) : 1 \leq j < m\} \cup \{(w_i[m], a_i[1], b_i[m])\}.$$

The structure of  $T_i$  depends on  $m$ . It involves “internal” elements  $a_i[j] \in X_2, b_i[j] \in X_3$  which will not occur outside of  $T_i$  and “external” elements  $w_i[j], \bar{w}_i[j]$ , elements of  $X_1$ , which will occur in other triples. Since none of the internal elements will appear outside of  $T_i$ , any matching will have to include exactly  $m$  triples from  $T_i$ , either all triples in  $T_i^t$  or all triples in  $T_i^f$ . Hence the set  $T_i$  forces a matching to choose between setting  $w_i$  true and setting  $w_i$  false. Thus, a matching  $M'$  specifies a truth assignment, with a variable  $w_i$  being set true if and only if  $M' \cap T_i = T_i^t$ .

For each clause  $C_j$ , let

$$c_j = \{(w_i[j], s_1[j], s_2[j]) : w_i \in C_j\} \cup \{(\bar{w}_i[j], s_1[j], s_2[j]) : \bar{w}_i \in C_j\};$$

$|c_j| = 3$ . The elements  $s_1[j] \in X_2, s_2[j] \in X_3$  are internal. Thus any matching  $M'$  will contain exactly one triple from  $c_j$ . This can only be done, however, if some  $w_i[j]$  (or  $\bar{w}_i[j]$ ) for a literal  $w_i \in C_j$  ( $\bar{w}_i \in C_j$ ) does not occur in the triples in  $T_i \cap M'$ , which will be the case if and only if the truth assignment, determined by  $M'$ , sets true  $w_i$  ( $\bar{w}_i$ , respectively), i.e.,  $C_j$  is satisfied.

Up to now,  $X_1$  contains  $2mn$  elements:  $w_i[j], \bar{w}_i[j]$  for  $1 \leq i \leq n$  and  $1 \leq j \leq m$ ;  $X_2$  contains  $m(n+1)$  elements:  $a_i[j], s_1[j]$ ;  $X_3$  contains  $m(n+1)$  elements:  $b_i[j], s_2[j]$ . If a matching exists, because of the internal elements in the sets  $T_i$  and  $c_j$ , it must contain exactly  $mn + m = m(n+1)$  triples belonging to these sets.

We now define a set  $G$  consisting of triples containing the external elements  $w_i[j], \bar{w}_i[j] \in X_1$  and  $m(n-1)$  additional internal elements belonging to  $X_2$  ( $X_3$ ), so that  $|X_1| = |X_2| = |X_3| = 2mn$ :

$$G = \{(w_i[j], g_1[k], g_2[k]), (\bar{w}_i[j], g_1[k], g_2[k]) : 1 \leq k \leq m(n-1), 1 \leq i \leq n, 1 \leq j \leq m\}.$$

Thus each pair of internal elements  $g_1[k], g_2[k]$  must be matched with a unique  $w_i[j]$  or  $\bar{w}_i[j]$  that does not occur in any triples of  $M' \setminus G$ . There are exactly  $m(n-1)$  such external elements and the structure of  $G$  insures that they can always be matched by choosing  $M' \cap G$  appropriately. Thus  $G$  guarantees that, whenever a set satisfies all the constraints imposed by the sets  $T_i$  and  $c_j$ , then it can be extended to a matching.

Finally, let  $M = (\bigcup_{i=1}^n T_i) \cup (\bigcup_{j=1}^m c_j) \cup G$ . It is a subset of  $X_1 \times X_2 \times X_3$ , with

$$X_1 = \{w_i[j], \bar{w}_i[j] : 1 \leq i \leq n, 1 \leq j \leq m\},$$

$$X_2 = \{a_i[j] : 1 \leq i \leq n, 1 \leq j \leq m\} \cup \{s_1[j] : 1 \leq j \leq m\} \cup \{g_1[j] : 1 \leq j \leq m(n-1)\},$$

$$X_3 = \{b_i[j] : 1 \leq i \leq n, 1 \leq j \leq m\} \cup \{s_2[j] : 1 \leq j \leq m\} \cup$$

$$\cup \{g_2[j] : 1 \leq j \leq m(n-1)\}.$$

All in all,  $M$  contains  $2mn + 3m + 2m^2n(n-1)$  elements and is constructed in polynomial time.

From the comments made during the description of  $M$ , it follows that  $M$  cannot contain a matching unless  $E$  can be satisfied by some truth assignment to its variables. Conversely, if there exists a truth assignment that satisfies  $E$ , let  $M' \subseteq M$  be constructed as follows: for each clause  $C_j$ , let  $z_j \in \{w_i, \bar{w}_i : 1 \leq i \leq n\} \cap C_j$  be a literal that is set true (there is at least one). Set

$$M' = \left( \bigcup_{w_i=\text{true}} T_i^t \right) \cup \left( \bigcup_{w_i=\text{false}} T_i^f \right) \cup \left( \bigcup_{j=1}^m \{(z_j[j], s_1[j], s_2[j])\} \right) \cup G',$$

where  $G'$  is a well chosen subset of  $G$  that includes all the  $g_1[k], g_2[k]$  and remaining  $w_i[j]$  and  $\bar{w}_i[j]$ . Such a  $G'$  can always be found and the resulting  $M'$  is a matching included in  $M$ .

Next, for all variables  $u_i$  ( $1 \leq i \leq m_1$ ), let  $M_1$  contain one triple belonging to  $T_i^t$  and let  $M_2 = M \setminus M_1$ .

This construction is polynomial. We now have to prove that

for every truth assignment to  $u_1, \dots, u_{m_1}$ , there exists a truth assignment to  $v_{m_1+1}, \dots, v_{m_1+m_2}$ , that satisfies  $E$   
if and only if

for all  $S_1 \subseteq M_1$ , there exists  $S_2 \subseteq M_2$ , such that  $S_1 \cup S_2$  is a matching with sets  $X_1, X_2, X_3, M_1$  and  $M_2$  as above.

First suppose that for all  $S_1 \subseteq M_1$ , there exists  $S_2 \subseteq M_2$ , such that  $S_1 \cup S_2$  is a matching. For any truth assignment to  $u_1, \dots, u_{m_1}$ , let  $S_1$  contain the triples in  $M_1$  that correspond to the variables that are set true. Let  $S_2 \subseteq M_2$  be such that  $S_1 \cup S_2$  is a matching. Assign true to those variables  $v_j$  for which  $T_j^t \subseteq S_2$  and false to the others. This assignment makes  $E$  true.

Conversely, assume that for every truth assignment to  $u_1, \dots, u_{m_1}$ , there exists a truth assignment to  $v_{m_1+1}, \dots, v_{m_1+m_2}$ , that satisfies  $E$ . Let  $S_1$  be any subset of  $M_1$ . Assign true to those variables  $u_i$  for which  $T_i^t \cap S_1$  is nonempty and false to the others. Assign true to the variables  $v_j$  so that  $E$  is true. There exists a matching  $S$  that contains  $T_i^t, T_j^t$  for all the true variables  $u_i, v_j$  and for none of the false variables. Let  $S_2 = S \setminus S_1$ :  $S = S_1 \cup S_2$  and  $S_2 \subseteq M_2$ .

Next, starting from any instance of  $\forall\exists\text{-3-DM}$ , we have to construct, in polynomial time, an instance of UB-LIN in such a way that positive and negative instances correspond in UB-LIN and  $\forall\exists\text{-3-DM}$ .

Let  $M_1, M_2, X_1, X_2, X_3$  be an instance of  $\forall\exists\text{-3-DM}$ . Let  $M = M_1 \cup M_2$  (so  $|M| = |M_1| + |M_2|$ ), let  $p = |X_i|$  and  $X_i = \{x_{i,1}, x_{i,2}, \dots, x_{i,p}\}$  for  $i = 1, 2, 3$ . Let  $w = p$  and

$$\mathbf{H} = \begin{bmatrix} \mathbf{H}_1 \\ \mathbf{H}_2 \end{bmatrix}$$

be a binary matrix of dimensions  $(3p + |M_1|) \times 8|M|$ , where  $\mathbf{H}_1$  and  $\mathbf{H}_2$  have dimensions  $3p \times 8|M|$  and  $|M_1| \times 8|M|$ , respectively. If  $t = (x_{1,i}, x_{2,j}, x_{3,k})$  belongs to  $M$ , then we let  $\mathbf{H}_1$  contain one column,  $\mathbf{H}_1^{t(0)}$ , with exactly three ones in the positions corresponding to  $x_{1,i}, x_{2,j}$  and  $x_{3,k}$ , and seven columns,  $\mathbf{H}_1^{t(1)}, \mathbf{H}_1^{t(2)}, \dots, \mathbf{H}_1^{t(7)}$ , obtained from  $\mathbf{H}_1^{t(0)}$  by replacing ones by zeros in all possible ways. So each triple  $t \in M$  is associated with eight columns in  $\mathbf{H}$ . Each row in  $\mathbf{H}_2$  corresponds to a triple in  $M_1$ , with ones in the eight columns associated with this triple and zeros elsewhere.

This construction is polynomial. We now have to prove that

$\forall S_1 \subseteq M_1, \exists S_2 \subseteq M_2$ , such that  $S_1 \cup S_2$  is a matching

if and only if

$\forall \mathbf{y} \in \mathbb{F}^m, \exists \mathbf{x} \in \mathbb{F}^n$ , such that  $\mathbf{Hx}^T = \mathbf{y}$  and  $w(\mathbf{x}) \leq w$ ,

with  $m = 3p + |M_1|, n = 8|M|$ , matrix  $\mathbf{H}$  as above and  $w = p = |X_1|$ .

Assume that for all  $S_1 \subseteq M_1$ , there exists  $S_2 \subseteq M_2$ , such that  $S_1 \cup S_2$  is a matching. Let  $\mathbf{y}$  be any vector of length  $3w + |M_1|$ . The last  $|M_1|$  coordinates of  $\mathbf{y}$  correspond to the triples in  $M_1$  and the ones in these locations select a subset  $S_1$  of  $M_1$ . Choose  $S_2 \subseteq M_2$ , such that  $S = S_1 \cup S_2$  is a matching. Let  $\mathbf{y}'$  be the vector of length  $3w$  obtained from  $\mathbf{y}$  by taking its first  $3w$  components. Let  $*$  stand for the componentwise product. Because  $\sum_{t \in S} \mathbf{H}_1^{t(0)} = 1^{3w}$ , we get:  $\mathbf{y}' = (\sum_{t \in S} \mathbf{H}_1^{t(0)}) * \mathbf{y}' = \sum_{t \in S} (\mathbf{H}_1^{t(0)} * \mathbf{y}')$ . Since  $\mathbf{H}_1^{t(0)} * \mathbf{y}' = \mathbf{H}_1^{t(j)}$  for some  $j$  between 0 and 7, this means that  $\mathbf{y}'$  is the sum of  $|S| = w$  columns of  $\mathbf{H}_1$ . But the way  $\mathbf{H}$  was constructed and  $S_1$  was chosen from  $\mathbf{y}$  also shows that the sum of these same  $w$  columns of  $\mathbf{H}$  is equal to  $\mathbf{y}$ , i.e.,  $\mathbf{y} = \mathbf{Hx}^T$ , with  $w(\mathbf{x}) = w$ . Since  $\mathbf{y}$  was arbitrary, the UB-LIN property holds.

Conversely, assume that for all  $\mathbf{y} \in \mathbb{F}^{3w + |M_1|}$ , there exists  $\mathbf{x} \in \mathbb{F}^{8|M|}$ , such that  $\mathbf{Hx}^T = \mathbf{y}$  and  $w(\mathbf{x}) \leq w$ . For any set  $S_1 \subseteq M_1$ , let  $\mathbf{y}$  be the vector with all ones in the first  $3w$  coordinates and with ones in those coordinates among the last  $|M_1|$  that correspond to triples in  $S_1$ . Then  $\mathbf{H}_1 \mathbf{x}^T = 1^{3w}$  and  $\mathbf{H}_1 \mathbf{x}^T$  is the sum of at most  $w$  columns of  $\mathbf{H}_1$ , each column containing at most three ones. Thus,  $\mathbf{H}_1 \mathbf{x}^T$  is the sum of exactly  $w$  columns of  $\mathbf{H}_1$ , each column containing exactly three ones. So  $\mathbf{Hx}^T$  is the sum of  $w$  columns  $\mathbf{H}^{t(0)}$  of  $\mathbf{H}$  and these  $w$  columns select a matching  $S$ . Since this sum has ones in just those positions among the last  $|M_1|$  that correspond to triples in  $S_1$ , it follows that the triples in  $M_1$  that are contained in  $S$  are just those in  $S_1$ . Therefore  $S = S_1 \cup S_2$ , where  $S_2 \subseteq M_2$ . Thus the  $\forall \exists$ -3-dimensional matching property holds.

This proves, together with  $\text{UB-LIN} \in \Pi_2$ , that  $\text{UB-LIN}$  is  $\Pi_2$ -complete.  $\square$

We now deal with the nonlinear case and state the (decision) problem of lowerbounding the covering radius of a binary code as follows:

NAME: Lower bound on the covering radius of a binary code (LB-NLIN).

INSTANCE: A binary code  $C \subseteq \mathbb{F}^n$ , given explicitly by its elements, an integer  $w$ .

QUESTION: Is it true that  $\exists \mathbf{y} \in \mathbb{F}^n$ , such that  $\forall \mathbf{c} \in C, d(\mathbf{y}, \mathbf{c}) \geq w$ ?

We get a YES answer to the question if and only if  $R(C) \geq w$ . This representation of the problem immediately shows that it belongs to NP, since it can be checked in polynomial time, for a given vector  $\mathbf{y}$ , whether  $d(\mathbf{y}, C) \geq w$  or not.

In order to prove the NP-completeness of LB-NLIN (Theorem 20.2.5 below), we need the following definitions, notations and easy lemmas.

We say that a vector  $\mathbf{v} = (v_1, v_2, \dots, v_{2n}) \in \mathbb{F}^{2n}$  is *doubled* if and only if  $v_{2i-1} = v_{2i}$  for all  $i = 1, 2, \dots, n$ . Let  $\mathbf{u}(i) \in \mathbb{F}^{2i}$  denote the vector  $(0101\dots01)$ . Let  $Y_{2n}^1 = \{(01|\mathbf{u}(n-1)), (10|\mathbf{u}(n-1)), (01|\overline{\mathbf{u}}(n-1)), (10|\overline{\mathbf{u}}(n-1))\}$ .

**Lemma 20.2.2** *If  $\mathbf{v} = (v_1, v_2, \dots, v_{2n}) \in \mathbb{F}^{2n}$  is such that for all  $\mathbf{y} \in Y_{2n}^1, d(\mathbf{v}, \mathbf{y}) \leq n$ , then  $v_2 = v_1$ .*  $\square$

Let  $Y_{2n}^j = s_j(Y_{2n}^1)$ , where  $s_j$  denotes the circular right shift of  $2j-2$  bits, for  $j = 2, 3, \dots, n$ .

**Lemma 20.2.3** *If  $\mathbf{v} = (v_1, v_2, \dots, v_{2n}) \in \mathbb{F}^{2n}$  is such that for all  $\mathbf{y} \in Y_{2n}^j, d(\mathbf{v}, \mathbf{y}) \leq n$ , then  $v_{2j} = v_{2j-1}$ .*  $\square$

Let  $Y_{2n} = \bigcup_{j=1}^n Y_{2n}^j$ ;  $|Y_{2n}| = 2n+2$ , since  $(01|\mathbf{u}(n-1))$  and  $(10|\overline{\mathbf{u}}(n-1))$  are invariant under all even circular shifts.

**Lemma 20.2.4** *A vector  $\mathbf{v} \in \mathbb{F}^{2n}$  is doubled if and only if  $d(\mathbf{y}, \mathbf{v}) \leq n$  for all  $\mathbf{y} \in Y_{2n}$ .*  $\square$

We are now ready to prove the following:

**Theorem 20.2.5** *The decision problem LB-NLIN is NP-complete.*

**Proof.** We reduce 3-satisfiability, which is mentioned to be NP-complete in Section 20.1, to LB-NLIN.

NAME: 3-satisfiability (3-SAT).

INSTANCE: A boolean formula  $E$ , in conjunctive normal form, with exactly three distinct literals in each clause.

QUESTION: Can  $E$  be satisfied?

Starting from any instance of 3-SAT, we have to construct, in polynomial time, an instance of LB-NLIN in such a way that positive and negative instances correspond in LB-NLIN and 3-SAT. Let  $E = C_1 \wedge C_2 \wedge \dots \wedge C_m$  be an instance of 3-SAT, each clause  $C_j$ , defined over the set of variables  $\{x_1, x_2, \dots, x_n\}$ , consisting of exactly three distinct literals. For each clause  $C_j$ , let  $\mathbf{z}(C_j) = (z_1, \dots, z_{2n}) \in \mathbb{F}^{2n}$  be the vector defined by

$z_{2i-1} = z_{2i} = 0$  if  $C_j$  contains the literal  $\bar{x}_i$ ;

$z_{2i-1} = z_{2i} = 1$  if  $C_j$  contains the literal  $x_i$ ;

$z_{2i-1} = 0$  and  $z_{2i} = 1$  otherwise.

We define  $C \subseteq \mathbb{F}^{2n+2}$  as follows:

$$C = \{(\mathbf{z}(C_j)|00) : 1 \leq j \leq m\} \cup Y_{2(n+1)}.$$

Finally, let  $w = n + 1$ . The code  $C$  contains  $m + 4 + 2n$  codewords and its construction is polynomial in  $nm$ , the size of the instance of 3-SAT. We now have to prove that

$E$  can be satisfied

if and only if

$C$  has covering radius at least  $w$ .

First suppose that  $E$  can be satisfied; a truth assignment to the variables  $\{x_1, x_2, \dots, x_n\}$  that satisfies  $E$  can be represented by a vector  $\mathbf{v} = (v_1, v_2, \dots, v_n) \in \mathbb{F}^n$ . Let  $\mathbf{v}^* = (v_1, v_1, v_2, v_2, \dots, v_n, v_n, 0, 0) \in \mathbb{F}^{2n+2}$ . Then for all  $\mathbf{c} \in Y_{2(n+1)}$ ,  $d(\mathbf{c}, \mathbf{v}^*) \leq n + 1$  (by Lemma 20.2.4). Moreover, in each clause  $C_j$  there is at least one literal which is set true by  $\mathbf{v}$ ; it is easy to see then that  $d((\mathbf{z}(C_j)|00), \mathbf{v}^*) \leq 2 + 2 + 0 + (n - 3) = n + 1$ . Finally, for all  $\mathbf{c} \in C$ ,  $d(\mathbf{c}, \mathbf{v}^*) \leq n + 1$ . This implies that  $d(C, \bar{\mathbf{v}}^*) \geq 2n + 2 - (n + 1) = n + 1$ , so  $R(C) \geq w$ .

Conversely, assume that  $R(C) \geq w = n + 1$ . Then there exists  $\mathbf{v}^* \in \mathbb{F}^{2n+2}$ ,  $d(\mathbf{v}^*, C) \geq n + 1$  and  $d(\bar{\mathbf{v}}^*, \mathbf{c}) \leq n + 1$  for all codewords  $\mathbf{c}$ . In particular, for all  $\mathbf{c} \in Y_{2(n+1)}$ ,  $d(\bar{\mathbf{v}}^*, \mathbf{c}) \leq n + 1$ . By Lemma 20.2.4,  $\bar{\mathbf{v}}^*$  is doubled:

$\bar{\mathbf{v}}^* = (v_1, v_1, v_2, v_2, \dots, v_{n+1}, v_{n+1})$ . Furthermore,  $d(\bar{\mathbf{v}}^*, (\mathbf{z}(C_j)|00)) \leq n + 1$  for all  $j$ , so

$$d((v_1, v_1, v_2, v_2, \dots, v_n, v_n), \mathbf{z}(C_j)) \leq n + 1.$$

Let  $\mathbf{v} = (v_1, v_2, \dots, v_n)$ . The structure of  $\mathbf{z}(C_j)$  shows that there exists  $i \in \{1, \dots, n\}$  such that  $z_{2i-1} = z_{2i}$  and  $d((v_i, v_i), (z_{2i-1}, z_{2i})) = 0$ . This means that the truth assignment defined by  $\mathbf{v}$  satisfies clause  $C_j$ : if  $z_{2i-1} = z_{2i} = v_i = 1$  (respectively, 0), then variable  $x_i$  is true (respectively, false) and  $x_i$  (respectively,  $\bar{x}_i$ ) belongs to  $C_j$ . Hence  $E$  is satisfied.  $\square$

As an immediate consequence, the decision problem associated to the problem of *upperbounding* the covering radius of a nonlinear code is co-NP-complete.

## 20.3 Derandomization

Recall (see Definition 3.7.5) that a binary  $n \times m$  array is called *t-independent* or *t-surjective* if any  $n \times t$  subarray contains among its rows all  $2^t$  possible *t*-tuples (see for instance Sections 3.7 and 6.2 for the use of surjectivity for covering codes — especially 2-surjectivity).

We denote by  $f(n, t)$  the maximum number of columns in a *t-surjective* array with  $n$  rows, and by  $g(m, t)$  the minimum number of rows in a *t-surjective* array with  $m$  columns. The study of  $f(n, t)$  is equivalent to that of  $g(m, t)$ . In Section 3.7, we use for  $g(m, t)$  the alternative notation  $ms_2(m, t)$ .

A family  $\mathcal{F}$  of vectors of  $\mathbb{F}^n$  is said to be *t-independent*, or *t-surjective*, if  $\mathbf{M}$ , the  $n \times |\mathcal{F}|$  two-dimensional array whose columns are the elements of  $\mathcal{F}$ , is *t-surjective*. Thus  $f(n, t)$  is the maximum size of a *t-independent* family of vectors of  $\mathbb{F}^n$ . Let us mention two applications of the study of  $f(n, t)$ .

1. VLSI testing. Suppose a circuit  $\mathcal{C}$  has  $N$  binary inputs with the property that each output is influenced by at most  $t$  inputs. Let  $\mathcal{F}$  be a *t-independent* family of vectors of  $\mathbb{F}^n$  of size  $|\mathcal{F}| = N$ . Then the  $n$  rows of  $\mathbf{M}$  make up an exhaustive set of *test vectors* for the circuit  $\mathcal{C}$ : this means that if  $\mathcal{C}$  responds correctly to the  $n$  input vectors, then we can guarantee that  $\mathcal{C}$  is not faulty.
2. Writing on binary memories with defects. In a defective memory, some positions are stuck at “0” while others are stuck at “1”. Suppose the total number of defective positions does not exceed  $t$ . A code adapted to such a memory is a set  $\{\mathbf{M}_i\}$  of row-disjoint  $n \times |\mathcal{F}_i|$  two-dimensional arrays, where each  $\mathcal{F}_i$  is *t-independent*. Encoding message  $i$  is done by picking a row out of  $\mathbf{M}_i$  that “matches” the memory’s defects.

For  $t = 2$ , the problem of determining  $f(n, t)$  has been solved (cf. Section 6.2). In the general case  $t \geq 3$  however, gaps remain between lower and upper estimates of the size of the largest  $t$ -independent families.

## Constructive issues

We use the following terminology for  $t$ -independent families. An infinite sequence  $(\mathcal{F}_n)_{n=1}^{\infty}$ , where each  $\mathcal{F}_n$  is a  $t$ -independent family of vectors of  $\mathbb{F}^n$ , is called *constructive* if there exists an algorithm that computes any member of  $\mathcal{F}_n$  in (worst case) time complexity polynomial in  $n$ . It is called *semi-constructive* if there is an algorithm which computes any member of  $\mathcal{F}_n$  in complexity polynomial in  $|\mathcal{F}_n|$ .

Nonconstructive bounds on the maximum size  $f(n, t)$  of a  $t$ -independent family of vectors of  $\mathbb{F}^n$ , when  $n$  goes to infinity for constant  $t$ , have been obtained by random arguments proving that  $f(n, t) = 2^{c_t n}$  with

$$(t2^t \ln 2)^{-1}(1 + o(1)) \leq c_t \leq 2^{-t}. \quad (20.3.1)$$

Semi-constructive  $t$ -independent families  $(\mathcal{F}_n)$  which also satisfy

$$\Omega(t^{-1}2^{-t}) \leq \frac{1}{n} \log |\mathcal{F}_n| \quad (20.3.2)$$

have been obtained, although the constants are worse than those obtained by random arguments. Theorem 20.3.5 below gives better semi-constructive family sizes.

Up to now, the best result on the largest possible constructive exponential sized  $t$ -independent families is

$$|\mathcal{F}_n| = 2^{c_t n + o(n)} \text{ where } c_t = 8t^{-3}2^{-2t}(1 + o(1)). \quad (20.3.3)$$

We now use an altogether different strategy, somewhat in the spirit of derandomization, for obtaining semi-constructive  $t$ -independent families. The object is to turn a randomized algorithm into a deterministic one. The idea is to replace random choice on an exponentially large space by exhaustive search on a polynomially small sample space that “inherits” the original probability distribution.

The problem of finding the minimum number  $g(m, t)$  of rows of a  $t$ -surjective array of length  $m$  can be rephrased (see Becker and Simon [64] and Zémor and Cohen [703]) as a *transversal* or *covering* problem, namely:

**Problem 1** Find the minimum cardinality of a subset  $\mathcal{R}$  of  $\mathbb{F}^m$  such that

$$\mathcal{R} \cap K_{m-t} \neq \emptyset$$

for every  $(m - t)$ -dimensional face  $K_{m-t}$  of  $\mathbb{F}^m$ .

This is reminiscent of the classical covering problem:

**Problem 2** Find the minimum cardinality of a subset  $C$  of  $\mathbb{F}^n$  such that

$$C \cap \mathcal{B}_r(\mathbf{x}) \neq \emptyset$$

for every sphere of radius  $r$ .

The problem is now sufficiently transformed for us to apply a theorem which gives an efficient covering by means of a greedy algorithm. View  $\mathbb{F}^m$  as the vertex set of a hypergraph, the set  $\mathcal{H}$  of hyperedges being the  $(m-t)$ -dimensional faces (see Berge [66] for an account on hypergraphs). Note that every hyperedge has size  $b = 2^{m-t}$  and that every vertex belongs to  $\Delta = \binom{m}{t}$  hyperedges:  $(\mathbb{F}^m, \mathcal{H})$  is  $b$ -uniform and  $\Delta$ -regular. Let us restate the Johnson-Stein-Lovász theorem in a form convenient to us.

**Theorem 20.3.4** *If  $(V, \mathcal{H})$  is a  $b$ -uniform and  $\Delta$ -regular hypergraph, then a greedy algorithm outputs a transversal of  $(V, \mathcal{H})$  with at most  $\frac{|V|}{b}(1 + \ln \Delta)$  elements.*

**Proof.** For an elementary proof, see Theorem 12.2.1. □

Consequently,

$$g(m, t) \leq 2^t(1 + \ln \binom{m}{t}).$$

Asymptotically (for large  $m$ ), this reduces to the lower bound in (20.3.1). As it stands, the complexity of the greedy algorithm is exponential in  $m$ , and we have not gained anything on the existential result of (20.3.1).

We now improve on this in the following way. Consider an  $[m, k]$  linear code  $C$  such that its dual  $C^\perp$  has minimum distance  $t+1$ . Then (see the last paragraph of Section 2.2)  $C$  is an orthogonal array of strength  $t$ . In other words, the  $2^k$  codewords of  $C$  make up the rows of a  $t$ -independent array with the stronger requirement that on any  $t$  given column positions, every binary  $t$ -tuple appears in exactly  $2^{k-t}$  rows.

Consider now the induced hypergraph  $(C, \mathcal{H}')$  where  $\mathcal{H}' = \{H \cap C : H \in \mathcal{H}\}$ . Clearly,  $(C, \mathcal{H}')$  is  $\binom{m}{t}$ -regular and  $2^{k-t}$ -uniform because of the orthogonal array property. Applying Theorem 20.3.4, we obtain with a greedy algorithm a transversal of  $(C, \mathcal{H}')$ , which is also a transversal of  $(\mathbb{F}^m, \mathcal{H})$ . Its size is the same as before, but we now have a substantial gain in complexity: the set of vertices on which we are performing our greedy algorithm has size  $2^k$  instead of  $2^m$ . For a given  $t$  and for  $m$  a large enough primitive length ( $m = 2^i - 1$ ), we can choose for  $C^\perp$  a BCH code (see Section 10.1) with dimension  $m-k = m - \lfloor \frac{t}{2} \rfloor \log(m+1)$ , yielding  $|C| = (m+1)^{\lfloor t/2 \rfloor}$ . The greedy

Table 20.1: Achievable sizes for  $t$ -independent families  $\mathcal{F}$  :  $|\mathcal{F}| \geq 2^{c_t n}$ .

	constructive	semi-constructive		existential	
$t = 3$	$1/12.34$	i	$1/9.50$	ii	$1/7.44$
$t = 4$	$1/148.68$	ii	$1/44.36$	iv	$1/27.32$
$t$	$c_t \approx 8/t^3 2^{2t}$	v	$c_t \approx 1/t 2^t \ln 2$	iv	$c_t \approx 1/(t-1) 2^t \ln 2$
i. Sloane [593]. ii. Cohen and Zémor [172]. iii. Roux [565]. iv. Theorem 20.3.5. v. (20.3.3).					

algorithm is now polynomial in  $m$ , which means that the  $t$ -independent family we obtain in this manner is semi-constructive. This is an example of derandomization.

Reverting to the notation of  $t$ -independent families, we have obtained:

**Theorem 20.3.5** *There is a semi-constructive sequence  $\mathcal{F}_n$  of  $t$ -independent families of  $\text{IF}^n$  of size  $2^{c_t n}$  with  $c_t = (1/t 2^t \ln 2)(1 + o(1))$ .*  $\square$

This coincides with the lower bound of (20.3.1), and is the best to date in the semi-constructive case for  $t \geq 4$ .

## 20.4 Notes

For results on the complexity of other problems related to coding theory, see Berlekamp, McEliece and van Tilborg [69], Ntafos and Hakimi [504], Diaconis and Graham [200], Lobstein and Cohen [451], Bruck and Naor [106], Lobstein [450], Stern [623], Barg [50], Vardy [660], mainly from an NP-completeness point of view.

**§20.1** For a deeper, more formal account of the theory of NP-completeness and polynomial hierarchy, we refer the interested reader to Garey and D. S. Johnson [247] and Barthélemy, Cohen and Lobstein [51], which have been largely used for the exposition of Section 20.1.

The  $\Pi_k$ -completeness of  $\forall_1 \exists_2 \forall_3 \dots Q_k$ -3-satisfiability is due to Meyer and Stockmeyer [484].

**§20.2** Theorem 20.2.1 was proved by McLoughlin [481] in 1984. In that proof, in the reduction of  $\forall \exists$ -3-satisfiability to  $\forall \exists$ -3-dimensional matching, the

construction of  $M$ , starting from formula  $E$ , is from Garey and D. S. Johnson [247].

Theorem 20.2.5 and the preceding lemmas are by Frances and Litman [241] (1994). However in [130], Carnielli mentions that “Interest in more specific methods of attack on the hyper-rook domain problem is justified because this problem is hard to treat in algorithmic terms: indeed, as pointed in [129], it is an NP-complete problem. This fact can be proved just by showing that a particular case of the problem, when formulated in algorithmic terms, reduces to the matrix domination problem (see [247, §A.12]) which is known to be an NP-complete problem.”

**§20.3** The study of  $f(n, t)$  originates in Rényi [550], under the name of *qualitative independence*, and has since been extensively studied by Kleitman and Spencer [380], Alon [14], Roux [565], Freiman, Lipkin and Levitin [242], Alon, Bruck, J. Naor, M. Naor and Roth [18], Sloane [593].

For applications to VLSI testing, see Seroussi and Bshouty [577]. About writing on memories with defects, see, e.g., Dumer [211] and references therein. Let us also mention that  $t$ -independent families have applications in  $\epsilon$ -biased probability spaces, see J. Naor and M. Naor [502], and derandomization, see Alon, Babai and Itai [16].

The values of  $f(n, 2)$  are known (see Section 3.7). A  $q$ -ary generalization, namely the qualitative 2-independence problem, is solved asymptotically by Gargano, Körner and Vaccaro [248].

Inequalities (20.3.1) are due to Kleitman and Spencer [380]. An improvement of their argument yielding better numerical constants is given by Roux [565].

Inequality (20.3.2) is by Freiman, Lipkin and Levitin [242], where the problem of finding the largest possible semi-constructive  $t$ -independent families is studied. Theorem 20.3.5 is by Cohen and Zémor [172].

The problem of finding the largest possible constructive exponential sized  $t$ -independent families was studied first in Alon [14], then by Alon, Bruck, J. Naor, M. Naor and Roth [18], where the inequality  $\Omega(t^{-1}2^{-3t}) \leq \frac{1}{n} \log |\mathcal{F}_n|$  was established. The improvement (20.3.3) is due to Cohen and Zémor [172].

# Bibliography

- [1] M. J. AALTONEN: Linear programming bounds for tree codes, *IEEE Trans. Inform. Th.*, vol. 25, pp. 85–90, 1979.
- [2] M. J. AALTONEN: Bounds on the information rate of a tree code as a function of the code's feedback decoding minimum distance, *Ann. Univ. Turku, Ser. A I*, No. 181, 1981.
- [3] M. J. AALTONEN: A new upper bound on nonbinary block codes, *Discrete Mathematics*, vol. 83, pp. 139–160, 1990.
- [4] E. H. L. AARTS and J. KORST: *Simulated Annealing and Boltzmann Machines: a Stochastic Approach to Combinatorial Optimization and Neural Computing*, Chichester: Wiley, 1989.
- [5] E. H. L. AARTS and P. J. M. van LAARHOVEN: Local search in coding theory, *Discrete Mathematics*, vol. 106/107, pp. 11–18, 1992.
- [6] E. H. L. AARTS and J. K. LENSTRA, Eds.: *Local Search Algorithms*, Wiley, to appear.
- [7] C. M. ADAMS and S. E. TAVARES: Generating and counting binary bent sequences, *IEEE Trans. Inform. Th.*, vol. 36, pp. 1170–1173, 1990.
- [8] M. J. ADAMS: Subcodes and covering radius, *IEEE Trans. Inform. Th.*, vol. 32, pp. 700–701, 1986.
- [9] R. AHLSWEDE: Coloring hypergraphs: a new approach to multi-user source coding–II, *J. Combinatorics, Information & System Sciences*, vol. 5, No. 3, pp. 220–268, 1980.
- [10] R. AHLSWEDE, L. A. BASSALYGO and M. S. PINSKER: Binary constant-weight codes correcting localized errors and defects, *Problemy Peredachi Informatsii*, vol. 30, No. 2, pp. 102–104, 1994. Translated in: *Problems of Inform. Transm.*, vol. 30, No. 2, pp. 10–13.
- [11] R. AHLSWEDE and G. SIMONYI: Reusable memories in the light of the old arbitrarily varying and a new outputwise varying channel theory, *IEEE Trans. Inform. Th.*, vol. 37, pp. 1143–1150, 1991.
- [12] R. AHLSWEDE and Z. ZHANG: Coding for write-efficient memory, *Information and Control*, vol. 83, pp. 80–97, 1989.

- [13] J. M. van der AKKER, J. H. KOOLEN and R. J. M. VAESSENS: Perfect codes with distinct protective radii, *Discrete Mathematics*, vol. 81, pp. 103–109, 1990. Addendum, *Discrete Mathematics*, vol. 89, p. 325, 1991.
- [14] N. ALON: Explicit construction of exponential sized families of  $k$ -independent sets, *Discrete Mathematics*, vol. 58, pp. 191–193, 1986.
- [15] N. ALON: Transmitting in the  $n$ -dimensional cube, *Discrete Applied Mathematics*, vol. 37/38, pp. 9–11, 1992.
- [16] N. ALON, L. BABAI and A. ITAI: A fast and simple randomized algorithm for the maximal independent set problem, *J. Algorithms*, vol. 7, pp. 567–583, 1986.
- [17] N. ALON, E. E. BERGMANN, D. COPPERSMITH and A. M. ODLYZKO: Balancing sets of vectors, *IEEE Trans. Inform. Th.*, vol. 34, pp. 128–130, 1988.
- [18] N. ALON, J. BRUCK, J. NAOR, M. NAOR and R. ROTH: Construction of asymptotically good low-rate error-correcting codes through pseudo-random graphs, *IEEE Trans. Inform. Th.*, vol. 38, pp. 509–516, 1992.
- [19] N. ALON, M. B. NATHANSON and I. RUZSA: The polynomial method and restricted sums of congruence classes, Preprint, 1996.
- [20] N. ALON and J. H. SPENCER: *The Probabilistic Method*, New York: Wiley, 1992.
- [21] D. R. ANDERSON: A new class of cyclic codes, *SIAM J. Applied Mathematics*, vol. 16, pp. 181–197, 1968.
- [22] I. ANDERSON: *Combinatorics of Finite Sets*, Oxford: Clarendon Press, 1987.
- [23] E. F. ASSMUS, Jr., and H. F. MATTSON, Jr.: Error-correcting codes: an axiomatic approach, *Information and Control*, vol. 6, pp. 315–330, 1963.
- [24] E. F. ASSMUS, Jr., and H. F. MATTSON, Jr.: Coding and combinatorics, *SIAM Review*, vol. 16, pp. 349–388, 1974.
- [25] E. F. ASSMUS, Jr., and H. F. MATTSON, Jr.: Some 3-error correcting BCH codes have covering radius 5, *IEEE Trans. Inform. Th.*, vol. 22, pp. 348–349, 1976.
- [26] E. F. ASSMUS, Jr., H. F. MATTSON, Jr., and R. TURYN: Cyclic codes, Final Report, Document No. AFCRL-66-348, Sylvania App. Res. Lab., Waltham, United States, 1966.
- [27] E. F. ASSMUS, Jr., and V. S. PLESS: On the covering radius of extremal self-dual codes, *IEEE Trans. Inform. Th.*, vol. 29, pp. 359–363, 1983.
- [28] J. ASTOLA: On the nonexistence of certain perfect Lee-error-correcting codes, *Ann. Univ. Turku, Ser. A I*, No. 167, 1975.
- [29] J. ASTOLA: On perfect codes in the Lee-metric, *Ann. Univ. Turku, Ser. A I*, No. 176, p. 56, 1978.
- [30] J. ASTOLA: A note on perfect arithmetic codes, *IEEE Trans. Inform. Th.*, vol. 32, pp. 443–445, 1986.

- [31] S. V. AVGUSTINOVICH: On one property of perfect binary codes, *Diskr. Analys i Issledovanie Operatsii*, vol. 2, No. 1, pp. 4–6, 1995 (in Russian).
- [32] S. V. AVGUSTINOVICH and F. I. SOLOVJOVA: On projections of perfect binary codes, *Proc. Seventh Joint Swedish-Russian Internat. Workshop on Information Theory*, pp. 25–26, St-Petersburg, 1995.
- [33] S. V. AVGUSTINOVICH and F. I. SOLOVJOVA: Construction of perfect binary codes by the sequential translations of the  $i$ -components, *Proc. 5th Internat. Workshop on Algebraic and Combinatorial Coding Theory*, pp. 9–14, Sozopol, 1996.
- [34] S. V. AVGUSTINOVICH and F. I. SOLOVJOVA: Existence of nonsystematic perfect binary codes, *Proc. 5th Internat. Workshop on Algebraic and Combinatorial Coding Theory*, pp. 15–19, Sozopol, 1996.
- [35] S. V. AVGUSTINOVICH and F. I. SOLOVJOVA: On nonsystematic perfect binary codes, *Problemy Peredachi Informatsii*, to appear.
- [36] J. AX: Zeroes of polynomials over finite fields, *American J. Math.*, vol. 86, pp. 255–261, 1964.
- [37] T. S. BAICHEVA: Covering radius of ternary cyclic codes with length up to 20, *Proc. 4th Internat. Workshop on Algebraic and Combinatorial Coding Theory*, pp. 12–17, Novgorod, 1994.
- [38] T. S. BAICHEVA: Least covering radius of two-dimensional codes over  $GF(3)$  and  $GF(4)$ , *Proc. Internat. Workshop on Optimal Codes*, pp. 7–10, Sozopol, 1995.
- [39] T. S. BAICHEVA: Least covering radii of ternary linear codes, *Proc. 5th Internat. Workshop on Algebraic and Combinatorial Coding Theory*, pp. 20–24, Sozopol, 1996.
- [40] T. S. BAICHEVA and E. D. VELIKOVA: Least covering radius of three-dimensional codes over  $GF(3)$ , *Proc. 25th Conf. of the Union of Bulgarian Mathematicians*, pp. 68–71, 1996.
- [41] T. S. BAICHEVA and E. D. VELIKOVA: Covering radii of ternary linear codes of small dimensions and codimensions, *IEEE Trans. Inform. Th.*, submitted.
- [42] P. BALDI: On a generalized family of colorings, *Graphs and Combinatorics*, vol. 6, pp. 95–110, 1990.
- [43] K. BALL: On packing unequal squares, *J. Combinatorial Th.*, Ser. A, vol. 75, pp. 353–357, 1996.
- [44] E. BANNAI: On perfect codes in the Hamming schemes  $H(n, q)$  with  $q$  arbitrary, *J. Combinatorial Th.*, Ser. A, vol. 23, pp. 52–67, 1977.
- [45] E. BANNAI: Codes in bi-partite distance-regular graphs, *J. London Math. Soc.* (2), vol. 16, pp. 197–202, 1977.
- [46] E. BANNAI: Orthogonal polynomials in coding theory and algebraic combinatorics, in: *Orthogonal Polynomials*, Nevai, Ed., pp. 25–53, Kluwer, 1990.

- [47] E. BANNAI and T. ITO: *Algebraic Combinatorics I - Association Schemes*, Benjamin-Cummins, California, 1984.
- [48] I. BÁRÁNY: A short proof of Kneser's conjecture, *J. Combinatorial Th.*, Ser. A, vol. 25, pp. 325–326, 1978.
- [49] A. M. BARG: At the dawn of the theory of codes, *Mathematical Intelligencer*, vol. 15, pp. 20–26, 1993.
- [50] A. M. BARG: Some new NP-complete coding problems, *Problemy Peredachi Informatsii*, vol. 30, No. 3, pp. 23–28, 1994. Translated in: *Problems of Inform. Transm.*, vol. 30, No. 3, pp. 209–214.
- [51] J. P. BARTHÉLEMY, G. D. COHEN and A. C. LOBSTEIN: *Complexité algorithmique et problèmes de communications*, Paris: Masson, 1992.
- [52] L. A. BASSALYGO: New upper bounds for error-correcting codes, *Problemy Peredachi Informatsii*, vol. 1, No. 4, pp. 41–45, 1965 (in Russian). Also in: *Key Papers in the Development of Coding Theory*, Berlekamp, Ed., pp. 244–245, IEEE Press, 1974.
- [53] L. A. BASSALYGO: A generalization of Lloyd's theorem to the case of any alphabet, *Problemy Upravleniya i Teorii Informatsii*, vol. 2, No. 2, pp. 133–137, 1973. Translated in: *Problems of Control and Information Th.*, vol. 2, No. 2, pp. 25–28.
- [54] L. A. BASSALYGO: A necessary condition for the existence of perfect codes in the Lee metric, *Math. Notes*, vol. 15, pp. 178–181, 1974.
- [55] L. A. BASSALYGO, S. I. GELFAND and M. S. PINSKER: Coding for channels with localized errors, *Proc. Fourth Joint Swedish-Soviet Internat. Workshop on Information Theory*, pp. 95–99, Gotland, 1989.
- [56] L. A. BASSALYGO, H. D. L. HOLLMANN, J. KÖRNER and S. LITSYN: Tiling Hamming space with few spheres, Preprint, 1996.
- [57] L. A. BASSALYGO, G. V. ZAITSEV and V. A. ZINOVIEV: On uniformly packed codes, *Problemy Peredachi Informatsii*, vol. 10, No. 1, pp. 9–14, 1974. Translated in: *Problems of Inform. Transm.*, vol. 10, No. 1, pp. 6–9.
- [58] L. A. BASSALYGO and V. A. ZINOVIEV: Remark on uniformly packed codes, *Problemy Peredachi Informatsii*, vol. 13, No. 3, pp. 22–25, 1977. Translated in: *Problems of Inform. Transm.*, vol. 13, No. 3, pp. 178–180.
- [59] L. A. BASSALYGO, V. A. ZINOVIEV and V. K. LEONTIEV: Perfect codes over arbitrary alphabet, *Proc. Third Internat. Symp. on Information Theory*, part II, pp. 23–28, Tallinn, 1973 (in Russian).
- [60] L. A. BASSALYGO, V. A. ZINOVIEV, V. K. LEONTIEV and N. I. FELDMAN: Nonexistence of perfect codes over some composite alphabets, *Problemy Peredachi Informatsii*, vol. 11, No. 3, pp. 3–13, 1975. Translated in: *Problems of Inform. Transm.*, vol. 11, No. 3, pp. 181–189.
- [61] H. BAUER, B. GANTER and F. HERGERT: Algebraic techniques for non-linear codes, *Combinatorica*, vol. 3, pp. 21–33, 1983.

- [62] J. BECK and T. FIALA: “Integer-making” theorems, *Discrete Applied Mathematics*, vol. 3, pp. 1–8, 1981.
- [63] J. BECK and J. H. SPENCER: Balancing matrices with line shifts, *Combinatorica*, vol. 3, pp. 299–304, 1983.
- [64] B. BECKER and H. U. SIMON: How robust is the  $n$ -cube?, *Inform. Comput.*, vol. 77, pp. 162–178, 1988.
- [65] C. BERGE: *Graphes*, Paris: Gauthier-Villars, 1983.
- [66] C. BERGE: *Hypergraphes*, Paris: Gauthier-Villars, 1987.
- [67] T. BERGER: *Rate Distortion Theory*, Englewood Cliffs: Prentice-Hall, 1971.
- [68] E. R. BERLEKAMP: *Algebraic Coding Theory*, New York: McGraw-Hill, 1968.
- [69] E. R. BERLEKAMP, R. J. MCELIECE and H. C. A. van TILBORG: On the inherent intractability of certain coding problems, *IEEE Trans. Inform. Th.*, vol. 24, pp. 384–386, 1978.
- [70] E. R. BERLEKAMP and L. R. WELCH: Weight distribution of the cosets of the (32, 6) Reed-Muller code, *IEEE Trans. Inform. Th.*, vol. 18, pp. 203–207, 1972.
- [71] J. BERNASCONI: Optimization problems and statistical mechanics, *Proc. Workshop on Chaos and Complexity*, pp. 245–259, Singapore, 1988.
- [72] M. R. BEST: On the existence of perfect codes, Report ZN 82/78, Mathematical Centre, Amsterdam, the Netherlands, 1978.
- [73] M. R. BEST: A contribution to the nonexistence of perfect codes, Ph. D. Thesis, University of Amsterdam, the Netherlands, 1982.
- [74] M. R. BEST: Perfect codes hardly exist, *IEEE Trans. Inform. Th.*, vol. 29, pp. 349–351, 1983.
- [75] M. R. BEST, A. E. BROUWER, F. J. MACWILLIAMS, A. M. ODLYZKO and N. J. A. SLOANE: Bounds for binary codes of length less than 25, *IEEE Trans. Inform. Th.*, vol. 24, pp. 81–93, 1978.
- [76] M. BEVERAGGI: Problèmes combinatoires en codage algébrique, Thèse de Doctorat, Université Paris 6, France, 120 pp., 1987.
- [77] M. BEVERAGGI and G. D. COHEN: On the density of best coverings in Hamming spaces, *Lecture Notes in Computer Science*, No. 311, pp. 39–44, Springer-Verlag, 1988.
- [78] M. C. BHANDARI and C. DURAIRAJAN: A note on bounds for  $q$ -ary covering codes, *IEEE Trans. Inform. Th.*, vol. 42, pp. 1640–1642, 1996.
- [79] M. C. BHANDARI and M. S. GARG: Comments on “On the covering radius of codes”, *IEEE Trans. Inform. Th.*, vol. 36, pp. 953–954, 1990.
- [80] M. C. BHANDARI and M. S. GARG: A note on the covering radius of optimum codes, *Discrete Applied Mathematics*, vol. 33, pp. 3–9, 1991.

- [81] N. L. BIGGS: Perfect codes in graphs, *J. Combinatorial Th.*, Ser. B, vol. 15, pp. 289–296, 1973.
- [82] N. L. BIGGS: Perfect codes and distance-transitive graphs, in: *Combinatorics*, McDonough and Mavron, Eds., London Math. Soc., Lecture Notes, No. 13, pp. 1–8, Cambridge University Press, 1974.
- [83] I. F. BLAKE and R. C. MULLIN: *The Mathematical Theory of Coding*, New York: Academic Press, 1975.
- [84] U. BLASS and S. LITSYN: Several new lower bounds for football pool systems, *Ars Combinatoria*, to appear.
- [85] U. BLASS and S. LITSYN: The smallest covering code of length 8 and radius 2 has 12 words, *Ars Combinatoria*, to appear.
- [86] V. M. BLINOVSKII: Bounds for codes in the case of list decoding of finite volume, *Problemy Peredachi Informatsii*, vol. 22, No. 1, pp. 11–25, 1986. Translated in: *Problems of Inform. Transm.*, vol. 22, No. 1, pp. 7–19.
- [87] V. M. BLINOVSKII: Lower asymptotic bound on the number of linear code words in a sphere of given radius in  $F_q^n$ , *Problemy Peredachi Informatsii*, vol. 23, No. 2, pp. 50–53, 1987. Translated in: *Problems of Inform. Transm.*, vol. 23, No. 2, pp. 130–132.
- [88] V. M. BLINOVSKII: Asymptotically exact uniform bounds for spectra of cosets of linear codes, *Problemy Peredachi Informatsii*, vol. 26, No. 1, pp. 99–103, 1990. Translated in: *Problems of Inform. Transm.*, vol. 26, No. 1, pp. 83–86.
- [89] V. M. BLINOVSKII: Covering the Hamming space with sets translated by linear code vectors, *Problemy Peredachi Informatsii*, vol. 26, No. 3, pp. 21–26, 1990. Translated in: *Problems of Inform. Transm.*, vol. 26, No. 3, pp. 196–201.
- [90] A. BLOKHUIS and C. W. H. LAM: More coverings by rook domains, *J. Combinatorial Th.*, Ser. A, vol. 36, pp. 240–244, 1984.
- [91] E. BOMBIERI: On exponential sums in finite fields, *American J. Math.*, vol. 88, pp. 71–105, 1966.
- [92] J. M. BORDEN: Coding for write-unidirectional memories, Unpublished, 1986.
- [93] A. BRACE and D. E. DAYKIN: Sperner type theorems for finite sets, *Proc. British Combinatorial Conf.*, pp. 18–37, 1972.
- [94] A. E. BROUWER: Some lotto numbers from an extension of Turán's theorem, Report 152, Mathematical Centre, Amsterdam, the Netherlands, i+6 pp., 1981.
- [95] A. E. BROUWER, J. B. SHEARER, N. J. A. SLOANE and W. D. SMITH: A new table of constant weight codes, *IEEE Trans. Inform. Th.*, vol. 36, pp. 1334–1380, 1990.
- [96] A. E. BROUWER and T. VERHOEFF: An updated table of minimum-distance bounds for binary linear codes, *IEEE Trans. Inform. Th.*, vol. 39, pp. 662–677, 1993.

- [97] A. E. BROUWER and M. VOORHOEVE: Turan theory and the lotto problem, *Math. Centre Tracts*, vol. 106, pp. 99–105, 1979.
- [98] T. A. BROWN and J. H. SPENCER: Minimization of  $\pm 1$  matrices under line shifts, *Colloq. Math.*, vol. 23, pp. 165–171, 1971.
- [99] R. A. BRUALDI, N. CAI and V. S. PLESS: Orphan structure of the first-order Reed-Muller codes, *Discrete Mathematics*, vol. 102, pp. 239–247, 1992.
- [100] R. A. BRUALDI and V. S. PLESS: Orphans of the first order Reed-Muller codes, *IEEE Trans. Inform. Th.*, vol. 36, pp. 399–401, 1990.
- [101] R. A. BRUALDI and V. S. PLESS: On the covering radius of a code and its subcodes, *Discrete Mathematics*, vol. 83, pp. 189–199, 1990.
- [102] R. A. BRUALDI and V. S. PLESS: On the length of codes with a given covering radius, in: *Coding Theory and Design Theory. Part I: Coding Theory*, Ray-Chaudhuri, Ed., pp. 9–15, New York: Springer-Verlag, 1990.
- [103] R. A. BRUALDI and V. S. PLESS: Subcodes of Hamming codes, *Congressus Numerantium*, vol. 70, pp. 153–158, 1990.
- [104] R. A. BRUALDI and V. S. PLESS: Covering radius, in: *Handbook of Coding Theory*, Brualdi, Huffman and Pless, Eds., Elsevier, to appear.
- [105] R. A. BRUALDI, V. S. PLESS and R. M. WILSON: Short codes with a given covering radius, *IEEE Trans. Inform. Th.*, vol. 35, pp. 99–109, 1989.
- [106] J. BRUCK and M. NAOR: The hardness of decoding linear codes with preprocessing, *IEEE Trans. Inform. Th.*, vol. 36, pp. 381–385, 1990.
- [107] P. B. BUSSCHBACH: Constructive methods to solve problems of  $s$ -surjectivity, conflict resolution, coding in defective memories, Rapport Interne ENST 84-D005, Ecole Nationale Supérieure des Télécommunications, Paris, France, 1984.
- [108] P. B. BUSSCHBACH, M. G. L. GERRETZEN and H. C. A. van TILBORG: On the covering radius of binary linear codes meeting the Griesmer bound, *IEEE Trans. Inform. Th.*, vol. 31, pp. 465–468, 1985.
- [109] A. CÁCERES and O. MORENO: On the estimation of minimum distance of duals of BCH codes, *Congressus Numerantium*, vol. 81, pp. 205–208, 1991.
- [110] A. R. CALDERBANK: Covering radius and the chromatic number of Kneser graphs, *J. Combinatorial Th.*, Ser. A, vol. 54, pp. 129–131, 1990.
- [111] A. R. CALDERBANK: Covering bounds for codes, *J. Combinatorial Th.*, Ser. A, vol. 60, pp. 117–122, 1992.
- [112] A. R. CALDERBANK: Covering machines, *Discrete Mathematics*, vol. 106/107, pp. 105–110, 1992.
- [113] A. R. CALDERBANK, P. C. FISHBURN and A. RABINOVICH: Covering properties of convolutional codes and associated lattices, *IEEE Trans. Inform. Th.*, vol. 41, pp. 732–746, 1995.
- [114] A. R. CALDERBANK and N. J. A. SLOANE: Inequalities for covering codes, *IEEE Trans. Inform. Th.*, vol. 34, pp. 1276–1280, 1988.

- [115] P. J. CAMERON and J. H. van LINT: *Graph Theory, Coding Theory and Block Designs*, London Math. Soc., Lecture Notes, No. 19, Cambridge University Press, 1975.
- [116] P. J. CAMERON, J. A. THAS and S. E. PAYNE: Polarities of generalized hexagons and perfect codes, *Geometriae Dedicata*, vol. 5, pp. 525–528, 1976.
- [117] P. CAMION, B. COURTEAU and P. DELSARTE: On  $r$ -partition designs in Hamming spaces, *Applicable Algebra in Engineering, Communication and Computing*, vol. 2, pp. 147–162, 1992.
- [118] H. T. CAO, R. L. DOUGHERTY and H. JANWA: A [55, 16, 19] binary Goppa code and related codes having large minimum distance, *IEEE Trans. Inform. Theory*, vol. 37, pp. 1432–1433, 1991.
- [119] C. CARLET: A transformation on Boolean functions, its consequences on some problems related to Reed-Muller codes, *Lecture Notes in Computer Science*, No. 514, pp. 42–50, Springer-Verlag, 1991.
- [120] C. CARLET: Partially-bent functions, *Designs, Codes and Cryptography*, vol. 3, pp. 135–145, 1993.
- [121] C. CARLET: Two new classes of bent functions, *Lecture Notes in Computer Science*, No. 765, pp. 77–101, Springer-Verlag, 1994.
- [122] C. CARLET: Partial Spreads généralisés, *Comptes-Rendus de l'Académie des Sciences*, Ser. I, vol. 318, pp. 967–970, 1994.
- [123] C. CARLET: Generalized partial spreads, *IEEE Trans. Inform. Th.*, vol. 41, pp. 1482–1487, 1995.
- [124] C. CARLET and P. GUILLOT: A characterization of binary bent functions, *J. Combinatorial Th.*, Ser. A, vol. 76, pp. 328–335, 1996.
- [125] C. CARLET, J. SEBERRY and X. M. ZHANG: Comments on “Generating and counting binary bent sequences”, *IEEE Trans. Inform. Th.*, vol. 40, p. 600, 1994.
- [126] L. CARLITZ and S. UCHIYAMA: Bounds for exponential sums, *Duke Math. J.*, vol. 24, pp. 37–41, 1957. Also in: *Key Papers in the Development of Coding Theory*, Berlekamp, Ed., pp. 275–276, IEEE Press, 1974.
- [127] W. A. CARNIELLI: Some investigations on covering problems, in: *Collected Papers*, Alas, Da Costa and Höning, Eds., pp. 127–134, São Paulo, Brazil, 1982.
- [128] W. A. CARNIELLI: On covering and coloring problems for rook domains, *Discrete Mathematics*, vol. 57, pp. 9–16, 1985.
- [129] W. A. CARNIELLI: Limites superiores e inferiores para problemas de cobertura em espacios de Hamming, *Proc. 16th Brazilian Mathematical Colloquium*, Rio de Janeiro, 1987.
- [130] W. A. CARNIELLI: Hyper-rook domain inequalities, *Stud. Appl. Math.*, vol. 82, pp. 59–69, 1990.
- [131] V. ČERNÝ: Thermodynamical approach to the traveling salesman problem: an efficient simulation algorithm, *J. Opt. Th. Appl.*, vol. 45, pp. 41–51, 1985.

- [132] I. CHARON, O. HUDRY and A. C. LOBSTEIN: A new method for constructing codes, *Proc. 4th Internat. Workshop on Algebraic and Combinatorial Coding Theory*, pp. 62–65, Novgorod, 1994.
- [133] S. I. CHECHIOTA: On the limit distribution of the distance between a random vector and some binary codes, *Problemy Peredachi Informatsii*, vol. 31, No. 1, pp. 90–98, 1995. Translated in: *Problems of Inform. Transm.*, vol. 31, No. 1, pp. 78–85.
- [134] W. CHEN and I. S. HONKALA: Lower bounds for  $q$ -ary covering codes, *IEEE Trans. Inform. Th.*, vol. 36, pp. 664–671, 1990.
- [135] W. CHEN and D. LI: Lower bounds for multiple covering codes, Preprint.
- [136] L. CHIHARA and D. STANTON: Zeros of generalized Krawtchouk polynomials, *J. Approx. Th.*, vol. 60, No. 1, pp. 43–57, 1990.
- [137] T. S. CHIHARA: *An Introduction to Orthogonal Polynomials*, New York: Gordon and Breach, 1978.
- [138] V. CHVATAL: A greedy heuristic for the set-covering problem, *Mathematics of Operations Research*, vol. 4, pp. 233–235, 1979.
- [139] W. E. CLARK, L. A. DUNNING and D. G. ROGERS: Binary set functions and parity check matrices, *Discrete Mathematics*, vol. 80, pp. 249–265, 1990.
- [140] W. E. CLARK and J. PEDERSEN: Sum-free sets in vector spaces over  $GF(2)$ , *J. Combinatorial Th.*, Ser. A, vol. 61, pp. 222–229, 1992.
- [141] R. F. CLAYTON: Multiple packings and coverings in algebraic coding theory, Ph. D. Thesis, University of California in Los Angeles, United States, 62 pp., 1987.
- [142] R. F. CLAYTON: Perfect multiple coverings in metric schemes, in: *Coding Theory and Design Theory. Part I: Coding Theory*, Ray-Chaudhuri, Ed., pp. 51–64, New York: Springer-Verlag, 1990.
- [143] G. D. COHEN: A nonconstructive upper bound on covering radius, *IEEE Trans. Inform. Th.*, vol. 29, pp. 352–353, 1983.
- [144] G. D. COHEN: Non-linear covering codes: a few results and conjectures, *Lecture Notes in Computer Science*, No. 356, pp. 225–229, Springer-Verlag, 1989.
- [145] G. D. COHEN: Covering radius and writing on memories, *Lecture Notes in Computer Science*, No. 508, pp. 1–10, Springer-Verlag, 1990.
- [146] G. D. COHEN: Applications of coding theory to communication combinatorial problems, *Discrete Mathematics*, vol. 83, pp. 237–248, 1990.
- [147] G. D. COHEN, J. L. DORNSTETTER and P. GODLEWSKI: *Codes correcteurs d'erreurs*, Paris: Masson, 1992.
- [148] G. D. COHEN and P. FRANKL: On tilings of the binary vector space, *Discrete Mathematics*, vol. 31, pp. 271–277, 1980.
- [149] G. D. COHEN and P. FRANKL: On cliques and partitions in Hamming spaces, *Annals of Discrete Mathematics*, vol. 17, pp. 211–217, 1983.

- [150] G. D. COHEN and P. FRANKL: On generalized perfect codes and Steiner systems, *Annals of Discrete Mathematics*, vol. 18, pp. 197–200, 1983.
- [151] G. D. COHEN and P. FRANKL: Good coverings of Hamming spaces with spheres, *Discrete Mathematics*, vol. 56, pp. 125–131, 1985.
- [152] G. D. COHEN and P. GODLEWSKI: Some cryptographic aspects of wom-codes, *Lecture Notes in Computer Science*, No. 218, pp. 458–467, Springer-Verlag, 1986.
- [153] G. D. COHEN, P. GODLEWSKI and F. MERKX: Linear binary codes for write-once memories, *IEEE Trans. Inform. Th.*, vol. 32, pp. 697–700, 1986.
- [154] G. D. COHEN, I. S. HONKALA and S. LITSYN: On weighted coverings and packings with diameter one, *CISM Courses and Lectures*, No. 339, pp. 43–49, Springer-Verlag, 1993.
- [155] G. D. COHEN, I. S. HONKALA, S. LITSYN and H. F. MATTSON, Jr.: Weighted coverings and packings, *IEEE Trans. Inform. Th.*, vol. 41, pp. 1856–1867, 1995.
- [156] G. D. COHEN, M. G. KARPOVSKY, H. F. MATTSON, Jr., and J. R. SCHATZ: Covering radius — survey and recent results, *IEEE Trans. Inform. Th.*, vol. 31, pp. 328–343, 1985.
- [157] G. D. COHEN and S. LITSYN: On the covering radius of Reed-Muller codes, *Discrete Mathematics*, vol. 106/107, pp. 147–155, 1992.
- [158] G. D. COHEN, S. LITSYN, A. C. LOBSTEIN and H. F. MATTSON, Jr.: Covering radius 1985–1994, *Applicable Algebra in Engineering, Communication and Computing*, special issue, to appear.
- [159] G. D. COHEN, S. LITSYN and H. F. MATTSON, Jr.: On perfect weighted coverings with small radius, *Lecture Notes in Computer Science*, No. 573, pp. 32–41, Springer-Verlag, 1992.
- [160] G. D. COHEN, S. LITSYN and H. F. MATTSON, Jr.: Binary perfect weighted coverings, I, The linear case, in: *Sequences II*, Capocelli, DeSantis and Vaccaro, Eds., pp. 36–51, Springer-Verlag, 1993.
- [161] G. D. COHEN, I. S. HONKALA, S. LITSYN and P. SOLÉ: Long packing and covering codes, *IEEE Trans. Inform. Th.*, submitted.
- [162] G. D. COHEN, S. LITSYN, A. VARDY and G. ZÉMOR: Tilings of binary spaces, *SIAM J. Discrete Mathematics*, vol. 9, pp. 393–412, 1996.
- [163] G. D. COHEN, S. LITSYN and G. ZÉMOR: Upper bounds on generalized distances, *IEEE Trans. Inform. Th.*, vol. 40, pp. 2090–2092, 1994.
- [164] G. D. COHEN, S. LITSYN and G. ZÉMOR: On greedy algorithms in coding theory, *IEEE Trans. Inform. Th.*, vol. 42, pp. 2053–2057, 1996.
- [165] G. D. COHEN, A. C. LOBSTEIN and N. J. A. SLOANE: Further results on the covering radius of codes, *IEEE Trans. Inform. Th.*, vol. 32, pp. 680–694, 1986.

- [166] G. D. COHEN, A. C. LOBSTEIN and N. J. A. SLOANE: On a conjecture concerning coverings of Hamming space, *Lecture Notes in Computer Science*, No. 228, pp. 79–89, Springer-Verlag, 1986.
- [167] G. D. COHEN and B. MONTARON: Empilements parfaits de boules dans les espaces vectoriels binaires, *Comptes-Rendus de l'Académie des Sciences, Ser. A*, vol. 288, pp. 578–582, 1979.
- [168] G. D. COHEN, J. RIFÁ and G. ZÉMOR: On the classification of linear binary uniquely decodable codes, Preprint, 1996.
- [169] G. D. COHEN and G. SIMONYI: Coding for write-unidirectional memories and conflict resolution, *Discrete Applied Mathematics*, vol. 24, pp. 103–114, 1989.
- [170] G. D. COHEN and G. ZÉMOR: An application of combinatorial group theory to coding, *Ars Combinatoria*, vol. 23-A, pp. 81–89, 1987.
- [171] G. D. COHEN and G. ZÉMOR: Write-isolated memories, *Discrete Mathematics*, vol. 114, pp. 105–113, 1993.
- [172] G. D. COHEN and G. ZÉMOR: Intersecting codes and independent families, *IEEE Trans. Inform. Th.*, vol. 40, pp. 1872–1881, 1994.
- [173] S. D. COHEN: The length of primitive BCH codes with minimal covering radius, Preprint, 1996.
- [174] M. COHN: On the channel capacity of read/write isolated memory, *Discrete Applied Mathematics*, vol. 56, pp. 1–8, 1995.
- [175] J. H. CONWAY and N. J. A. SLOANE: *Sphere Packings, Lattices, and Groups*, New York: Springer-Verlag, 1988.
- [176] T. M. COVER and J. A. THOMAS: *Elements of Information Theory*, New York: Wiley, 1991.
- [177] I. CSISZÁR and J. KÖRNER: *Information Theory: Coding Theorems for Discrete Memoryless Systems*, New York: Academic Press, 1981.
- [178] D. M. CVETKOVIĆ and J. H. van LINT: An elementary proof of Lloyd's theorem, *Proc. Kon. Ned. Akad. v. Wetensch. (a)*, vol. 80, pp. 6–10, 1977.
- [179] A. A. DAVYDOV: Construction of linear covering codes, *Problemy Peredachi Informatsii*, vol. 26, No. 4, pp. 38–55, 1990. Translated in: *Problems of Inform. Transm.*, vol. 26, No. 4, pp. 317–331.
- [180] A. A. DAVYDOV: Constructions and families of  $q$ -ary linear covering codes and saturated sets of points in projective geometry, *Proc. Fifth Joint Soviet-Swedish Internat. Workshop on Information Theory*, pp. 46–49, Moscow, 1991.
- [181] A. A. DAVYDOV: Constructions of codes with covering radius 2, *Lecture Notes in Computer Science*, No. 573, pp. 23–31, Springer-Verlag, 1992.
- [182] A. A. DAVYDOV: On constructions of nonlinear covering codes, *Proc. Seventh Joint Swedish-Russian Internat. Workshop on Information Theory*, pp. 67–71, St-Petersburg, 1995.

- [183] A. A. DAVYDOV: Constructions and families of covering codes and saturated sets of points in projective geometry, *IEEE Trans. Inform. Th.*, vol. 41, pp. 2071–2080, 1995.
- [184] A. A. DAVYDOV: On nonbinary linear codes with covering radius two, *Proc. 5th Internat. Workshop on Algebraic and Combinatorial Coding Theory*, pp. 105–110, Sozopol, 1996.
- [185] A. A. DAVYDOV: Constructions of nonlinear covering codes, *IEEE Trans. Inform. Th.*, submitted.
- [186] A. A. DAVYDOV and A. Y. DROZHINA-LABINSKAYA: Binary linear codes with covering radii 3 and 4, *Proc. 2nd Internat. Workshop on Algebraic and Combinatorial Coding Theory*, pp. 56–57, Leningrad, 1990.
- [187] A. A. DAVYDOV and A. Y. DROZHINA-LABINSKAYA: Table and families of short  $[n, n - r]$  codes with a given covering radius  $R$ , Preprint, 1990.
- [188] A. A. DAVYDOV and A. Y. DROZHINA-LABINSKAYA: Constructions of binary linear covering codes, *Proc. 3rd Internat. Workshop on Algebraic and Combinatorial Coding Theory*, pp. 51–54, Voneshta Voda, 1992.
- [189] A. A. DAVYDOV and A. Y. DROZHINA-LABINSKAYA: Constructions, families, and tables of binary linear covering codes, *IEEE Trans. Inform. Th.*, vol. 40, pp. 1270–1279, 1994.
- [190] A. A. DAVYDOV and L. M. TOMBAK: Quasiperfect linear binary codes with distance 4 and complete caps in projective geometry, *Problemy Peredachi Informatsii*, vol. 25, No. 4, pp. 11–23, 1989. Translated in: *Problems of Inform. Transm.*, vol. 25, No. 4, pp. 265–275.
- [191] P. DELIGNE: La conjecture de Weil I, Institut Hautes Etudes Sci., *Publ. Math.*, vol. 43, pp. 273–307, 1974.
- [192] C. DELORME and P. SOLÉ: Diameter, covering index, covering radius and eigenvalues, *European J. Combinatorics*, vol. 12, pp. 95–108, 1991.
- [193] P. DELSARTE: An algebraic approach to the association schemes of coding theory, Philips Research Reports Supplements, No. 10, 1973.
- [194] P. DELSARTE: Four fundamental parameters of a code and their combinatorial significance, *Information and Control*, vol. 23, pp. 407–438, 1973.
- [195] P. DELSARTE and J.-M. GOETHALS: Unrestricted codes with the Golay parameters are unique, *Discrete Mathematics*, vol. 12, pp. 211–224, 1975.
- [196] P. DELSARTE and P. PIRET: Do most binary linear codes achieve the Goblick bound on the covering radius?, *IEEE Trans. Inform. Th.*, vol. 32, pp. 826–828, 1986.
- [197] M. DEZA: The effectiveness of noise correction or detection, *Problemy Peredachi Informatsii*, vol. 1, No. 3, pp. 29–39, 1965 (in Russian).
- [198] M. DEZA and F. HOFFMAN: Some results related to generalized Varshamov–Gilbert bound, *IEEE Trans. Inform. Th.*, vol. 23, pp. 517–518, 1977.
- [199] M. DEZA, M. G. KARPOVSKY and V. MILMAN: Codes correcting an arbitrary set of errors, *Revue CETHEDEC*, vol. 66, pp. 65–76, 1981.

- [200] P. DIACONIS and R. L. GRAHAM: The Radon transform on  $\mathbf{Z}_2^k$ , *Pacific J. Math.*, vol. 118, pp. 323–345, 1985.
- [201] J. F. DILLON: A survey of bent functions, *NCA Tech. J.*, pp. 191–215, 1972.
- [202] S. M. DODUNEKOV: The optimal double-error-correcting codes of Zetterberg and Dumer-Zinoviev are quasiperfect, *Comptes-Rendus de l'Académie Bulgare des Sciences*, vol. 38, pp. 1121–1123, 1985.
- [203] S. M. DODUNEKOV: Some quasi-perfect double error correcting codes, *Problemy Upravleniya i Teorii Informatsii*, vol. 15, No. 5, pp. 367–375, 1986. Translated in: *Problems of Control and Information Th.*, vol. 15, No. 5.
- [204] S. M. DODUNEKOV: Griesmer codes with maximum covering radius, *Problemy Peredachi Informatsii*, vol. 23, No. 4, pp. 110–113, 1987. Translated in: *Problems of Inform. Transm.*, vol. 23, No. 4, pp. 344–346.
- [205] S. M. DODUNEKOV and S. B. ENCHEVA: Uniqueness of some linear sub-codes of the extended binary Golay code, *Problemy Peredachi Informatsii*, vol. 29, No. 1, pp. 45–51, 1993. Translated in: *Problems of Inform. Transm.*, vol. 29, No. 1, pp. 38–43.
- [206] S. M. DODUNEKOV, K. N. MANEV and V. D. TONCHEV: On the covering radius of binary  $[14, 6]$  codes containing the all-one vector, *IEEE Trans. Inform. Th.*, vol. 34, pp. 591–593, 1988.
- [207] S. M. DODUNEKOV and N. L. MANEV: An improvement of the Griesmer bound for some small minimum distances, *Discrete Applied Mathematics*, vol. 12, pp. 103–114, 1985.
- [208] D. DOLEV, D. MAIER, H. MAIRSON and J. ULLMAN: Correcting faults in write-once memory, *Assoc. for Computing Machinery*, pp. 225–229, 1984.
- [209] R. L. DOUGHERTY and H. JANWA: Covering radius computations for binary cyclic codes, *Mathematics of Computation*, vol. 57, pp. 415–434, 1991.
- [210] D. E. DOWNIE and N. J. A. SLOANE: The covering radius of cyclic codes of length up to 31, *IEEE Trans. Inform. Th.*, vol. 31, pp. 446–447, 1985.
- [211] I. I. DUMER: Asymptotically optimal codes correcting memory defects of fixed multiplicity, *Problemy Peredachi Informatsii*, vol. 25, No. 4, pp. 3–10, 1989. Translated in: *Problems of Inform. Transm.*, vol. 25, No. 4, pp. 259–265.
- [212] I. I. DUMER: Concatenated codes and their generalizations, in: *Handbook of Coding Theory*, Brualdi, Huffman and Pless, Eds., Elsevier, to appear.
- [213] A. DÜR: On the covering radius of Reed-Solomon codes, *Discrete Mathematics*, vol. 126, pp. 99–105, 1994.
- [214] I. DVORÁKOVÁ-RULÍKOVÁ: Perfect codes in regular graphs, *Commentationes Mathematicae Universitatis Carolinae*, No. 29, pp. 79–83, 1988.
- [215] C. van EIJL, G. D. COHEN and G. ZÉMOR: Error-correction for WIMs and WUMs, *Lecture Notes in Computer Science*, No. 539, pp. 159–170, Springer-Verlag, 1991.

- [216] A. A. EL GAMAL, L. A. HEMACHANDRA, I. SHPERLING and V. K. WEI: Using simulated annealing to design good codes, *IEEE Trans. Inform. Th.*, vol. 33, pp. 116–123, 1987.
- [217] M. H. EL-ZAHAR and M. K. KHAIRAT: On the weight distribution of the coset leaders of the first-order Reed-Muller code, *IEEE Trans. Inform. Th.*, vol. 33, pp. 744–747, 1987.
- [218] S. B. ENCHEVA: On binary linear codes which satisfy the two-way chain condition, *IEEE Trans. Inform. Th.*, vol. 42, pp. 1038–1047, 1996.
- [219] G. ETIENNE: Perfect codes and regular partitions in graphs and groups, *European J. Combinatorics*, vol. 8, pp. 139–144, 1987.
- [220] T. ETZION: On the nonexistence of perfect codes in the Johnson scheme, *SIAM J. Discrete Mathematics*, vol. 9, pp. 201–209, 1996.
- [221] T. ETZION: Nonequivalent  $q$ -ary perfect codes, *SIAM J. Discrete Mathematics*, vol. 9, pp. 413–423, 1996.
- [222] T. ETZION and G. GREENBERG: Constructions of perfect mixed codes and other covering codes, *IEEE Trans. Inform. Th.*, vol. 39, pp. 209–214, 1993.
- [223] T. ETZION, G. GREENBERG and I. S. HONKALA: Normal and abnormal codes, *IEEE Trans. Inform. Th.*, vol. 39, pp. 1453–1456, 1993.
- [224] T. ETZION and A. VARDY: Perfect binary codes: constructions, properties, and enumeration, *IEEE Trans. Inform. Th.*, vol. 40, pp. 754–763, 1994.
- [225] T. ETZION and A. VARDY: On perfect codes and tilings: problems and solutions, Preprint, 1996.
- [226] T. ETZION, V. K. WEI and Z. ZHANG: Bounds on the sizes of constant weight covering codes, *Designs, Codes and Cryptography*, vol. 5, pp. 217–239, 1995.
- [227] E. FACHINI and J. KÖRNER: Tight packings of Hamming spheres, *J. Combinatorial Th.*, Ser. A, vol. 76, pp. 292–294, 1996.
- [228] G. FANG: Binary block codes for correcting asymmetric or unidirectional errors, Ph. D. Thesis, Eindhoven University of Technology, the Netherlands, 97 pp., 1993.
- [229] G. FANG, H. C. A. van TILBORG and F. W. SUN: Weakly perfect binary block codes for correcting asymmetric errors, *Proc. Internat. Symp. on Communications*, pp. 57–60, Tainan, Taiwan, 1991.
- [230] G. FANG, H. C. A. van TILBORG and F. W. SUN: On uniformly weakly perfect codes for correcting asymmetric errors; some bounds and constructions, *Collection of Papers Dedicated to the Memory of David Gevorkian*, to appear.
- [231] G. FANG, H. C. A. van TILBORG, F. W. SUN and I. S. HONKALA: Some features of binary block codes for correcting asymmetric errors, *Lecture Notes in Computer Science*, No. 673, pp. 105–120, Springer-Verlag, 1993.
- [232] G. FAZEKAS and V. I. LEVENSHTEIN: On upper bounds for code distance and covering radius of designs in polynomial metric spaces, *Proc. Fifth Joint Soviet-Swedish Internat. Workshop on Information Theory*, pp. 65–68, Moscow, 1991.

- [233] G. FAZEKAS and V. I. LEVENSHTEIN: On upper bounds for code distance and covering radius of designs in polynomial metric spaces, *J. Combinatorial Th.*, Ser. A, vol. 70, pp. 267–288, 1995.
- [234] L. FEJES TÓTH: *Lagerungen in der Ebene, auf der Kugel und in Raum*, 2nd ed., Springer-Verlag, 1972.
- [235] M. R. FELLOWS: Encoding graphs in graphs, Ph. D. Thesis, University of California, San Diego, United States, 112 pp., 1985.
- [236] M. R. FELLOWS: Data structures for reluctant media, Internal Report CS-86-144, Washington State University, United States, 1986.
- [237] H. FERNANDES and E. RECHTSCHAFFEN: The football pool problem for 7 and 8 matches, *J. Combinatorial Th.*, Ser. A, vol. 35, pp. 109–114, 1983.
- [238] P. C. FISHBURN and N. J. A. SLOANE: The solution to Berlekamp’s switching game, *Discrete Mathematics*, vol. 74, pp. 263–290, 1989.
- [239] G. D. FORNEY, Jr.: *Concatenated Codes*, Cambridge, MA: MIT Press, 1966.
- [240] M. K. FORT, Jr., and G. A. HEDLUND: Minimal coverings of pairs by triples, *Pacific J. Math.*, vol. 8, pp. 709–719, 1958.
- [241] M. FRANCES and A. LITMAN: On covering problems of codes, Technical Report No. 827, Technion, Haifa, Israel, 8 pp., 1994.
- [242] G. FREIMAN, E. LIPKIN and L. LEVITIN: A polynomial algorithm for constructing families of  $k$ -independent sets, *Discrete Mathematics*, vol. 70, pp. 137–147, 1988.
- [243] Z. FÜREDI, G. J. SZÉKELY and Z. ZUBOR: On the lottery problem, *J. Combinatorial Designs*, submitted.
- [244] E. M. GABIDULIN, A. A. DAVYDOV and L. M. TOMBAK: Codes of covering radius 2 and other new covering codes, *Proc. 10th All-Union Symp. on Redundancy Problems in Information Systems*, part I, pp. 14–17, Leningrad, 1989 (in Russian).
- [245] E. M. GABIDULIN, A. A. DAVYDOV and L. M. TOMBAK: Linear codes with covering radius 2 and other new covering codes, *IEEE Trans. Inform. Th.*, vol. 37, pp. 219–224, 1991.
- [246] R. G. GALLAGER: *Information Theory and Reliable Communication*, New York: Wiley, 1968.
- [247] M. R. GAREY and D. S. JOHNSON: *Computers and Intractability, a Guide to the Theory of NP-Completeness*, New York: Freeman, 1979.
- [248] L. GARGANO, J. KÖRNER and U. VACCARO: Sperner capacities, *Graphs and Combinatorics*, vol. 9, pp. 31–46, 1993.
- [249] L. GARGANO, J. KÖRNER and U. VACCARO: Capacities: from information theory to extremal set theory, *J. Combinatorial Th.*, Ser. A, vol. 68, pp. 296–316, 1994.
- [250] E. N. GILBERT: A comparison of signalling alphabets, *Bell Syst. Tech. J.*, vol. 31, pp. 504–522, 1952.

- [251] T. J. GOBLICK, Jr.: Coding for a discrete information source with a distortion measure, Ph. D. Thesis, Massachusetts Institute of Technology, Cambridge, United States, 1962.
- [252] P. GODLEWSKI: Wom-codes construits à partir des codes de Hamming, *Discrete Mathematics*, vol. 65, pp. 237–243, 1987.
- [253] P. GODLEWSKI and G. D. COHEN: Authorized writing for “write-once” memories, *Lecture Notes in Computer Science*, No. 219, pp. 111–115, Springer-Verlag, 1986.
- [254] J.-M. GOETHALS and S. L. SNOVER: Nearly perfect binary codes, *Discrete Mathematics*, vol. 3, pp. 65–88, 1972.
- [255] J.-M. GOETHALS and H. C. A. van TILBORG: Uniformly packed codes, *Philips Research Reports*, vol. 30, pp. 9–36, 1975.
- [256] M. J. E. GOLAY: Notes on digital coding, *Proc. IEEE*, vol. 37, p. 657, 1949. Also in: *Key Papers in the Development of Coding Theory*, Berlekamp, Ed., p. 13, IEEE Press, 1974.
- [257] S. W. GOLOMB and E. C. POSNER: Rook domains, Latin squares, affine planes, and error-distributing codes, *IEEE Trans. Inform. Th.*, vol. 10, pp. 196–208, 1964.
- [258] S. W. GOLOMB and L. R. WELCH: Algebraic coding and the Lee metric, in: *Error Correcting Codes*, Mann, Ed., pp. 175–194, New York: Wiley, 1968.
- [259] S. W. GOLOMB and L. R. WELCH: Perfect codes in the Lee metric and the packing of polyominoes, *SIAM J. Applied Mathematics*, vol. 18, pp. 302–317, 1970.
- [260] D. M. GORDON: Perfect multiple error-correcting arithmetic codes, *Mathematics of Computation*, vol. 49, pp. 621–633, 1987.
- [261] D. M. GORDON, G. KUPERBERG and O. PATASHNIK: New constructions for covering designs, *J. Combinatorial Designs*, vol. 3, pp. 269–284, 1995.
- [262] D. M. GORDON, O. PATASHNIK, G. KUPERBERG and J. H. SPENCER: Asymptotically optimal covering designs, *J. Combinatorial Th.*, Ser. A, vol. 75, pp. 270–280, 1996.
- [263] Y. GORDON and H. S. WITSENHAUSEN: On extensions of the Gale-Berlekamp switching problem and constants of  $\ell_p$ -spaces, *Israel J. Math.*, vol. 11, pp. 216–229, 1972.
- [264] D. GORENSTEIN, W. W. PETERSON and N. ZIERLER: Two-error correcting Bose-Chaudhury codes are quasi-perfect, *Information and Control*, vol. 3, pp. 291–294, 1960.
- [265] R. L. GRAHAM and N. J. A. SLOANE: On the covering radius of codes, *IEEE Trans. Inform. Th.*, vol. 31, pp. 385–401, 1985.
- [266] J. H. GRIESMER: A bound for error-correcting codes, *IBM J. Res. Develop.*, vol. 4, pp. 532–542, 1960.
- [267] M. GUNDLACH: On codes with distinct protective radii, *Atti Sem. Mat. Fis. Univ. Modena*, vol. 32, pp. 372–396, 1983.

- [268] M. GUNDLACH: On strongly tactical codes, *Lecture Notes in Computer Science*, No. 229, pp. 17–26, Springer-Verlag, 1986.
- [269] L. HABSIEGER: Lower bounds for  $q$ -ary coverings by spheres of radius 1, *J. Combinatorial Th.*, Ser. A, vol. 67, pp. 199–222, 1994.
- [270] L. HABSIEGER: Some new lower bounds for ternary covering codes, *Electronic J. Combinatorics*, <http://ejc.math.gatech.edu:8080/> Journal/ Volume 3/ festschrift.html, 1996.
- [271] L. HABSIEGER: A new lower bound for the football pool problem for 7 matches, *J. Th. des Nombres de Bordeaux*, to appear.
- [272] L. HABSIEGER: Binary codes with covering radius one: some new lower bounds, *Discrete Mathematics*, to appear.
- [273] L. HABSIEGER and D. STANTON: More zeros of Krawtchouk polynomials, *Graphs and Combinatorics*, vol. 9, pp. 163–172, 1993.
- [274] M. W. van der HAM: Simulated annealing applied in coding theory, Master's Thesis, Eindhoven University of Technology, the Netherlands, 50 pp., 1988.
- [275] H. O. HÄMÄLÄINEN, I. S. HONKALA, M. K. KAIKKONEN and S. LITSYN: Bounds for binary multiple covering codes, *Designs, Codes and Cryptography*, vol. 3, pp. 251–275, 1993.
- [276] H. O. HÄMÄLÄINEN, I. S. HONKALA, S. LITSYN and P. R. J. ÖSTERGÅRD: Bounds for binary codes that are multiple coverings of the farthest-off points, *SIAM J. Discrete Mathematics*, vol. 8, pp. 196–207, 1995.
- [277] H. O. HÄMÄLÄINEN, I. S. HONKALA, S. LITSYN and P. R. J. ÖSTERGÅRD: Football pools - a game for mathematicians, *American Mathematical Monthly*, vol. 102, pp. 579–588, 1995.
- [278] H. O. HÄMÄLÄINEN and S. RANKINEN: Upper bounds for football pool problems and mixed covering codes, *J. Combinatorial Th.*, Ser. A, vol. 56, pp. 84–95, 1991.
- [279] R. W. HAMMING: Error detecting and error correcting codes, *Bell Syst. Tech. J.*, vol. 29, pp. 147–160, 1950. Also in: *Key Papers in the Development of Coding Theory*, Berlekamp, Ed., pp. 9–12, IEEE Press, 1974.
- [280] P. HAMMOND: Nearly perfect codes in distance-regular graphs, *Discrete Mathematics*, vol. 14, pp. 41–56, 1976.
- [281] P. HAMMOND:  $q$ -coverings, codes, and line graphs, *J. Combinatorial Th.*, Ser. B, vol. 30, pp. 32–35, 1981.
- [282] P. HAMMOND: On the non-existence of perfect and nearly perfect codes, *Discrete Mathematics*, vol. 39, pp. 105–109, 1982.
- [283] P. HAMMOND and D. H. SMITH: Perfect codes in the graphs  $O_k$ , *J. Combinatorial Th.*, Ser. B, vol. 19, pp. 239–255, 1975.
- [284] H. HANANI, D. ORNSTEIN and V. T. SÓS: On the lottery problem, *Magyar Tud. Akad. Mat. Kutató Int. Közl.*, vol. 9, pp. 155–158, 1964.

- [285] A. HARTMAN, W. H. MILLS and R. C. MULLIN: Covering triples by quadruples: an asymptotic solution, *J. Combinatorial Th.*, Ser. A, vol. 41, pp. 117–138, 1986.
- [286] A. HARTMAN, R. C. MULLIN and D. R. STINSON: Exact covering configurations and Steiner systems, *J. London Math. Soc.* (2), vol. 25, pp. 193–200, 1982.
- [287] O. HEDEN: Perfect codes in antipodal distance-transitive graphs, *Math. Scand.*, vol. 35, pp. 29–37, 1974.
- [288] O. HEDEN: A generalized Lloyd theorem and mixed perfect codes, *Math. Scand.*, vol. 37, pp. 13–26, 1975.
- [289] O. HEDEN: A new construction of group and nongroup perfect codes, *Information and Control*, vol. 34, pp. 314–323, 1977.
- [290] O. HEDEN: A binary perfect code of length 15 and codimension 0, *Designs, Codes and Cryptography*, vol. 4, pp. 213–220, 1994.
- [291] C. HEEGARD: Partitioned linear block codes for computer memory with “stuck-at” defects, *IEEE Trans. Inform. Th.*, vol. 29, pp. 831–842, 1983.
- [292] C. HEEGARD and A. A. EL GAMAL: On the capacity of computer memory with defects, *IEEE Trans. Inform. Th.*, vol. 29, pp. 731–739, 1983.
- [293] H. J. HELGERT and R. D. STINAFF: Minimum-distance bounds for binary linear codes, *IEEE Trans. Inform. Th.*, vol. 19, pp. 344–356, 1973.
- [294] H. J. HELGERT and R. D. STINAFF: Shortened BCH codes, *IEEE Trans. Inform. Th.*, vol. 19, pp. 818–820, 1973.
- [295] T. HELLESETH: All binary 3-error-correcting BCH codes of length  $2^m - 1$  have covering radius 5, *IEEE Trans. Inform. Th.*, vol. 24, pp. 257–258, 1978.
- [296] T. HELLESETH: No primitive binary  $t$ -error correcting BCH code with  $t > 2$  is quasi-perfect, *IEEE Trans. Inform. Th.*, vol. 25, pp. 361–362, 1979.
- [297] T. HELLESETH: On the covering radius of cyclic linear codes and arithmetic codes, *Discrete Applied Mathematics*, vol. 11, pp. 157–173, 1985.
- [298] T. HELLESETH and T. KLØVE: The Newton radius of codes, *IEEE Trans. Inform. Th.*, submitted.
- [299] T. HELLESETH, T. KLØVE and V. I. LEVENSHTEIN: The Newton radius of equidistant codes, *Proc. Internat. Symp. on Information Theory and its Applications*, vol. 2, pp. 721–722, Victoria, 1996.
- [300] T. HELLESETH, T. KLØVE and J. MYKKELTVEIT: On the covering radius of binary codes, *IEEE Trans. Inform. Th.*, vol. 24, pp. 627–628, 1978.
- [301] T. HELLESETH and H. F. MATTSON, Jr.: On the cosets of the simplex code, *Discrete Mathematics*, vol. 56, pp. 169–189, 1985.
- [302] M. HERZOG and J. SCHÖNHEIM: Linear and nonlinear single-error correcting perfect mixed codes, *Information and Control*, vol. 18, pp. 364–368, 1971.

- [303] M. HERZOG and J. SCHÖNHEIM: Group partition, factorization and the vector covering problem, *Canad. Math. Bull.*, vol. 15, pp. 207–214, 1972.
- [304] R. HILL: Caps and codes, *Discrete Mathematics*, vol. 22, pp. 111–137, 1978.
- [305] J. W. P. HIRSCHFELD: *Projective Geometries over Finite Fields*, Oxford: Clarendon Press, 1979.
- [306] Y. HONG: On the nonexistence of unknown perfect 6- and 8-codes in Hamming schemes  $H(n, q)$  with  $q$  arbitrary, *Osaka J. Math.*, vol. 21, pp. 687–700, 1984.
- [307] Y. HONG: On the nonexistence of nontrivial perfect  $e$ -codes and tight  $2e$ -designs in Hamming schemes  $H(N, q)$  with  $e \geq 3$  and  $q \geq 3$ , *Graphs and Combinatorics*, vol. 2, pp. 145–164, 1986.
- [308] I. S. HONKALA: On the intersections and unions of Hamming spheres, in: *The Very Knowledge of Coding*, Laakso and Salomaa, Eds., pp. 70–81, Turku, Finland, 1987.
- [309] I. S. HONKALA: Lower bounds for binary covering codes, *IEEE Trans. Inform. Th.*, vol. 34, pp. 326–329, 1988.
- [310] I. S. HONKALA: Combinatorial bounds for binary constant weight and covering codes, Ph. D. Thesis, University of Turku, Finland, 108 pp., 1989.
- [311] I. S. HONKALA: On the normality of codes with covering radius one, *Proc. Fourth Joint Swedish-Soviet Internat. Workshop on Information Theory*, pp. 223–226, Gotland, 1989.
- [312] I. S. HONKALA: Modified bounds for covering codes, *IEEE Trans. Inform. Th.*, vol. 37, pp. 351–365, 1991.
- [313] I. S. HONKALA: On  $(k, t)$ -subnormal covering codes, *IEEE Trans. Inform. Th.*, vol. 37, pp. 1203–1206, 1991.
- [314] I. S. HONKALA: All binary codes with covering radius one are subnormal, *Discrete Mathematics*, vol. 94, pp. 229–232, 1991.
- [315] I. S. HONKALA: On lengthening of covering codes, *Discrete Mathematics*, vol. 106/107, pp. 291–295, 1992.
- [316] I. S. HONKALA: A Graham-Sloane type construction for  $s$ -surjective matrices, *J. Algebraic Combinatorics*, vol. 1, pp. 347–351, 1992.
- [317] I. S. HONKALA: A lower bound on binary codes with covering radius one, *Lecture Notes in Computer Science*, No. 781, pp. 34–37, Springer-Verlag, 1994.
- [318] I. S. HONKALA: On the normality of multiple covering codes, *Discrete Mathematics*, vol. 125, pp. 229–239, 1994.
- [319] I. S. HONKALA: On  $(q, 1)$ -subnormal  $q$ -ary covering codes, *Discrete Applied Mathematics*, vol. 52, pp. 213–221, 1994.
- [320] I. S. HONKALA: A new lower bound on codes with covering radius one, *Proc. Internat. Symp. on Information Theory and its Applications*, vol. 1, pp. 39–41, Sydney, 1994.

- [321] I. S. HONKALA: Combinatorial lower bounds on binary codes with covering radius one, *Ars Combinatoria*, to appear.
- [322] I. S. HONKALA and H. O. HÄMÄLÄINEN: A new construction for covering codes, *IEEE Trans. Inform. Th.*, vol. 34, pp. 1343–1344, 1988.
- [323] I. S. HONKALA and H. O. HÄMÄLÄINEN: Bounds for abnormal binary codes with covering radius one, *IEEE Trans. Inform. Th.*, vol. 37, pp. 372–375, 1991.
- [324] I. S. HONKALA, Y. KAIPAINEN and A. TIETÄVÄINEN: Long binary narrow-sense BCH codes are normal, *Applicable Algebra in Engineering, Communication and Computing*, to appear.
- [325] I. S. HONKALA, T. LAIHONEN and S. LITSYN: On covering radius and discrete Chebyshev polynomials, Preprint, 1996.
- [326] I. S. HONKALA and S. LITSYN: Generalizations of the covering radius problem in coding theory, *Bull. Institute of Combinatorics and its Applications*, vol. 17, pp. 39–46, 1996.
- [327] I. S. HONKALA, S. LITSYN and A. TIETÄVÄINEN: On algebraic methods in covering radius problems, *Lecture Notes in Computer Science*, No. 948, pp. 21–32, Springer-Verlag, 1995.
- [328] I. S. HONKALA and P. R. J. ÖSTERGÅRD: Code design, in: *Local Search Algorithms*, Aarts and Lenstra, Eds., Chapter 13, Wiley, to appear.
- [329] I. S. HONKALA and A. TIETÄVÄINEN: Codes and number theory, in: *Handbook of Coding Theory*, Brualdi, Huffman and Pless, Eds., Elsevier, to appear.
- [330] J. A. van der HORST and T. BERGER: Complete decoding of triple-error-correcting binary BCH codes, *IEEE Trans. Inform. Th.*, vol. 22, pp. 138–147, 1976.
- [331] X. D. HOU: Covering radius and error correcting codes, Ph. D. Thesis, University of Illinois, Chicago, United States, 77 pp., 1990.
- [332] X. D. HOU: Some results on the norm of codes, *IEEE Trans. Inform. Th.*, vol. 36, pp. 683–685, 1990.
- [333] X. D. HOU: New lower bounds for covering codes, *IEEE Trans. Inform. Th.*, vol. 36, pp. 895–899, 1990.
- [334] X. D. HOU: An improved sphere covering bound for the codes with  $n = 3R+2$ , *IEEE Trans. Inform. Th.*, vol. 36, pp. 1476–1478, 1990.
- [335] X. D. HOU: Binary linear quasi-perfect codes are normal, *IEEE Trans. Inform. Th.*, vol. 37, pp. 378–379, 1991.
- [336] X. D. HOU: On the covering radius of subcodes of a code, *IEEE Trans. Inform. Th.*, vol. 37, pp. 1706–1707, 1991.
- [337] X. D. HOU: Some inequalities about the covering radius of Reed-Muller codes, *Designs, Codes and Cryptography*, vol. 2, pp. 215–224, 1992.

- [338] X. D. HOU: Some results on the covering radii of Reed-Muller codes, *IEEE Trans. Inform. Th.*, vol. 39, pp. 366–378, 1993.
- [339] X. D. HOU: Further results on the covering radii of the Reed-Muller codes, *Designs, Codes and Cryptography*, vol. 3, pp. 167–177, 1993.
- [340] X. D. HOU: Covering radius of the Reed-Muller code  $R(1, 7)$  — a simpler proof, *J. Combinatorial Th.*, Ser. A, vol. 74, pp. 337–341, 1996.
- [341] X. D. HOU: On the covering radius of  $R(1, m)$  in  $R(3, m)$ , *IEEE Trans. Inform. Th.*, vol. 42, pp. 1035–1037, 1996.
- [342] X. D. HOU: The covering radius of  $R(1, 9)$  in  $R(4, 9)$ , *Designs, Codes and Cryptography*, vol. 8, pp. 285–292, 1996.
- [343] X. D. HOU: The Reed-Muller code  $R(1, 7)$  is normal, *Designs, Codes and Cryptography*, to appear.
- [344] X. D. HOU: On the norm and covering radius of the first order Reed-Muller codes, submitted.
- [345] H. JANWA: Relations among parameters of codes, Ph. D. Thesis, Syracuse University, United States, 116 pp., 1986.
- [346] H. JANWA: Some new upper bounds on the covering radius of binary linear codes, *IEEE Trans. Inform. Th.*, vol. 35, pp. 110–122, 1989.
- [347] H. JANWA: Some optimal codes from algebraic geometry and their covering radii, *European J. Combinatorics*, vol. 11, pp. 249–266, 1990.
- [348] H. JANWA: On the parameters of algebraic geometric codes, *Lecture Notes in Computer Science*, No. 539, pp. 19–28, Springer-Verlag, 1991.
- [349] H. JANWA and H. F. MATTSON, Jr.: Covering radii of even subcodes of  $t$ -dense codes, *Lecture Notes in Computer Science*, No. 229, pp. 120–130, Springer-Verlag, 1986.
- [350] H. JANWA and H. F. MATTSON, Jr.: On the normality of binary linear codes, *IEEE Trans. Inform. Th.*, submitted.
- [351] H. JANWA and H. F. MATTSON, Jr.: Some upper bounds on the covering radii of linear codes over  $\mathbf{F}_q$  and their applications, Preprint, 1996.
- [352] D. S. JOHNSON: Approximation algorithms for combinatorial problems, *J. Comput. System Sciences*, vol. 9, pp. 256–298, 1974.
- [353] S. M. JOHNSON: A new upper bound for error-correcting codes, *IEEE Trans. Inform. Th.*, vol. 8, pp. 203–207, 1962.
- [354] S. M. JOHNSON: A new lower bound for coverings by rook domains, *Utilitas Mathematica*, vol. 1, pp. 121–140, 1972.
- [355] G. A. KABATYANSKII and V. I. PANCHENKO: Unit sphere packings and coverings of the Hamming space, *Problemy Peredachi Informatsii*, vol. 24, No. 4, pp. 3–16, 1988. Translated in: *Problems of Inform. Transm.*, vol. 24, No. 4, pp. 261–272.
- [356] Y. KAIKPAINEN: Chow variety, Licentiate Thesis, University of Turku, Finland, 1993 (in Finnish).

- [357] Y. KAIPIAINEN: On the covering radius of long non-binary BCH codes, Ph. D. Thesis, University of Turku, Finland, 100 pp., 1995.
- [358] J. G. KALBFLEISCH and R. G. STANTON: A combinatorial problem in matching, *J. London Math. Soc.*, vol. 44, pp. 60–64, 1969 and (2), vol. 1, p. 398, 1969.
- [359] J. G. KALBFLEISCH, R. G. STANTON and J. D. HORTON: On covering sets and error-correcting codes, *J. Combinatorial Th.*, Ser. A, vol. 11, pp. 233–250, 1971.
- [360] J. G. KALBFLEISCH and P. H. WEILAND: Some new results for the covering problem, in: *Recent Progress in Combinatorics*, Tutte, Ed., pp. 37–45, New York: Academic Press, 1969.
- [361] H. J. L. KAMPS and J. H. van LINT: The football pool problem for 5 matches, *J. Combinatorial Th.*, Ser. A, vol. 3, pp. 315–325, 1967.
- [362] H. J. L. KAMPS and J. H. van LINT: A covering problem, *Combinatorial Theory and its Applications*, vol. II, pp. 679–685, in: *Colloquia Mathematica Societatis János Bolyai*, Ser. 4, 1970.
- [363] M. G. KARPOVSKY: Weight distribution of translates, covering radius and perfect codes correcting errors of the given multiplicities, *IEEE Trans. Inform. Th.*, vol. 27, pp. 462–472, 1981.
- [364] M. G. KARPOVSKY and V. MILMAN: On subspaces contained in subsets of finite homogeneous spaces, *Discrete Mathematics*, vol. 22, pp. 273–280, 1978.
- [365] M. G. KARPOVSKY and V. MILMAN: Coordinate density of sets of vectors, *Discrete Mathematics*, vol. 24, pp. 177–184, 1978.
- [366] T. KASAMI: Weight distributions of Bose-Chaudhuri-Hocquenghem codes, in: *Combinatorial Mathematics and its Applications*, Bose and Dowling, Eds., Chapter 20, University of North Carolina Press, 1969. Also in: *Key Papers in the Development of Coding Theory*, Berlekamp, Ed., pp. 268–274, IEEE Press, 1974.
- [367] T. KASAMI, T. FUJIWARA and S. LIN: An approximation to the weight distribution of binary linear codes, *IEEE Trans. Inform. Th.*, vol. 31, pp. 769–780, 1985.
- [368] T. KASAMI and N. TOKURA: On the weight structure of Reed-Muller codes, *IEEE Trans. Inform. Th.*, vol. 16, pp. 752–759, 1970.
- [369] T. KASAMI, N. TOKURA and S. AZUMI: On the weight enumeration of weights less than  $2.5d$  of Reed-Muller codes, Preprint, Faculty of Engineering, Osaka University, Japan, 1974.
- [370] T. KASAMI, S. YAMAMURA and A. V. KUZNETSOV: Volume of additive matched error- and defect-correcting codes, *Problemy Peredachi Informatsii*, vol. 14, No. 2, pp. 3–10, 1978. Translated in: *Problems of Inform. Transm.*, vol. 14, No. 2, pp. 79–84.
- [371] G. O. H. KATONA and J. SRIVASTAVA: Minimal 2-coverings of a finite affine space based on  $GF(2)$ , *J. Statist. Planning Inference*, vol. 8, pp. 375–388, 1983.

- [372] G. L. KATSMAN: Covering radius of codes being dual to iterative ones, *Proc. Fifth Joint Soviet-Swedish Internat. Workshop on Information Theory*, pp. 91–92, Moscow, 1991.
- [373] G. L. KATSMAN: Bounds on covering radius of dual product codes, *Lecture Notes in Computer Science*, No. 573, pp. 52–57, Springer-Verlag, 1992.
- [374] K. E. KILBY and N. J. A. SLOANE: On the covering radius problem for codes: I Bounds on normalized covering radius, II Codes of low dimension; normal and abnormal codes, *SIAM J. Algebraic and Discrete Methods*, vol. 8, pp. 604–627, 1987.
- [375] S. KIRKPATRICK, C. D. GELATT, Jr., and M. P. VECCHI: Optimization by simulated annealing, *Science*, vol. 220, pp. 671–680, 1983.
- [376] A. KLAPPER: On the existence of secure feedback registers, *Lecture Notes in Computer Science*, No. 1070, pp. 256–267, Springer-Verlag, 1996.
- [377] A. KLAPPER: The multicovering radii of codes, Preprint, 1996.
- [378] Y. KLEIN, S. LITSYN and A. VARDY: Two new bounds on the size of binary codes with a minimum distance of three, *Designs, Codes and Cryptography*, vol. 6, pp. 219–227, 1995.
- [379] D. J. KLEITMAN: On a combinatorial conjecture of Erdős, *J. Combinatorial Th.*, vol. 1, pp. 209–214, 1966.
- [380] D. J. KLEITMAN and J. H. SPENCER: Families of  $k$ -independent sets, *Discrete Mathematics*, vol. 6, pp. 255–262, 1973.
- [381] T. KLØVE: On Robinson's coding problem, *IEEE Trans. Inform. Th.*, vol. 29, pp. 450–454, 1983.
- [382] D. E. KNUTH: Efficient balanced codes, *IEEE Trans. Inform. Th.*, vol. 32, pp. 51–53, 1986.
- [383] E. KOLEV: Codes over  $GF(3)$  of length 5, 27 codewords and covering radius 1, *J. Combinatorial Designs*, vol. 1, pp. 265–275, 1993.
- [384] E. KOLEV: Mixed covering codes with two binary and four ternary coordinates, *Lecture Notes in Computer Science*, No. 948, pp. 312–322, Springer-Verlag, 1995.
- [385] E. KOLEV and I. LANDGEV: On some mixed covering codes of small length, *Lecture Notes in Computer Science*, No. 781, pp. 38–50, Springer-Verlag, 1994.
- [386] K. U. KOSCHNICK: A new upper bound for the football pool problem for nine matches, *J. Combinatorial Th.*, Ser. A, vol. 62, pp. 162–167, 1993.
- [387] I. KRASIKOV and S. LITSYN: On spectra of BCH codes, *IEEE Trans. Inform. Th.*, vol. 41, pp. 786–788, 1995.
- [388] I. KRASIKOV and S. LITSYN: On integral zeros of Krawtchouk polynomials, *J. Combinatorial Th.*, Ser. A, vol. 74, pp. 71–99, 1996.
- [389] J. KRATOCHVÍL: 1-perfect codes over self-complementary graphs, *Commentationes Mathematicae Universitatis Carolinae*, No. 26, pp. 589–595, 1985.

- [390] J. KRATOCHVÍL: Perfect codes over graphs, *J. Combinatorial Th.*, Ser. B, vol. 40, pp. 224–228, 1986.
- [391] J. KRATOCHVÍL: Perfect codes in general graphs, *Colloquia Mathematica Societatis János Bolyai*, vol. 52, pp. 357–364, 1988.
- [392] J. KRATOCHVÍL: *Perfect Codes in General Graphs*, Prague: Academia, 1991.
- [393] J. KRATOCHVÍL: Regular codes in regular graphs are difficult, *Discrete Mathematics*, vol. 133, pp. 191–205, 1994.
- [394] P. V. KUMAR and R. A. SCHOLTZ: Bounds on the linear span of bent sequences, *IEEE Trans. Inform. Th.*, vol 29, pp. 854–862, 1983.
- [395] R. P. KURSHAN and N. J. A. SLOANE: Coset analysis of Reed-Muller codes via translates of finite vector spaces, *Information and Control*, vol. 20, pp. 410–414, 1972.
- [396] N. N. KUZZJURIN: On the difference between asymptotically good packings and coverings, *European J. Combinatorics*, vol. 16, pp. 35–40, 1995.
- [397] A. V. KUZNETSOV: Coding in a channel with generalized defects and random errors, *Problemy Peredachi Informatsii*, vol. 21, No. 1, pp. 28–34, 1985. Translated in: *Problems of Inform. Transm.*, vol. 21, No. 1, pp. 20–25.
- [398] A. V. KUZNETSOV and B. S. TSYBAKOV: Coding in memories with defective cells, *Problemy Peredachi Informatsii*, vol. 10, No. 2, pp. 52–60, 1974. Translated in: *Problems of Inform. Transm.*, vol. 10, No. 2, pp. 132–138.
- [399] A. V. KUZNETSOV and A. J. H. VINCK: On the general defective channel with informed encoder and capacities of some constrained memories, *IEEE Trans. Inform. Th.*, vol. 40, pp. 1866–1871, 1994.
- [400] H. LAAKSO: Nonexistence of nontrivial perfect codes in the case  $q = p_1^a p_2^b p_3^c$ ,  $e \geq 3$ , *Ann. Univ. Turku*, Ser. A I, No. 177, pp. 1–43, 1979.
- [401] P. J. M. van LAARHOVEN and E. H. L. AARTS: *Simulated Annealing: Theory and Applications*, Dordrecht: Reidel, 1987.
- [402] P. J. M. van LAARHOVEN, E. H. L. AARTS, J. H. van LINT and L. T. WILLE: New upper bounds for the football pool problem for 6, 7 and 8 matches, *J. Combinatorial Th.*, Ser. A, vol. 52, pp. 304–312, 1989.
- [403] J. M. LABORDE: Une nouvelle famille de codes binaires, parfaits, non linéaires, *Comptes-Rendus de l'Académie des Sciences*, Ser. I, vol. 297, pp. 67–70, 1983.
- [404] J. M. LABORDE: Sur le nombre domatique du  $n$ -cube et une conjecture de Zelinka, *European J. Combinatorics*, vol. 8, pp. 175–177, 1987.
- [405] G. LACHAUD and J. WOLFMANN: The weights of the orthogonals of the extended quadratic binary Goppa codes, *IEEE Trans. Inform. Th.*, vol. 36, pp. 686–692, 1990.
- [406] J. LAHTONEN: An optimal polynomial for a covering radius problem, *Discrete Mathematics*, vol. 105, pp. 313–317, 1992.

- [407] T. LAIHONEN and S. LITSYN: On upper bounds for minimum distance and covering radius of nonbinary codes, *Designs, Codes and Cryptography*, submitted.
- [408] E. R. LAMKEN, W. H. MILLS, R. C. MULLIN and S. A. VANSTONE: Coverings of pairs by quintuples, *J. Combinatorial Th.*, Ser. A, vol. 44, pp. 49–68, 1987.
- [409] S. LANG and A. WEIL: Number of points of varieties in finite fields, *American J. Math.*, vol. 76, pp. 819–827, 1954.
- [410] P. LANGEVIN: The covering radius of  $RM(1, 9)$  into  $RM(3, 9)$ , *Lecture Notes in Computer Science*, No. 514, pp. 51–59, Springer-Verlag, 1991.
- [411] P. LANGEVIN: On the orphans and covering radius of the Reed-Muller codes, *Lecture Notes in Computer Science*, No. 539, pp. 234–240, Springer-Verlag, 1991.
- [412] P. LANGEVIN: On generalized bent functions, *CISM Courses and Lectures*, No. 339, pp. 147–157, Springer-Verlag, 1993.
- [413] A. LEMPEL: Matrix factorization over  $GF(2)$  and trace orthogonal bases of  $GF(2^n)$ , *SIAM J. Comput.*, vol. 4, pp. 175–186, 1975.
- [414] H. W. LENSTRA, Jr.: Two theorems on perfect codes, *Discrete Mathematics*, vol. 3, pp. 125–132, 1972.
- [415] M. LEVAN and K. T. PHELPS: Personal communication, 1996.
- [416] V. I. LEVENSHTEIN: Bounds on the maximal cardinality of a code with bounded modulus of the inner product, *Soviet Math. — Dokl.*, vol. 25, No. 2, pp. 526–531, 1982.
- [417] V. I. LEVENSHTEIN: Bounds for packings of metric spaces and some of their applications, *Problemy Kibernetiki*, vol. 40, pp. 43–110, 1983 (in Russian).
- [418] V. I. LEVENSHTEIN: A simple proof of the main inequalities for fundamental parameters of codes in polynomial association schemes, *Proc. 4th Internat. Workshop on Algebraic and Combinatorial Coding Theory*, pp. 143–146, Novgorod, 1994.
- [419] V. I. LEVENSHTEIN: Krawtchouk polynomials and universal bounds for codes and designs in Hamming spaces, *IEEE Trans. Inform. Th.*, vol. 41, pp. 1303–1321, 1995.
- [420] F. LEVY-DIT-VEHEL and S. LITSYN: On the covering radius of long Goppa codes, *Lecture Notes in Computer Science*, No. 948, pp. 341–346, Springer-Verlag, 1995.
- [421] F. LEVY-DIT-VEHEL and S. LITSYN: More on the covering radius of BCH codes, *IEEE Trans. Inform. Th.*, vol. 42, pp. 1023–1028, 1996.
- [422] F. LEVY-DIT-VEHEL and S. LITSYN: Parameters of Goppa codes revisited, *IEEE Trans. Inform. Th.*, submitted.
- [423] D. LI and W. CHEN: New lower bounds for binary covering codes, *IEEE Trans. Inform. Th.*, vol. 40, pp. 1122–1129, 1994.

- [424] R. LIDL and H. NIEDERREITER: *Finite Fields*, Reading, MA: Addison Wesley, 1983.
- [425] B. LINDSTRÖM: On group and nongroup perfect codes in  $q$  symbols, *Math. Scand.*, vol. 25, pp. 149–158, 1969.
- [426] B. LINDSTRÖM: Group partitions and mixed perfect codes, *Canad. Math. Bull.*, vol. 18, pp. 57–60, 1975.
- [427] K. LINDSTRÖM: The nonexistence of unknown nearly perfect binary codes, *Ann. Univ. Turku, Ser. A I*, No. 169, pp. 7–28, 1975.
- [428] K. LINDSTRÖM: All nearly perfect codes are known, *Information and Control*, vol. 35, pp. 40–47, 1977.
- [429] K. LINDSTRÖM and M. J. AALTONEN: The nonexistence of nearly perfect nonbinary codes for  $1 \leq e \leq 10$ , *Ann. Univ. Turku, Ser. A I*, No. 172, 1976.
- [430] J. H. van LINT: 1967–1969 Report of the Discrete Mathematics Group, Report 69-WSK-04, Eindhoven University of Technology, the Netherlands, 1969.
- [431] J. H. van LINT: On the nonexistence of perfect 2- and 3-Hamming-error-correcting codes over  $GF(q)$ , *Information and Control*, vol. 16, pp. 396–401, 1970.
- [432] J. H. van LINT: On the nonexistence of perfect 5-, 6-, and 7-Hamming-error-correcting codes over  $GF(q)$ , Report 70-WSK-06, Eindhoven University of Technology, the Netherlands, 1970.
- [433] J. H. van LINT: *Coding Theory*, New York: Springer-Verlag, 1971.
- [434] J. H. van LINT: Nonexistence theorems for perfect error-correcting-codes, in: *Computers in Algebra and Number Theory*, vol. IV, SIAM-AMS Proceedings, 1971.
- [435] J. H. van LINT: On the nonexistence of certain perfect codes, in: *Computers in Number Theory*, Atkin and Birch, Eds., pp. 227–282, New York: Academic Press, 1971.
- [436] J. H. van LINT: Recent results on perfect codes and related topics, in: *Combinatorics*, Hall and van Lint, Eds., vol. 1, pp. 158–178, Mathematical Centre, Amsterdam, 1974.
- [437] J. H. van LINT: A survey of perfect codes, *Rocky Mountain J. Math.*, vol. 5, pp. 199–224, 1975.
- [438] J. H. van LINT: *Introduction to Coding Theory*, New York: Springer-Verlag, 1982.
- [439] J. H. van LINT: Recent results on covering problems, *Lecture Notes in Computer Science*, No. 357, pp. 7–21, Springer-Verlag, 1989.
- [440] J. H. van LINT, Jr.: Covering radius problems, Master's Thesis, Eindhoven University of Technology, the Netherlands, 41 pp., 1988.
- [441] J. H. van LINT, Jr., and G. J. M. van WEE: Generalized bounds on binary/ternary mixed packing and covering codes, *J. Combinatorial Th.*, Ser. A, vol. 57, pp. 130–143, 1991.

- [442] S. LITSYN: An updated table of best known binary codes, Preprint, 1996.
- [443] S. LITSYN, C. J. MORENO and O. MORENO: Divisibility properties and new bounds for cyclic codes and exponential sums in one and several variables, *Applicable Algebra in Engineering, Communication and Computing*, vol. 5, pp. 105–116, 1994.
- [444] S. LITSYN, P. SOLÉ and R. STRUIK: On the covering radius of a code as a function of the dual distance and the code rate, Preprint, 1996.
- [445] S. LITSYN and A. TIETÄVÄINEN: Upper bounds on the covering radius of a code with a given dual distance, *European J. Combinatorics*, vol. 17, pp. 265–270, 1996.
- [446] S. LITSYN and A. VARDY: The uniqueness of the Best code, *IEEE Trans. Inform. Th.*, vol. 40, pp. 1693–1698, 1994.
- [447] S. P. LLOYD: Binary block coding, *Bell Syst. Tech. J.*, vol. 36, pp. 517–535, 1957. Also in: *Key Papers in the Development of Coding Theory*, Berlekamp, Ed., pp. 246–251, IEEE Press, 1974.
- [448] A. C. LOBSTEIN: Rayon de recouvrement de codes binaires non-linéaires, *Traitement du Signal*, vol. 1, No. 2–1, pp. 105–114, 1984.
- [449] A. C. LOBSTEIN: Contributions au codage combinatoire: ordres additifs, rayon de recouvrement, Thèse, Télécom Paris, France, 163 pp., 1985.
- [450] A. C. LOBSTEIN: The hardness of solving Subset Sum with preprocessing, *IEEE Trans. Inform. Th.*, vol. 36, pp. 943–946, 1990.
- [451] A. C. LOBSTEIN and G. D. COHEN: Sur la complexité d'un problème de codage, *RAIRO Informatique Théorique et Applications*, vol. 21, No. 1, pp. 25–32, 1987.
- [452] A. C. LOBSTEIN, G. D. COHEN and N. J. A. SLOANE: Recouvrements d'espaces de Hamming binaires, *Comptes-Rendus de l'Académie des Sciences*, Ser. I, vol. 301, pp. 135–138, 1985.
- [453] A. C. LOBSTEIN and V. S. PLESS: The length function: a revised table, *Lecture Notes in Computer Science*, No. 781, pp. 51–55, Springer-Verlag, 1994.
- [454] A. C. LOBSTEIN and P. SOLÉ: Arithmetic codes - Survey, recent and new results, *Lecture Notes in Computer Science*, No. 539, pp. 246–258, Springer-Verlag, 1991.
- [455] A. C. LOBSTEIN and G. J. M. van WEE: On normal and subnormal  $q$ -ary codes, *IEEE Trans. Inform. Th.*, vol. 35, pp. 1291–1295, 1989, and vol. 36, p. 1498, 1990.
- [456] A. C. LOBSTEIN and V. A. ZINOVIEV: On new perfect binary nonlinear codes, *Applicable Algebra in Engineering, Communication and Computing*, submitted.
- [457] L. LOVÁSZ: On the ratio of optimal integral and fractional covers, *Discrete Mathematics*, vol. 13, pp. 383–390, 1975.
- [458] L. LOVÁSZ: Covers, packings, and some heuristic algorithms, *Proc. 5th British Combinatorial Conf.*, pp. 417–429, 1975.

- [459] L. LOVÁSZ: Kneser's conjecture, chromatic number and homotopy, *J. Combinatorial Th.*, Ser. A, vol. 25, pp. 319–324, 1978.
- [460] L. LOVÁSZ, J. H. SPENCER and K. VESZTERGOMBI: Discrepancy of set-systems and matrices, *European J. Combinatorics*, vol. 7, pp. 151–160, 1986.
- [461] J. E. MACDONALD: Design methods for maximum minimum-distance error-correcting codes, *IBM J. Res. Develop.*, vol. 4, pp. 43–57, 1960.
- [462] F. J. MACWILLIAMS: Combinatorial problems of elementary group theory, Ph. D. Thesis, Harvard University, United States, 1962.
- [463] F. J. MACWILLIAMS: Orthogonal matrices over finite fields, *American Mathematical Monthly*, vol. 76, pp. 152–164, 1969.
- [464] F. J. MACWILLIAMS and N. J. A. SLOANE: *The Theory of Error-Correcting Codes*, Amsterdam: North-Holland, 1977.
- [465] J. A. MAIORANA: A classification of the cosets of the Reed-Muller code  $R(1, 6)$ , *Mathematics of Computation*, vol. 57, pp. 403–414, 1991.
- [466] K. N. MANEV and E. D. VELIKOVA: The covering radius and weight distribution of cyclic codes over  $GF(4)$  of lengths up to 13, *Proc. 2nd Internat. Workshop on Algebraic and Combinatorial Coding Theory*, pp. 150–153, Leningrad, 1990.
- [467] H. B. MANN: *Addition Theorems*, New York: Wiley, 1965.
- [468] W. MANTEL: Problem 28 (solution by H. Gouwentak, W. Mantel, J. Texeira de Mattes, F. Schuh and W. A. Wythoff), *Wiskundige Opgaven*, vol. 10, pp. 60–61, 1907.
- [469] H. F. MATTSON, Jr.: An upper bound on covering radius, *Annals of Discrete Mathematics*, vol. 17, pp. 453–458, 1983.
- [470] H. F. MATTSON, Jr.: Another upper bound on covering radius, *IEEE Trans. Inform. Th.*, vol. 29, pp. 356–359, 1983.
- [471] H. F. MATTSON, Jr.: An improved upper bound on covering radius, *Lecture Notes in Computer Science*, No. 228, pp. 90–106, Springer-Verlag, 1986.
- [472] H. F. MATTSON, Jr.: Simplifications to “A new approach to the covering radius...”, *J. Combinatorial Th.*, Ser. A, vol. 57, pp. 311–315, 1991.
- [473] H. F. MATTSON, Jr., and J. R. SCHATZ: A brief survey of covering radius, *Annals of Discrete Mathematics*, vol. 18, pp. 617–624, 1983.
- [474] H. F. MATTSON, Jr., and G. SOLOMON: A new treatment of Bose-Chaudhuri codes, *J. Soc. Indust. Appl. Math.*, vol. 9, pp. 654–669, 1961. Also in: *Key Papers in the Development of Coding Theory*, Berlekamp, Ed., pp. 82–86, IEEE Press, 1974.
- [475] J. G. MAULDON: Covering theorems for groups, *Quart. J. Math. Oxford*, vol. 1, pp. 284–287, 1950.
- [476] R. J. MCELIECE: Weight congruences for  $p$ -ary cyclic codes, *Discrete Mathematics*, vol. 3, pp. 172–192, 1972.

- [477] R. J. MCELIECE: *The Theory of Information and Coding*, Encyclopedia of Mathematics and its Applications, vol. 3, Reading, MA: Addison Wesley, 1977.
- [478] R. J. MCELIECE: *Finite Fields for Computer Scientists and Engineers*, Kluwer, 1987.
- [479] R. J. MCELIECE, E. R. RODEMICH, H. C. RUMSEY and L. R. WELCH: New upper bounds on the rate of a code via the Delsarte-MacWilliams inequalities, *IEEE Trans. Inform. Th.*, vol. 23, pp. 157–166, 1977.
- [480] A. MCLOUGHLIN: The covering radius of the  $(m-3)$ rd order Reed-Muller codes and a lower bound on the covering radius of the  $(m-4)$ th order Reed-Muller codes, *SIAM J. Applied Mathematics*, vol. 37, pp. 419–422, 1979.
- [481] A. MCLOUGHLIN: The complexity of computing the covering radius of a code, *IEEE Trans. Inform. Th.*, vol. 30, pp. 800–804, 1984.
- [482] A. MENEZES, I. F. BLAKE, X. GAO, R. C. MULLIN, S. A. VANSTONE and T. YAGHOOBIAN: *Applications of Finite Fields*, Kluwer, 1993.
- [483] F. MERKX: Wom-codes constructed with projective geometries, *Traitemet du Signal*, vol. 1, No. 2–2, pp. 227–231, 1984.
- [484] A. R. MEYER and L. J. STOCKMEYER: The equivalence problem for regular expressions with squaring requires exponential time, *Proc. 13th Ann. IEEE Symp. on Switching and Automata Theory*, pp. 125–129, 1972.
- [485] W. H. MILLS: On the covering of pairs by quadruples I, *J. Combinatorial Th.*, Ser. A, vol. 13, pp. 55–78, 1972.
- [486] W. H. MILLS: On the covering of pairs by quadruples II, *J. Combinatorial Th.*, Ser. A, vol. 15, pp. 138–166, 1973.
- [487] W. H. MILLS: Covering designs I: Coverings by a small number of subsets, *Ars Combinatoria*, vol. 8, pp. 199–315, 1979.
- [488] W. H. MILLS: A covering of pairs by quintuples, *Ars Combinatoria*, vol. 18, pp. 21–31, 1983.
- [489] W. H. MILLS and R. C. MULLIN: Coverings and packings, in: *Contemporary Design Theory: A Collection of Surveys*, Dinitz and Stinson, Eds., pp. 371–399, Wiley, 1992.
- [490] E. MINKES: A non-deterministic algorithm for the covering radius, covering radius bounds and code constructions, Master's Thesis, Delft University of Technology, the Netherlands, 21 pp., 1996.
- [491] M. MOLLARD: Les invariants du  $n$ -cube, Thèse de 3ème cycle, Université de Grenoble, France, 113 pp., 1981.
- [492] M. MOLLARD: Une généralisation de la fonction parité, application à la construction de codes parfaits, Rapport de Recherche No. 395, Laboratoire de Mathématiques Appliquées, Grenoble, France, 1983.
- [493] M. MOLLARD: Une nouvelle famille de 3-codes parfaits sur  $GF(q)$ , *Discrete Mathematics*, vol. 49, pp. 209–212, 1984.

- [494] M. MOLLARD: A generalized parity function and its use in the construction of perfect codes, *SIAM J. Algebraic and Discrete Methods*, vol. 7, pp. 113–115, 1986.
- [495] B. MONTARON and G. D. COHEN: Codes parfaits binaires à plusieurs rayons, *Revue CETHEDEC*, vol. 2, pp. 35–58, 1979.
- [496] C. J. MORENO and O. MORENO: Exponential sums and Goppa codes I, *Proc. American Math. Soc.*, vol. 111, pp. 523–531, 1991.
- [497] C. J. MORENO and O. MORENO: Exponential sums and Goppa codes II, *IEEE Trans. Inform. Th.*, vol. 38, pp. 1222–1229, 1992.
- [498] O. MORENO: Further results on quasiperfect codes related to the Goppa codes, *Congressus Numerantium*, vol. 40, pp. 249–256, 1983.
- [499] O. MORENO and C. J. MORENO: Constructive elementary approach to the covering radius of long BCH codes, *Proc. 2nd Internat. Workshop on Algebraic and Combinatorial Coding Theory*, pp. 162–165, Leningrad, 1990.
- [500] O. MORENO and C. J. MORENO: The MacWilliams-Sloane conjecture on the tightness of the Carlitz-Uchiyama bound and the weights of duals of BCH codes, *IEEE Trans. Inform. Th.*, vol. 40, pp. 1894–1907, 1994.
- [501] J. MYKKELTVEIT: The covering radius of the (128, 8) Reed-Muller code is 56, *IEEE Trans. Inform. Th.*, vol. 26, pp. 359–362, 1980.
- [502] J. NAOR and M. NAOR: Small bias probability spaces: efficient constructions and applications, *Proc. 22nd STOC*, pp. 213–223, 1990.
- [503] A. F. NIKIFOROV, S. K. SUSLOV and V. B. UVAROV: *Classical Orthogonal Polynomials of Discrete Variable*, Moscow: Nauka, 1985 (in Russian).
- [504] S. C. NTAFOS and S. L. HAKIMI: On the complexity of some coding problems, *IEEE Trans. Inform. Th.*, vol. 27, pp. 794–796, 1981.
- [505] M. NUMATA: On the minimal covering of 3-dimensional Hamming scheme, *Ann. Rep. Fac. Educ. Iwate University*, vol. 52, No. 1, pp. 73–84, 1992.
- [506] K. J. NURMELA: Constructing combinatorial designs by local search, J. Sc. Thesis, Research Report, Ser. A, No. 27, Helsinki University of Technology, Finland, 76 pp., 1993.
- [507] K. J. NURMELA and P. R. J. ÖSTERGÅRD: Constructing covering designs by simulated annealing, Technical Report, Ser. B, No. 10, Helsinki University of Technology, Finland, 25 pp., 1993.
- [508] K. J. NURMELA and P. R. J. ÖSTERGÅRD: Upper bounds for covering designs by simulated annealing, *Congressus Numerantium*, vol. 96, pp. 93–111, 1993.
- [509] K. NYBERG: Constructions of bent functions and difference sets, *Lecture Notes in Computer Science*, No. 473, pp. 151–160, Springer-Verlag, 1991.
- [510] J. E. OLSON and J. H. SPENCER: Balancing families of sets, *J. Combinatorial Th.*, Ser. A, vol. 25, pp. 29–37, 1978.

- [511] P. R. J. ÖSTERGÅRD: A new binary code of length 10 and covering radius 1, *IEEE Trans. Inform. Th.*, vol. 37, pp. 179–180, 1991.
- [512] P. R. J. ÖSTERGÅRD: Upper bounds for  $q$ -ary covering codes, *IEEE Trans. Inform. Th.*, vol. 37, pp. 660–664, 1991, and vol. 37, p. 1738, 1991.
- [513] P. R. J. ÖSTERGÅRD: Constructions of mixed covering codes, Research Report, Ser. A, No. 18, Helsinki University of Technology, Finland, 44 pp., 1991.
- [514] P. R. J. ÖSTERGÅRD: Further results on  $(k, t)$ -subnormal covering codes, *IEEE Trans. Inform. Th.*, vol. 38, pp. 206–210, 1992.
- [515] P. R. J. ÖSTERGÅRD: Construction methods for covering codes, Ph. D. Thesis, Research Report, Ser. A, No. 25, Helsinki University of Technology, Finland, 107 pp., 1993.
- [516] P. R. J. ÖSTERGÅRD: Construction methods for mixed covering codes, in: *Analysis, Algebra, and Computers in Mathematical Research*, Gyllenberg and Persson, Eds., pp. 387–408, New York: Dekker, 1994.
- [517] P. R. J. ÖSTERGÅRD: New upper bounds for the football pool problem for 11 and 12 matches, *J. Combinatorial Th.*, Ser. A, vol. 67, pp. 161–168, 1994.
- [518] P. R. J. ÖSTERGÅRD: New multiple covering codes by tabu search, *Australasian J. Combinatorics*, vol. 12, pp. 145–155, 1995.
- [519] P. R. J. ÖSTERGÅRD: A combinatorial proof for the football pool problem for six matches, *J. Combinatorial Th.*, Ser. A, vol. 76, pp. 160–163, 1996.
- [520] P. R. J. ÖSTERGÅRD: The football pool problem, *Congressus Numerantium*, vol. 114, pp. 33–43, 1996.
- [521] P. R. J. ÖSTERGÅRD: A coloring problem in Hamming spaces, *European J. Combinatorics*, to appear.
- [522] P. R. J. ÖSTERGÅRD: New constructions for  $q$ -ary covering codes, *Ars Combinatoria*, to appear.
- [523] P. R. J. ÖSTERGÅRD: Constructing covering codes by tabu search, *J. Combinatorial Designs*, to appear.
- [524] P. R. J. ÖSTERGÅRD and H. O. HÄMÄLÄINEN: New upper bounds for binary-ternary mixed covering codes, Research Report, Ser. A, No. 22, Helsinki University of Technology, Finland, 33 pp., 1993.
- [525] P. R. J. ÖSTERGÅRD and H. O. HÄMÄLÄINEN: A new table of binary/ternary mixed covering codes, *Designs, Codes and Cryptography*, to appear.
- [526] P. R. J. ÖSTERGÅRD and M. K. KAIKKONEN: New upper bounds for binary covering codes, *Discrete Mathematics*, to appear.
- [527] W. M. C. J. van OVERVELD: The four cases of write unidirectional memory codes over arbitrary alphabets, *IEEE Trans. Inform. Th.*, vol. 37, pp. 872–878, 1991.
- [528] W. M. C. J. van OVERVELD: On the capacity region for deterministic two-way channels and write unidirectional memories, Ph. D. Thesis, Eindhoven University of Technology, the Netherlands, 210 pp., 1991.

- [529] J. PACH and J. H. SPENCER: Explicit codes with low covering radius, *IEEE Trans. Inform. Th.*, vol. 34, pp. 1281–1285, 1988.
- [530] V. I. PANCHENKO: Packings and coverings over an arbitrary alphabet, *Problemy Peredachi Informatsii*, vol. 24, No. 4, pp. 93–96, 1988. Translated in: *Problems of Inform. Transm.*, vol. 24, No. 4, pp. 331–333.
- [531] N. J. PATTERSON and D. H. WIEDEMANN: The covering radius of the  $(2^{15}, 16)$  Reed-Muller code is at least 16276, *IEEE Trans. Inform. Th.*, vol. 29, pp. 354–356, 1983.
- [532] N. J. PATTERSON and D. H. WIEDEMANN: Correction to “The covering radius of the  $(2^{15}, 16)$  Reed-Muller code is at least 16276”, *IEEE Trans. Inform. Th.*, vol. 36, p. 443, 1990.
- [533] R. PENROSE: Pentaplexity: a class of nonperiodic tilings of the plane, *Mathematical Intelligencer*, vol. 2, pp. 32–37, 1979.
- [534] W. W. PETERSON and E. J. WELDON, Jr.: *Error-Correcting Codes*, 2nd ed., Cambridge, MA: MIT Press, 1972.
- [535] K. T. PHELPS: A combinatorial construction of perfect codes, *SIAM J. Algebraic and Discrete Methods*, vol. 4, pp. 398–403, 1983.
- [536] K. T. PHELPS: A general product construction for error correcting codes, *SIAM J. Algebraic and Discrete Methods*, vol. 5, pp. 224–228, 1984.
- [537] K. T. PHELPS: A product construction for perfect codes over arbitrary alphabets, *IEEE Trans. Inform. Th.*, vol. 30, pp. 769–771, 1984.
- [538] K. T. PHELPS: Dual product constructions of Reed-Muller type codes, *IEEE Trans. Inform. Th.*, vol. 32, pp. 103–106, 1986.
- [539] K. T. PHELPS and M. LEVAN: Kernels of nonlinear Hamming codes, *Designs, Codes and Cryptography*, vol. 6, pp. 247–257, 1995.
- [540] K. T. PHELPS and M. LEVAN: Nonsystematic perfect codes, Preprint, 1996.
- [541] V. S. PLESS: On the uniqueness of the Golay codes, *J. Combinatorial Th.*, vol. 5, pp. 215–228, 1968.
- [542] V. S. PLESS: *Introduction to the Theory of Error-Correcting Codes*, 2nd ed., New York: Wiley, 1989.
- [543] M. PLOTKIN: Binary codes with specified minimum distances, *IEEE Trans. Inform. Th.*, vol. 6, pp. 445–450, 1960.
- [544] K. A. POST: Nonexistence theorems on perfect Lee codes over large alphabets, *Information and Control*, vol. 29, pp. 369–380, 1975.
- [545] C. L. M. van PUL: On bounds on codes, Master’s Thesis, Eindhoven University of Technology, the Netherlands, 99 pp., 1982.
- [546] C. L. M. van PUL: Some distance problems in coding theory, Ph. D. Thesis, Eindhoven University of Technology, the Netherlands, 1987.
- [547] C. L. M. van PUL and T. ETZION: New lower bounds for constant weight codes, *IEEE Trans. Inform. Th.*, vol. 35, pp. 1324–1329, 1989.

- [548] A. O. H. RACSMÁNY: Perfect single-Lee-error-correcting codes, *Studia Sci. Math. Hungar.*, vol. 9, pp. 73–75, 1974.
- [549] T. R. N. RAO: *Error Coding for Arithmetic Processors*, New York: Academic Press, 1974.
- [550] A. RÉNYI: *Foundations of Probability*, New York: Wiley, 1971.
- [551] H. F. H. REUVERS: Some non-existence theorems for perfect codes over arbitrary alphabets, Thesis, Eindhoven University of Technology, the Netherlands, 1977.
- [552] J. RIFÁ and J. PUJOL: Translation invariant propelinear codes, *IEEE Trans. Inform. Th.*, to appear.
- [553] R. L. RIVEST and A. SHAMIR: How to reuse a “write-once” memory, *Information and Control*, vol. 55, pp. 1–19, 1982.
- [554] J. P. ROBINSON: An asymmetric error-correcting ternary code, *IEEE Trans. Inform. Th.*, vol. 24, pp. 258–261, 1978.
- [555] E. R. RODEMICH: Coverings by rook domains, *J. Combinatorial Th.*, Ser. A, vol. 9, pp. 117–128, 1970.
- [556] F. RODIER: On the weights of the elements of the duals of binary BCH codes, *Lecture Notes in Computer Science*, No. 539, pp. 384–390, Springer-Verlag, 1991.
- [557] F. RODIER: On the spectra of the duals of binary BCH codes of designed distance  $\delta = 9$ , *IEEE Trans. Inform. Th.*, vol. 38, pp. 478–479, 1992.
- [558] F. RODIER: On a conjecture of MacWilliams and Sloane, *CISM Courses and Lectures*, No. 339, pp. 89–95, Springer-Verlag, 1993.
- [559] V. RÖDL: On a packing and covering problem, *European J. Combinatorics*, vol. 6, pp. 69–78, 1985.
- [560] C. ROGERS: *Packing and covering*, New York: Cambridge University Press, 1964.
- [561] A. M. ROMANOV: New binary codes with minimal distance three, *Problemy Peredachi Informatsii*, vol. 19, No. 3, pp. 101–102, 1983 (in Russian).
- [562] C. ROOS: A note on the existence of perfect constant weight codes, *Discrete Mathematics*, vol. 47, pp. 121–123, 1983.
- [563] J. E. ROOS: An algebraic study of group and nongroup error-correcting codes, *Information and Control*, vol. 8, pp. 195–214, 1965.
- [564] O. ROTHHAUS: On “bent” functions, *J. Combinatorial Th.*, Ser. A, vol. 20, pp. 300–305, 1976.
- [565] G. ROUX:  $k$ -propriétés dans des tableaux de  $n$  colonnes: cas particulier de la  $k$ -surjectivité et de la  $k$ -permutativité, Thèse, Université Paris 6, France, 133 pp., 1987.
- [566] J. A. RUSH: Thin lattice coverings, *J. London Math. Soc.* (2), vol. 45, pp. 193–200, 1992.

- [567] S. SAIDI: Codes for perfectly correcting errors of limited size, *Discrete Mathematics*, vol. 118, pp. 207–223, 1993.
- [568] P. SAVICKÝ: On the bent Boolean functions that are symmetric, *European J. Combinatorics*, vol. 15, pp. 407–410, 1994.
- [569] J. R. SCHATZ: On the coset leaders of Reed-Muller codes, Ph. D. Thesis, Syracuse University, United States, 1979.
- [570] J. R. SCHATZ: The second order Reed-Muller code of length 64 has covering radius 18, *IEEE Trans. Inform. Th.*, vol. 27, pp. 529–530, 1981.
- [571] W. M. SCHMIDT: *Equations Over Finite Fields: an Elementary Approach*, Berlin: Springer-Verlag, 1976.
- [572] J. SCHÖNHEIM: On maximal systems of  $k$ -tuples, *Studia Sci. Math. Hungar.*, vol. 1, pp. 363–368, 1966.
- [573] J. SCHÖNHEIM: On linear and nonlinear single-error-correcting  $q$ -nary perfect codes, *Information and Control*, vol. 12, pp. 23–26, 1968.
- [574] J. SCHÖNHEIM: Semilinear codes and some combinatorial applications of them, *Information and Control*, vol. 15, pp. 61–66, 1969.
- [575] J. SCHÖNHEIM: Mixed codes, *Proc. Calgary Internat. Conf. on Combinatorial Structures and Their Applications*, p. 385, New York: Gordon and Breach, 1970.
- [576] N. V. SEMAKOV, V. A. ZINOVIEV and G. V. ZAITSEV: Uniformly packed codes, *Problemy Peredachi Informatsii*, vol. 7, No. 1, pp. 38–50, 1971. Translated in: *Problems of Inform. Transm.*, vol. 7, No. 1, pp. 30–39.
- [577] G. SEROUSSI and N. H. BSHOUTY: Vector sets for exhaustive testing of logic circuits, *IEEE Trans. Inform. Th.*, vol. 34, pp. 513–522, 1988.
- [578] G. SEROUSSI and A. LEMPEL: Maximum likelihood decoding of certain Reed-Muller codes, *IEEE Trans. Inform. Th.*, vol. 29, pp. 448–450, 1983.
- [579] C. E. SHANNON: Coding theorems for a discrete source with a fidelity criterion, Institute of Radio Engineers, *Internat. Convention Record*, vol. 7, part 4, pp. 142–163, 1959. Also in: *Key Papers in the Development of Information Theory*, Slepian, Ed., pp. 245–266, IEEE Press, 1973. Also in: *Collected Papers*, Sloane and Wyner, Eds., pp. 325–350, IEEE Press, 1993.
- [580] C. E. SHANNON: *Collected Papers*, Sloane and Wyner, Eds., IEEE Press, 1993.
- [581] H. S. SHAPIRO and D. L. SLOTNICK: On the mathematical theory of error correcting codes, *IBM J. Res. Develop.*, vol. 3, pp. 25–37, 1959.
- [582] I. I. SHARAPUDINOV: Asymptotic properties of Krawtchouk polynomials, *Math. Notes*, vol. 44, pp. 855–862, 1988.
- [583] I. E. SHPARLINSKI: *Computational and Algorithmic Problems in Finite Fields*, Dordrecht: Kluwer, 1992.
- [584] V. M. SIDEL'NIKOV: Weight spectrum of binary Bose-Chaudhuri-Hocquenghem codes, *Problemy Peredachi Informatsii*, vol. 7, No. 1, pp. 14–22, 1971. Translated in: *Problems of Inform. Transm.*, vol. 7, No. 1.

- [585] J. SIMONIS: The minimal covering radius  $t[15, 6]$  of a 6-dimensional binary linear code of length 15 is equal to 4, *IEEE Trans. Inform. Th.*, vol. 34, pp. 1344–1345, 1988.
- [586] J. SIMONIS: Covering radius: improving on the sphere-covering bound, *Lecture Notes in Computer Science*, No. 357, pp. 377–385, Springer-Verlag, 1989.
- [587] G. SIMONYI: On write-unidirectional memory codes, *IEEE Trans. Inform. Th.*, vol. 35, pp. 663–669, 1989.
- [588] T. SKOLEM, P. CHOWLA and D. J. LEWIS: The diophantine equation  $2^{n-2} - 7 = x^2$  and related problems, *Proc. American Math. Soc.*, vol. 10, pp. 663–669, 1959.
- [589] A. N. SKOROBOGATOV: On the covering radius of BCH codes, *Proc. Third Internat. Workshop on Information Theory*, pp. 308–309, Sochi, 1987.
- [590] A. N. SKOROBOGATOV: The parameters of subcodes of algebraic-geometric codes over prime subfields, *Discrete Applied Mathematics*, vol. 33, pp. 205–214, 1991.
- [591] N. J. A. SLOANE: A new approach to the covering radius of codes, *J. Combinatorial Th.*, Ser. A, vol. 42, pp. 61–86, 1986.
- [592] N. J. A. SLOANE: Unsolved problems related to the covering radius of codes, in: *Open Problems in Communication and Computation*, pp. 51–56, Springer-Verlag, 1987.
- [593] N. J. A. SLOANE: Covering arrays and intersecting codes, *J. Combinatorial Designs*, vol. 1, pp. 51–63, 1993.
- [594] N. J. A. SLOANE and E. R. BERLEKAMP: Weight enumerator for second-order Reed-Muller codes, *IEEE Trans. Inform. Th.*, vol. 16, pp. 745–751, 1970.
- [595] N. J. A. SLOANE and R. J. DICK: On the enumeration of cosets of first order Reed-Muller codes, *Proc. IEEE Internat. Conf. on Communications*, vol. 7, pp. 362–366, 1971.
- [596] N. J. A. SLOANE, S. M. REDDY and C. L. CHEN: New binary codes, *IEEE Trans. Inform. Th.*, vol. 18, pp. 503–510, 1972.
- [597] D. H. SMITH: Perfect codes in the graphs  $O_k$  and  $L(O_k)$ , *Glasgow Math. J.*, vol. 21, pp. 169–172, 1980.
- [598] S. L. SNOVER: The uniqueness of the Nordstrom-Robinson and the Golay binary codes, Ph. D. Thesis, Michigan State University, United States, 1973.
- [599] P. SOLÉ: Rayon de recouvrement et schémas d'association, Thèse, Télécom Paris, France, 66 pp., 1987.
- [600] P. SOLÉ: A Lloyd theorem in weakly metric association schemes, *European J. Combinatorics*, vol. 10, pp. 189–196, 1989.
- [601] P. SOLÉ: A limit law on the distance distribution of binary codes, *IEEE Trans. Inform. Th.*, vol. 36, pp. 229–232, 1990.

- [602] P. SOLÉ: Asymptotic bounds on the covering radius of binary codes, *IEEE Trans. Inform. Th.*, vol. 36, pp. 1470–1472, 1990.
- [603] P. SOLÉ: Covering codes and combinatorial optimization, *Lecture Notes in Computer Science*, No. 539, pp. 426–433, Springer-Verlag, 1991.
- [604] P. SOLÉ: Packing radius, covering radius, and dual distance, *IEEE Trans. Inform. Th.*, vol. 41, pp. 268–272, 1995.
- [605] P. SOLÉ and K. G. MEHROTRA: Generalization of the Norse bounds to codes of higher strength, *IEEE Trans. Inform. Th.*, vol. 37, pp. 190–192, 1991.
- [606] P. SOLÉ and P. STOKES: Covering radius, codimension and dual-distance width, *IEEE Trans. Inform. Th.*, vol. 39, pp. 1195–1203, 1993.
- [607] P. SOLÉ and T. ZASLAVSKY: The covering properties of the cycle code of a graph, *Discrete Applied Mathematics*, vol. 45, pp. 63–70, 1993.
- [608] F. I. SOLOVJOVA: On binary nongroup codes, *Methodi Diskr. Analiza*, vol. 37, pp. 65–76, 1981 (in Russian).
- [609] F. I. SOLOVJOVA: Factorization of code-generating disjunctive normal forms, *Methodi Diskr. Analiza*, vol. 47, pp. 66–88, 1988 (in Russian).
- [610] F. I. SOLOVJOVA: A class of binary perfect codes generated by  $q$ -ary codes, *Methodi Diskr. Analiza*, vol. 48, pp. 70–72, 1989 (in Russian).
- [611] F. I. SOLOVJOVA: Perfect codes and their projections, *Proc. 3rd Internat. Workshop on Algebraic and Combinatorial Coding Theory*, pp. 147–150, Voneshta Voda, 1992.
- [612] F. I. SOLOVJOVA: A combinatorial construction of perfect binary codes, *Proc. 4th Internat. Workshop on Algebraic and Combinatorial Coding Theory*, pp. 171–174, Novgorod, 1994.
- [613] J. H. SPENCER: Probabilistic methods, *Graphs and Combinatorics*, vol. 1, pp. 357–382, 1985.
- [614] J. H. SPENCER: Six standard deviations suffice, *Trans. American Math. Soc.*, vol. 289, pp. 679–706, 1985.
- [615] R. G. STANTON: Covering theorems in groups (or: how to win at football pools), in: *Recent Progress in Combinatorics*, Tutte, Ed., pp. 21–36, New York: Academic Press, 1969.
- [616] R. G. STANTON, J. D. HORTON and J. G. KALBFLEISCH: Covering theorems for vectors with special reference to the case of four and five components, *J. London Math. Soc. (2)*, vol. 1, pp. 493–499, 1969.
- [617] R. G. STANTON and J. G. KALBFLEISCH: Covering problems for dichotomized matchings, *Aequationes Math.*, vol. 1, pp. 94–103, 1968.
- [618] R. G. STANTON and J. G. KALBFLEISCH: Intersection inequalities for the covering problem, *SIAM J. Applied Mathematics*, vol. 17, pp. 1311–1316, 1969.
- [619] S. K. STEIN: Factoring by subsets, *Pacific J. Math.*, vol. 22, pp. 523–541, 1967.

- [620] S. K. STEIN: Algebraic tiling, *American Mathematical Monthly*, vol. 81, pp. 445–462, 1974.
- [621] S. K. STEIN: Two combinatorial covering problems, *J. Combinatorial Th.*, Ser. A, vol. 16, pp. 391–397, 1974.
- [622] F. STERBOUL: Le problème du loto, *Proc. Colloque Internat. Mathématiques Discrètes: Codes et Hypergraphes*, Brussels, 1978.
- [623] J. STERN: Approximating the number of error locations within a constant ratio is NP-complete, *Lecture Notes in Computer Science*, No. 673, pp. 325–331, Springer-Verlag, 1993.
- [624] P. STOKES: Some properties of the covering radius of error-correcting codes, Ph. D. Thesis, University of London, England, 1992.
- [625] P. STOKES: The domain of covering codes, *Lecture Notes in Math.*, No. 1518, pp. 170–177, Springer-Verlag, 1993.
- [626] R. STRUIK: Constructive non-existence proofs for covering codes, Presented at Oberwolfach Seminar on Information Theory, 1992.
- [627] R. STRUIK: Constructive non-existence proofs for linear covering codes, *Proc. IEEE Symp. on Information Theory*, p. 369, San Antonio, 1993.
- [628] R. STRUIK: An improvement of the van Wee bound for binary linear covering codes, *IEEE Trans. Inform. Th.*, vol. 40, pp. 1280–1284, 1994.
- [629] R. STRUIK: On the structure of linear codes with covering radius two and three, *IEEE Trans. Inform. Th.*, vol. 40, pp. 1406–1416, 1994.
- [630] R. STRUIK: Covering codes, Ph. D. Thesis, Eindhoven University of Technology, the Netherlands, 106 pp., 1994.
- [631] G. SZEGÖ: *Orthogonal Polynomials*, Colloquium Publications, vol. 23, New York: American Math. Soc., 1959.
- [632] T. SZÖNYI: Small complete arcs in Galois planes, *Geometriae Dedicata*, vol. 18, pp. 161–172, 1985.
- [633] H. TARNANEN: On character sums and codes, *Discrete Mathematics*, vol. 57, pp. 285–295, 1985.
- [634] H. TARNANEN: An elementary proof of the weight distribution formula of the first order shortened Reed-Muller coset code, *Applicable Algebra in Engineering, Communication and Computing*, submitted.
- [635] O. TAUSSKY and J. TODD: Covering theorems for groups, *Ann. Soc. Polonaise de Math.*, vol. 21, pp. 303–305, 1948.
- [636] O. TAUSSKY and J. TODD: Some discrete variable computations, *American Math. Soc. Proc. Symp. in Applied Math.*, pp. 201–209, Providence, 1960.
- [637] J. A. THAS: Two infinite classes of perfect codes in metrically regular graphs, *J. Combinatorial Th.*, Ser. B, vol. 23, pp. 236–238, 1977.
- [638] T. M. THOMPSON: *From Error-Correcting Codes Through Sphere Packings to Simple Groups*, AMS: Carus Mathematical Monographs 21, 1983.

- [639] A. TIETÄVÄINEN: On the nonexistence of perfect 4-Hamming-error-correcting codes, *Ann. Acad. Sci. Fennicae*, Ser. A I, No. 485, pp. 1–6, 1970.
- [640] A. TIETÄVÄINEN: On the nonexistence of perfect codes over finite fields, *SIAM J. Applied Mathematics*, vol. 24, pp. 88–96, 1973. Also in: *Key Papers in the Development of Coding Theory*, Berlekamp, Ed., pp. 252–260, IEEE Press, 1974.
- [641] A. TIETÄVÄINEN: A short proof for the nonexistence of unknown perfect codes over  $GF(q)$ ,  $q > 2$ , *Ann. Acad. Sci. Fennicae*, Ser. A I, No. 580, pp. 1–6, 1974.
- [642] A. TIETÄVÄINEN: Nonexistence of nontrivial perfect codes in case  $q = p_1^r p_2^s$ ,  $e \geq 3$ , *Discrete Mathematics*, vol. 17, pp. 199–205, 1977.
- [643] A. TIETÄVÄINEN: On the covering radius of long binary BCH codes, *Discrete Applied Mathematics*, vol. 16, pp. 75–77, 1987.
- [644] A. TIETÄVÄINEN: Codes and character sums, *Lecture Notes in Computer Science*, No. 388, pp. 3–12, Springer-Verlag, 1989.
- [645] A. TIETÄVÄINEN: An asymptotic bound on the covering radii of binary BCH codes, *IEEE Trans. Inform. Th.*, vol. 36, pp. 211–213, 1990.
- [646] A. TIETÄVÄINEN: An upper bound on the covering radius as a function of the dual distance, *IEEE Trans. Inform. Th.*, vol. 36, pp. 1472–1474, 1990.
- [647] A. TIETÄVÄINEN: On the covering radii of Reed-Muller codes, *Proc. 2nd Internat. Workshop on Algebraic and Combinatorial Coding Theory*, pp. 211–214, Leningrad, 1990.
- [648] A. TIETÄVÄINEN: Covering radius and dual distance, *Designs, Codes and Cryptography*, vol. 1, pp. 31–46, 1991.
- [649] A. TIETÄVÄINEN and A. PERKO: There are no unknown perfect binary codes, *Ann. Univ. Turku*, Ser. A I, No. 148, pp. 3–10, 1971.
- [650] H. C. A. van TILBORG: All binary,  $(n, e, r)$ -uniformly packed codes are known, Memorandum 1975-08, Eindhoven University of Technology, the Netherlands, 1975.
- [651] H. C. A. van TILBORG: Uniformly packed codes, Ph. D. Thesis, Eindhoven University of Technology, the Netherlands, 76 pp., 1976.
- [652] H. C. A. van TILBORG: On the uniqueness (resp. non existence) of certain codes meeting the Griesmer bound, *Information and Control*, vol. 44, pp. 16–35, 1980.
- [653] H. C. A. van TILBORG: *Error-Correcting Codes — A First Course*, Studentlitteratur, Lund, 1993.
- [654] D. T. TODOROV: A table for the coverings of pairs, *Proc. 15th Conf. of the Union of Bulgarian Mathematicians*, pp. 472–481, 1986.
- [655] M. TSFASMAN and S. G. VLÄDUTS: *Algebraic-Geometric Codes*, Dordrecht: Kluwer, 1991.

- [656] P. TURÁN: An extremal problem in graph theory, *Math. Fiz. Lapok*, vol. 48, pp. 436–452, 1941 (in Hungarian).
- [657] P. TURÁN: On the theory of graphs, *Colloq. Math.*, vol. 3, pp. 146–163, 1954.
- [658] P. TURÁN: Research problems, *Magyar Tud. Akad. Mat. Kutató Int. Közl.*, vol. 6, pp. 417–423, 1961.
- [659] R. J. M. VAESENNS, E. H. L. AARTS and J. H. van LINT: Genetic algorithms in coding theory—A table for  $A_3(n, d)$ , *Discrete Applied Mathematics*, vol. 45, pp. 71–87, 1993.
- [660] A. VARDY: The intractability of computing the minimum distance of a code, Preprint, 1996.
- [661] A. VARDY and Y. BE'ERY: Maximum-likelihood soft decision decoding of BCH codes, *IEEE Trans. Inform. Th.*, vol. 40, pp. 546–554, 1994.
- [662] A. VARDY and T. ETZION: Some constructions of perfect codes, *Lecture Notes in Computer Science*, No. 673, pp. 344–354, Springer-Verlag, 1993.
- [663] R. R. VARSHAMOV: Estimate of the number of signals in error-correcting codes, *Dokl. Akad. Nauk SSSR*, vol. 117, pp. 739–741, 1957 (in Russian).
- [664] J. L. VASILIEV: On nongroup close-packed codes, *Problemy Kibernetiki*, vol. 8, pp. 337–339, 1962 (in Russian). Also in: *Key Papers in the Development of Coding Theory*, Berlekamp, Ed., p. 100, IEEE Press, 1974.
- [665] J. L. VASILIEV and F. I. SOLOVJOVA: Interdependence between perfect binary codes and their projections, *Proc. Seventh Joint Swedish-Russian Internat. Workshop on Information Theory*, pp. 239–242, St-Petersburg, 1995.
- [666] J. L. VASILIEV and F. I. SOLOVJOVA: On code-generating factorization of  $n$ -dimensional unit cube and of perfect binary codes, *Problemy Peredachi Informatsii*, submitted.
- [667] E. D. VELIKOVA: Bounds on covering radius of linear codes, *Comptes-Rendus de l'Académie Bulgare des Sciences*, vol. 41, pp. 13–16, 1988.
- [668] E. D. VELIKOVA: Covering radius of some cyclic codes, *Proc. Internat. Workshop on Algebraic and Combinatorial Coding Theory*, pp. 165–169, Varna, 1988.
- [669] E. D. VELIKOVA: A generalization of some upper bounds on covering radius under an arbitrary additive metric, *Problems of Control and Information Th.*, vol. 19, No. 5–6, pp. 445–450, 1990.
- [670] E. D. VELIKOVA: The covering radius of two-dimensional codes over  $GF(4)$ , *Proc. 4th Internat. Workshop on Algebraic and Combinatorial Coding Theory*, pp. 190–193, Novgorod, 1994.
- [671] E. D. VELIKOVA and K. N. MANEV: The covering radius of cyclic codes of lengths 33, 35 and 39, *Annuaire de l'Université de Sofia*, T. 81, pp. 215–223, 1987.
- [672] T. VERHOEFF: An updated table of minimum-distance bounds for binary linear codes, *IEEE Trans. Inform. Th.*, vol. 33, pp. 665–680, 1987.

- [673] S. G. VLÄDUTS and A. N. SKOROBOGATOV: Covering radius for long BCH codes, *Problemy Peredachi Informatsii*, vol. 25, No. 1, pp. 38–45, 1989. Translated in: *Problems of Inform. Transm.*, vol. 25, No. 1, pp. 28–34.
- [674] E. W. WEBER: On the football pool problem for 6 matches: a new upper bound, *J. Combinatorial Th.*, Ser. A, vol. 35, pp. 106–108, 1983.
- [675] G. J. M. van WEE: Improved sphere bounds on the covering radius of codes, *IEEE Trans. Inform. Th.*, vol. 34, pp. 237–245, 1988.
- [676] G. J. M. van WEE: More binary covering codes are normal, *IEEE Trans. Inform. Th.*, vol. 36, pp. 1466–1470, 1990.
- [677] G. J. M. van WEE: Covering codes, perfect codes, and codes from algebraic curves, Ph. D. Thesis, Eindhoven University of Technology, the Netherlands, 209 pp., 1991.
- [678] G. J. M. van WEE: On the non-existence of certain perfect mixed codes, *Discrete Mathematics*, vol. 87, pp. 323–326, 1991.
- [679] G. J. M. van WEE: Bounds on packings and coverings by spheres in  $q$ -ary and mixed Hamming spaces, *J. Combinatorial Th.*, Ser. A, vol. 57, pp. 117–129, 1991.
- [680] G. J. M. van WEE: Some new lower bounds for binary and ternary covering codes, *IEEE Trans. Inform. Th.*, vol. 39, pp. 1422–1424, 1993.
- [681] G. J. M. van WEE, G. D. COHEN and S. LITSYN: A note on perfect multiple coverings of the Hamming space, *IEEE Trans. Inform. Th.*, vol. 37, pp. 678–682, 1991.
- [682] V. K. WEI: Generalized Hamming weights for linear codes, *IEEE Trans. Inform. Th.*, vol. 37, pp. 1412–1418, 1991.
- [683] P. M. WEICHSEL: Dominating sets in  $n$ -cubes, *J. Graph Th.*, vol. 18, No. 5, pp. 479–488, 1994.
- [684] A. WEIL: On some exponential sums, *Proc. Nat. Acad. Sci.*, vol. 34, pp. 204–207, 1948.
- [685] L. T. WILLE: The football pool problem for 6 matches: a new upper bound obtained by simulated annealing, *J. Combinatorial Th.*, Ser. A, vol. 45, pp. 171–177, 1987.
- [686] L. T. WILLE: Personal communication, 1987.
- [687] L. T. WILLE: Improved binary code coverings by simulated annealing, *Congressus Numerantium*, vol. 73, pp. 53–58, 1990.
- [688] L. T. WILLE: New binary covering codes obtained by simulated annealing, *IEEE Trans. Inform. Th.*, vol. 42, pp. 300–302, 1996.
- [689] F. M. J. WILLEMS: Converses for write-unidirectional memories, Report 89-E-220, Eindhoven University of Technology, the Netherlands, 12 pp., 1989.
- [690] H. S. WITSENHAUSEN and A. D. WYNER: On storage media with aftereffects, *Information and Control*, vol. 56, pp. 199–211, 1983.

- [691] J. K. WOLF, A. D. WYNER, J. ZIV and J. KÖRNER: Coding for a “write-once” memory, *AT & T Bell Lab. Tech. J.*, vol. 63, No. 6, 1984.
- [692] J. WOLFMANN: Codes projectifs à deux poids, “caps” complets et ensembles de différences, *J. Combinatorial Th.*, Ser. A, vol. 23, pp. 208–222, 1977.
- [693] J. WOLFMANN: Résultats sur les paramètres des codes linéaires, *Revue CETHEDEC*, vol. 2, pp. 25–33, 1979.
- [694] J. WOLFMANN: The weight of orthogonals of certain cyclic codes or extended Goppa codes, *Lecture Notes in Computer Science*, No. 357, pp. 476–480, Springer-Verlag, 1989.
- [695] A. D. WYNER and J. ZIV: On communication of analog data from a bounded source space, *Bell Syst. Tech. J.*, vol. 48, pp. 3139–3172, 1969.
- [696] Ø. YTREHUS: Binary  $[18,11]_2$  codes do not exist—nor do  $[64,53]_2$  codes, *IEEE Trans. Inform. Th.*, vol. 37, pp. 349–351, 1991.
- [697] S. K. ZAREMBA: A covering theorem for abelian groups, *J. London Math. Soc.*, vol. 26, pp. 71–72, 1950.
- [698] S. K. ZAREMBA: Covering problems concerning abelian groups, *J. London Math. Soc.*, vol. 27, pp. 242–246, 1952.
- [699] B. ZELINKA: Domatic numbers of cube graphs, *Math. Slovaca*, vol. 32, pp. 117–119, 1982.
- [700] G. ZÉMOR: Problèmes combinatoires liés à l’écriture sur des mémoires, Thèse, Télécom Paris, France, 109 pp., 1989.
- [701] G. ZÉMOR: Subset sums in binary spaces, *European J. Combinatorics*, vol. 13, pp. 221–230, 1992.
- [702] G. ZÉMOR and G. D. COHEN: Error-correcting WOM-codes, *IEEE Trans. Inform. Th.*, vol. 37, pp. 730–734, 1991.
- [703] G. ZÉMOR and G. D. COHEN: Application of coding theory to interconnection networks, *Discrete Applied Mathematics*, vol. 37/38, pp. 553–562, 1992.
- [704] Z. ZHANG: Linear inequalities for covering codes: Part I—pair covering inequalities, *IEEE Trans. Inform. Th.*, vol. 37, pp. 573–582, 1991.
- [705] Z. ZHANG and C. LO: Linear inequalities for covering codes: Part II—triple covering inequalities, *IEEE Trans. Inform. Th.*, vol. 38, pp. 1648–1662, 1992.
- [706] Z. ZHANG and C. LO: Lower bounds on  $t[n, k]$  from linear inequalities, *IEEE Trans. Inform. Th.*, vol. 38, pp. 194–197, 1992.
- [707] V. A. ZINOVIEV: Codes for correlation multi-address selection, Ph. D. Thesis, Moscow Institute of Physics and Technology, USSR, 200 pp., 1970 (in Russian).
- [708] V. A. ZINOVIEV: On generalized concatenated codes, *Colloquia Mathematica Societatis János Bolyai*, vol. 16, pp. 587–592, 1975.
- [709] V. A. ZINOVIEV: Generalized cascade codes, *Problemy Peredachi Informatsii*, vol. 12, No. 1, pp. 5–15, 1976. Translated in: *Problems of Inform. Transm.*, vol. 12, No. 1, pp. 2–9.

- [710] V. A. ZINOVIEV: Combinatorial methods of construction and analysis of nonlinear error-correcting codes, Doctor of Sciences Diss., Computer Centre of Russian Academy of Sciences, Moscow, 300 pp., 1988 (in Russian).
- [711] V. A. ZINOVIEV and G. L. KATSMAN: Universal codes families, *Problemy Peredachi Informatsii*, vol. 29, No. 2, pp. 3–8, 1993. Translated in: *Problems of Inform. Transm.*, vol. 29, No. 2, pp. 95–100.
- [712] V. A. ZINOVIEV and V. K. LEONTIEV: On perfect codes, *Problemy Peredachi Informatsii*, vol. 8, No. 1, pp. 26–35, 1972. Translated in: *Problems of Inform. Transm.*, vol. 8, No. 1, pp. 17–24.
- [713] V. A. ZINOVIEV and V. K. LEONTIEV: The nonexistence of perfect codes over Galois fields, *Problemy Upravleniya i Teorii Informatsii*, vol. 2, No. 2, pp. 123–132, 1973. Translated in: *Problems of Control and Information Th.*, vol. 2, No. 2, pp. 16–24.
- [714] V. A. ZINOVIEV and S. LITSYN: Dual distance of BCH codes, *Problemy Peredachi Informatsii*, vol. 22, No. 4, pp. 29–34, 1986. Translated in: *Problems of Inform. Transm.*, vol. 22, No. 4, pp. 272–277.

# Index

- acceptable
  - coordinate, 86, 379
  - partition, 91, 379
- adding a parity check, 45, 62, 93
- ADS, 89, 91, 379
- algorithm
  - greedy, 322, 435, 452, 453, 492
  - polynomial-time, 480
  - nondeterministic, 480
- alphabet, 15
- amalgamated direct sum, 89, 91, 379
- bad vector, 86
- ball, 16
- BDS, 110
- bent function, 259
- Berlekamp-Gale game, 13, 353
- binomial coefficient, 28
- block, 52
- blockwise direct sum, 110
- Boolean functions, 239
- bound
  - Carlitz-Uchiyama, 49
  - Chernoff, 334
  - Delsarte, 232, 248, 256, 268, 280, 419
  - Elias, 341
  - excess, 152, 153, 156, 171, 181
  - Gilbert-Varshamov, 338
  - Griesmer, 219
  - Hamming, 17, 221, 286, 339
  - Johnson, 184, 340
  - linear programming, 341
  - McEliece-Rodemich-Rumsey-Welch, 342
  - Norse, 235, 241
  - Plotkin, 339
- redundancy, 217
- Schönheim, 52
- Singleton, 50
- sphere-covering, 18, 146, 286, 333
- sphere-packing, 17, 286
  - using linear inequalities, 158, 365
- cap in a projective geometry, 447
  - complete, 447
- cascading, 72, 330
- Cayley graph, 14, 439
- cellular telecommunications, 14
- character, 43, 417
  - additive, 24, 44, 263
  - multiplicative, 44
  - trivial, 44, 263
- characteristic of a field, 41
- Christoffel-Darboux formula, 30
- chromatic number, 55, 224
- cloud encoding, 451
- code, 15
  - $p$ -seminormal, 117
  - $q$ -ary, 15
  - $q$ -normal, 113
  - $t$ -subnormal, 113
  - abnormal, 86, 102
  - arithmetic, 314
  - balanced, 149
  - BCH, 105, 262, 430
    - nonprimitive, 48, 265, 276
    - primitive, 48, 262
  - binary, 15
  - bipartite, 476
  - concatenated, 299
    - generalized, 299
  - constant weight, 55, 474
  - contracted, 98, 121

- covering, 2
- cyclic, 45, 279
  - nonprimitive, 46
  - primitive, 46
- dual, 20
- dual of BCH, 263, 279
- equivalent, 16, 296
- even weight, 21
- extended, 45, 62, 93, 385
- generalized uniformly packed, 318, 357
- Goethals, 52
- Golay, 51
  - binary, 51, 286, 426
  - ternary, 51, 289, 401
- Goppa, 50, 265, 280
  - irreducible, 51
- Hadamard, 51
- Hamming, 46, 106, 111, 119, 286
  - extended, 47
  - extended shortened, 47
  - shortened, 47
- inner, 299
- isomorphic, 296
- linear, 19, 295
- maximal, 18, 20, 424
- maximum distance separable, 50
- MDS, 50, 78, 83
- mixed, 24
- nearly perfect, 313, 357
- nonlinear, 20, 295
- nonsystematic, 316
- Nordstrom-Robinson, 52
- normal, 86
  - of full rank, 304
- optimal, 18, 20
- outer, 299
- perfect, 18, 47, 51, 113, 286, 405, 415
  - $p$ -radius, 467
  - $q$ -ary, 307
  - extended, 301
  - mixed, 310
- piecewise constant, 64, 381, 386
- Preparata, 51, 111, 311, 467
- punctured, 51
  - projective, 98
  - punctured, 45, 62, 386
  - quadratic residue, 50
  - Reed-Muller, 47, 238
    - first order, 47, 119, 241
    - of arbitrary order, 251
    - of order 2, 247
    - of order  $m - 3$ , 247
  - punctured, 48
- Reed-Solomon, 49, 265, 281
  - doubly extended, 49, 78
  - extended, 49
  - shortened, 50
  - triply extended, 49
- repetition, 22
- residual, 219
- self-complementary, 462
- self-dual, 50, 265, 280
  - doubly-even, 50
    - of type I, 50
    - of type II, 50
  - seminormal, 115
  - shortened, 45, 424
  - simplex, 48, 119, 241, 363
  - strongly  $p$ -seminormal, 82
  - strongly uniformly packed, 313, 357
  - subnormal, 109, 117
  - trivial, 15
  - uniformly packed
    - of the  $j$ -th order, 314, 357
    - of the first order, 314
  - uniquely decodable, 57
- codeword, 15
- codimension, 223
- codimension (or redundancy), 120
- complement of a vector, 19
- completeness, 481
- complexity, 479
- componentwise product of vectors, 19
- compression with distortion, 10
- conjugate, 45
- constraint
  - symmetric, 448
  - translation-invariant, 449
- constraint graph, 448

- construction
  - $(\mathbf{u}, \mathbf{u} + \mathbf{v})$ , 66, 330
  - ADS, 89, 91, 379
  - amalgamated direct sum, 89, 91, 379
  - BDS, 110
  - blockwise direct sum, 110
  - cascading, 72, 330
  - Davydov, 129
  - direct sum, 63
  - matrix, 70, 187, 368, 381, 386, 396
  - subspace direct sum, 115
- constructive sequence, 491
- coset, 22
  - leader, 22
  - elected, 22
  - weight, 22
- coset encoding, 423
- cover, 17, 461
- covering, 2
  - $L$ -covering, 356, 446, 461
  - perfect, 462
  - $m$ -covering, 356
  - perfect, 356
  - by spheres all of  $\neq$  radii, 470
  - group, 451, 453
  - heterodox, 461
  - multiple, 356, 372
    - of deep holes, 356, 385
    - perfect, 373
    - with repeated words, 372
  - of a sphere by spheres, 473
  - weighted, 356
    - perfect, 356
- covering by coverings, 82
- covering number, 452
- covering radius, 17
  - $\mu$ -fold, 378
  - normalized, 319
- cyclic
  - code, 45
  - group, 41
- cylinder, 442
- data compression, 10
- decision problem, 480
- decoding, 11
- decomposition of tilings, 412
- deep hole, 17
- degree of a vertex, 55
- density
  - $m$ -density, 355
  - of a code, 18, 112, 142, 328
- derandomization, 491
- design, 52
  - covering, 52
  - pair covering, 52, 159
- diameter of a graph, 440
- diameter of a set, 36
- dimension of a code, 20
- direct sum, 63
- discrepancy, 333
- distance
  - $i$ -th, 435
  - designed, 262
  - dual, 21, 26, 227
    - normalized, 319
    - graphic, 55, 440
    - Hamming, 16
    - minimum, 16
      - normalized, 319
  - distance distribution, 25, 417
  - domatic number, 452
  - dual
    - code, 20
    - distance, 21, 26, 227
      - normalized, 319
    - spectrum, 25, 227
  - edge of a graph, 55
  - efficiency of a WOM-code, 425
  - entropy function, 32
  - erasure, 11
  - error-correcting capability, 17
  - even vector, 16
  - excess, 151
    - $r$ -excess, 177
  - extending a code, 45
  - field, 15, 18, 41
    - finite, 18, 40
  - football pools, 12, 393

- generator element, 41
- generator matrix, 20
- graph, 55
  - Cayley, 14, 439
  - constraint, 448
  - Kneser, 224
- graphic distance, 55, 440
- group, 40
  - abelian (or commutative), 40
  - cyclic, 41
- GUAVA, 57
- Hamming
  - distance, 16
  - space, 15
  - weight, 16
- hereditary set, 36
- hypercube, 453
- hyperedge, 55
- hypergraph, 55, 492
  - $\Delta$ -regular, 55, 492
  - $b$ -uniform, 55, 492
- independence number, 55, 224
- independent set of a graph, 224
- inequality
  - induced, 160
  - pair covering, 160
- interconnection network, 12
- intersection of spheres, 33
- iterative improvement, 79
- kernel, 316
- Kneser graph, 224
- Krawtchouk
  - expansion, 30
  - polynomial, 25, 417
- Kronecker product, 51
- Latin square
  - mutually orthogonal, 83
- layer, 17
- Lee metric, 314
- lemma
  - Bassalygo-Elias, 340
- length function, 119
- length of a code, 15
- list decoding, 368
- Lloyd polynomial, 29, 290, 418
- Lloyd theorem, 290
  - for  $L$ -codes, 475
  - for mixed codes, 317
  - for tiles, 417
  - for weighted coverings, 359
- local search, 79
- MacWilliams identities, 25, 184, 227, 417
- matching, 484
- matrices
  - $R$ -closed, 132
- matrix
  - ( $R, R_1^*$ )-complementary, 132
  - $s$ -independent, 76
  - $s$ -surjective, 76, 455, 490
  - adjacency, 55
  - generator, 20
  - Hadamard, 51
  - Sylvester-type, 238
  - parity check, 21
- matrix factor, 249
- memory
  - constrained, 448
  - error correction, 456
  - defective, 435, 450, 455, 490
  - efficient, 457
  - reluctant, 450, 453
  - suspicious, 459
  - write-isolated, 449
  - write-once, 12, 423, 448
    - error correction, 428
    - the nonlinear case, 433
    - write-unidirectional, 449
- metric, 16
- minimum distance, 16
  - normalized, 319
- minimum weight, 21
- monotonicity property, 98
- nonconstructive bounds, 491
- norm, 86
  - $\mu$ -fold, 379
  - minimum, 86
  - of BCH codes, 277

- of Reed-Muller codes, 245
- normal
  - $\mu$ -fold, 379
  - $\mu$ -fold  $r$ -covering, 379
- normalized
  - covering radius, 319
  - dual distance, 319
  - minimum distance, 319
- NP-complete problem, 480
- odd vector, 16
- orphan, 258
- orthogonal array of strength  $s$ , 27
- orthogonal vectors, 20
- packing
  - $L$ -packing, 475
  - $m$ -packing, 357
- packing radius, 17
- packings by coverings, 451
- parity check, 45
  - generalized, 297
- parity check matrix, 21
- path, 55
- perfect segmentation, 304
- point, 15
- polynomial
  - annihilator, 359
  - generalized Lloyd, 359
  - Hermite, 32
  - irreducible, 42
  - Krawtchouk, 25, 417
  - Lloyd, 29, 290, 418
- polynomial hierarchy, 481
- polynomial reduction, 480
- polynomial ring, 41
- primitive element, 43
- projection, 24
- puncturing a code, 45, 62, 386
- qualitative independence, 494
- radius
  - covering, 17
  - multicovering, 472
  - Newton, 57
  - of a weighted covering, 356
- packing, 17
- rank, 304
- rate of a code, 319
- ring, 41
  - commutative, 41
- satisfiability
  - 3-satisfiability, 481
- saving one coordinate, 127
- scalar multiplication, 19
- scalar product of vectors, 20
- semi-constructive sequence, 491
- shell, 17
- shortening a code, 45, 424
- signature, 97
- simulated annealing, 79
- speech coding, 13
- sphere, 16
  - $L$ -sphere, 132, 403, 446, 461
- stabilizer of a tile, 409
- stable set of a graph, 224
- standard partition, 22
- Steiner system, 52, 66
- Stirling's formula, 32
- strength of a code, 27
- subcode
  - even weight, 16
  - odd weight, 16
  - subfield, 266
- subnorm, 91
  - $\mu$ -fold, 379
  - $t$ -subnorm, 110
  - minimum, 91
- subnormal
  - $\mu$ -fold, 379
  - $\mu$ -fold  $r$ -covering, 379
- subset sum, 14
- subspace direct sum, 115
- sum-free set, 446
  - maximal, 144, 446
- supercode lemma, 222, 266, 424
- support of a vector, 16
- syndrome of a vector, 21
- taboo search, 80
- theorem
  - Bombieri, 280

- Deligne, 272
- Johnson-Stein-Lovász, 322, 453,
  - 492
- Kleitman, 38, 225
- Lang-Weil, 277
- Weil-Carlitz-Uchiyama, 263
- tile, 404
  - linear, 405
  - nonperiodic, 409
  - periodic, 409
- tiling, 404
  - of full rank, 415
  - proper, 412
- time complexity function, 480
- trace function, 44, 262
- translate of a code, 19
- transversal in a hypergraph, 55
- transversal problem, 491
- travelling salesman, 480
- triangle inequality, 16
- unequal protection, 476
- union of spheres, 33
- urcoset, 258
- vertex of a graph, 55
- VLSI testing, 490
- Voronoi region, 22
- weight
  - Hamming, 16
  - minimum, 21
- weight distribution, 25
- wit, 423
- word, 15
- zeros of Krawtchouk polynomials, 32,
  - 234