Coding Theory

CO 331

Alfred Menezes

LaTeXed by Sibelius Peng

Preface

Disclaimer Much of the information on this set of notes is transcribed directly/indirectly from the lectures of CO 331 during Winter 2021 as well as other related resources. I do not make any warranties about the completeness, reliability and accuracy of this set of notes. Use at your own risk.

For any questions, send me an email via https://notes.sibeliusp.com/contact.

You can find my notes for other courses on https://notes.sibeliusp.com/.

Sibelius Peng

Contents

Preface 1

Introduction 3

1 Fundamentals 5
1.1 Basic Definitions and Concepts 5
1.2 Decoding Strategy 7
1.3 Error Correcting & Detecting Capabilities of a Code 9

2 Introduction to Finite Fields 12
2.1 Definitions 12
2.2 Finite fields: Non-existence 14
2.3 Existence of finite fields 15
2.4 Properties of finite fields 18

3 Linear codes 21
3.1 Definition 21
3.2 Properties of Linear Codes 21
3.3 The Dual Code 24
3.4 Parity-Check Matrix 25
3.5 Syndrome Decoding 26

4 Golay codes 28

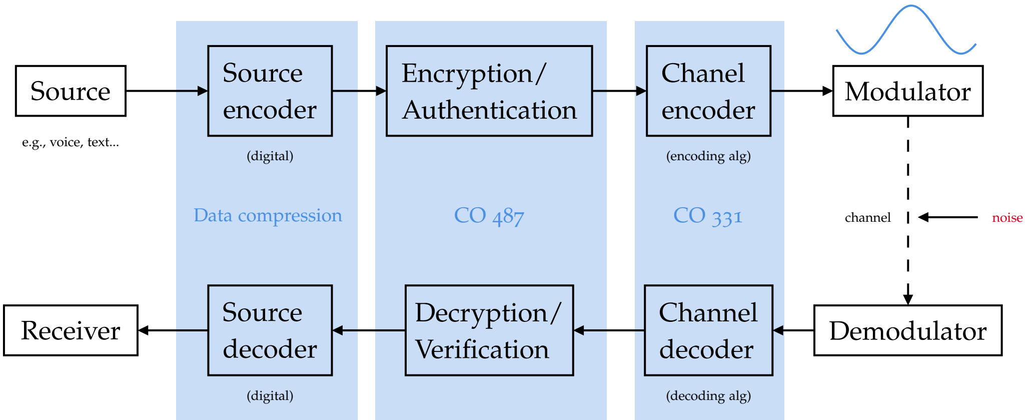
5 Cyclic codes 29
5.1 The Polynomial Ring $R = F[x]/(x^n - 1)$ 29
5.2 Ideals of $R = F[x]/(x^n - 1)$ 30
5.3 Dimension of a Cyclic Code 31
5.4 GM of a Cyclic Code 31
5.5 The Dual Code of a Cyclic Code 31

6 BCH codes 32
6.1 Subfields and Extension fields 32
6.2 Minimal Polynomials 32
6.3 Computing Minimal Polynomials 33
6.4 Factoring $x^n - 1$ over $\mathrm{GF}(q)$ 33
6.5 BCH Codes: Definition 34
6.6 BCH Bound 34
6.7 BCH Decoding 35

Introduction

Coding theory is about clever ways of adding redundancy to messages to allow (efficient) error detection and error correction.

Here is our communication model:



Example: Parity Code

Encoding algorithm Add a 0 bit to the (binary) msg m if the number of 1's in m is even; else add a 1 bit.

Decoding algorithm If the number of 1's in a received msg r is even, then accept r; else declare that an error has occurred.

Example: Replication Code

<table>
<tr><th>Source msgs</th><th>Codeword</th><th># err/codeword (always) detected</th><th># err/codeword (always) corrected *</th><th>Information rate</th></tr>
<tr><td>0</td><td>0</td><td rowspan="2">0</td><td rowspan="2">0</td><td rowspan="2">1</td></tr>
<tr><td>1</td><td>1</td></tr>
<tr><td>0</td><td>00</td><td rowspan="2">1</td><td rowspan="2">0</td><td rowspan="2">$\frac{1}{2}$</td></tr>
<tr><td>1</td><td>11</td></tr>
<tr><td>0</td><td>000</td><td rowspan="2">2</td><td rowspan="2">1</td><td rowspan="2">$\frac{1}{3}$</td></tr>
<tr><td>1</td><td>111</td></tr>
<tr><td>0</td><td>0000</td><td rowspan="2">3</td><td rowspan="2">1</td><td rowspan="2">$\frac{1}{4}$</td></tr>
<tr><td>1</td><td>1111</td></tr>
<tr><td>0</td><td>00000</td><td rowspan="2">4</td><td rowspan="2">2</td><td rowspan="2">$\frac{1}{5}$</td></tr>
<tr><td>1</td><td>11111</td></tr>
</table>

$\xrightarrow{\text{encoding algorithm}}$

*: using "nearest neighbour decoding"

Goal of Coding Theory

Design codes so that:

1. High information rate
2. High error-correcting capability
3. Efficient encoding & decoding algorithms

Course Overview

This course deals with *algebraic methods* for designing good (block) codes. The focus is on error correction (not on error detection). These codes are used in wireless communications, space probes, CD/DVD players, storage, QR codes, etc.

Some modern stuff are not covered: Turbo codes, LDPC codes, Raptor codes, . . . Their math theories are not so elegant as algebraic codes.

The big picture

Coding theory in its broadest sense deals with techniques for the *efficient*, *secure* and *reliable* transmission of data over communication channels that may be subject to *non-malicious errors* (noise) and *adversarial intrusion*. The latter includes passive intrusion (eavesdropping) and active intrusion (injection/deletion/modification).

1

Fundamentals

1.1 Basic Definitions and Concepts

alphabet

An **alphabet** A is a finite set of $q \geq 2$ symbols.

word

A **word** is a finite sequence of symbols from A (also: vector, tuple).

length

The **length** of a word is the number of symbols it has.

code

A **code** C over A is a set of words (of size ≥ 2).

codeword

A **codeword** is a word in the code C.

block code

A **block code** is a code in which all codewords have the same length.

A **block code of length** n **containing** M **codewords over** A is a subset $C \subseteq A^n$ with $|C| = M$. C is called an $[n, M]$-code over A.

Example:

$A = \{0, 1\}$. $C = \{00000, 11100, 00111, 10101\}$ is a $[5, 4]$-code over $\{0, 1\}$.

Messages		Codewords
00	$\to$	00000
10	$\to$	11100
01	$\to$	00111
11	$\to$	10101

Encoding of messages (1-1 map)

Assumptions about the communications channel

(1) The channel only transmits symbols from A ("hard decision decoding").

(2) No symbols are deleted, added, interchanged or transposed during transmission.

(3) The channel is a q-symmetric channel:

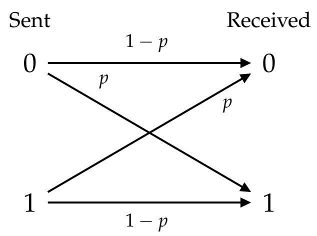
Let $A = \{a_1, \ldots, a_q\}$. Let $X_i =$ the i^{th} symbol sent. Let $Y_i =$ the i^{th} symbol received. Then for all $i \geq 1$, and all $i \leq j, k \leq q$,

$$\Pr(Y_i = a_j | X_i = a_k) = \begin{cases} 1 - p, & \text{if } j = k \\ \frac{p}{q-1}, & \text{if } j \neq k. \end{cases}$$

p is called the **symbol error probability** of the channel $(0 \leq p \leq 1)$.

Binary Symmetric Channel (BSC)

A 2-symmetric channel is called a binary symmetric channel.



For a BSC:

1. If $p = 0$, the channel is *perfect*.
2. If $p = 1/2$, the channel is *useless*.
3. If $1/2 < p \leq 1$, then flipping all received bits converts the channel to a BSC with $0 \leq p < 1/2$.
4. Henceforth, we will assume that $0 < p < 1/2$ for a BSC.

Exercise:

For a q-symmetric channel, show that one can take $0 < p < \frac{q-1}{q}$ WLOG.

One can first consider the case $q = 3$.

information rate

The **information rate** (or rate) R of an $[n, M]$-code C over A is $R = \frac{\log_q M}{n}$.

If C encodes messages that are k-tuples over A (so $M = |A^k| = q^k$), then $R = \frac{k}{n}$.

Note:
$0 \le R \le 1$. Ideally, R should be close to 1.

Example:
The rate of the binary code $C = \{00000, 11100, 00111, 10101\}$ is $R = \frac{2}{5}$.

Hamming distance

The **Hamming distance** (or distance) between two n-tuples over A is the number of coordinate positions in which they differ.

The Hamming distance (or distance) of an $[n, M]$-code C is $d(C) = \min\{d(x, y) : x, y \in C, x \neq y\}$.

Example:
The distance of $C = \{00000, 11100, 00111, 10101\}$ is $d(C) = 2$.

Theorem 1.1: properties of Hamming distance

For all $x, y, z \in A^n$,

1. $d(x, y) \ge 0$, with $d(x, y) = 0$ iff $x = y$.
2. $d(x, y) = d(y, x)$.
3. $d(x, y) + d(y, z) \ge d(x, y)$ ($\triangle$ inequality).

1.2 Decoding Strategy

Example:
Let $C = \{00000, 11100, 00111, 10101\}$. C is a $[5, 4]$-code over $\{0, 1\}$ (a binary code).

Error Detection If C is used for error detection only, the strategy is the following: A received word $r \in A^n$ is accepted if and only if $r \in C$.

Error Correction Let C be an $[n, M]$-code over A with distance d. Suppose $c \in C$ is transmitted, and $r \in A^n$ is received. The (channel) decoder must decide one of the following:

(i) No errors have occurred; *accept* r.

(ii) Errors have occurred; *correct*[1] (*decode*) r to a codeword $c \in C$?

(iii) Errors have occurred; *no correction is possible*.

Nearest Neighbour Decoding

(i) Incomplete Maximum Likelihood Decoding (IMLD):

If there is a unique codeword $c \in C$ such that $d(r, c)$ is minimum, then correct r to c. If no such c exists, then report that errors have occurred, but correction is not possible (ask for retransmission, or disregard information).

(ii) Complete Maximum Likelihood Decoding (CMLD):

[1] Error correction does not guarantee that the channel decoder always makes the correct decision. For example, $00000 \xrightarrow{\text{transmit}} 11100$ which is accepted.

Same as IMLD, except that if there are two or more $c \in C$ for which $d(r, c)$ is minimum, correct r to an arbitrary one of these.

Is IMLD a reasonable strategy?

Theorem 1.2

IMLD chooses the codeword c for which the conditional probability

$$P(r|c) = P(r \text{ is received}|c \text{ is sent})$$

is largest.

Proof:
Suppose $c_1, c_2 \in C$ with $d(c_1, r) = d_1$ and $d(c_2, r) = d_2$. Suppose $d_1 > d_2$.

Now

$$P(r|c_1) = (1-p)^{n-d_1}\left(\frac{p}{q-1}\right)^{d_1}$$

and

$$P(r|c_2) = (1-p)^{n-d_2}\left(\frac{p}{q-1}\right)^{d_2}$$

So,

$$\frac{P(r|c_1)}{P(r|c_2)} = (1-p)^{d_2-d_1}\left(\frac{p}{q-1}\right)^{d_1-d_2} = \left(\frac{p}{(1-p)(q-1)}\right)^{d_1-d_2}$$

Recall

$$p < \frac{q-1}{q} \implies pq < q-1 \implies 0 < q - pq - 1$$

$$\implies p < p + q - pq - 1 \implies p < (1-p)(q-1) \implies \frac{p}{(1-p)(q-1)} < 1$$

Hence

$$\frac{P(r|c_1)}{P(r|c_2)} < 1$$

and so

$$P(r|c_1) < P(r|c_2)$$

and the result follows. □

Minimum Error Probability Decoding (MED)

An *ideal strategy* would be to correct r to a codeword $c \in C$ for which $P(c|r) = P(r \text{ is received}|c \text{ is sent})$ is largest. This is MED.

Example: (IMLD/CMLD) is not the same as MED

Consider $C = \{\underset{c_1}{\underset{\uparrow}{000}}, \underset{c_2}{\underset{\uparrow}{111}}\}$. Suppose $P(c_1) = 0.1$ and $P(c_2) = 0.9$. Suppose $p = \frac{1}{4}$ (for a BSC).

Suppose $r = 100$ is the received word. Then

$$P(c_1|r) = \frac{P(r|c_1)\cdot P(c_1)}{P(r)} = \frac{p(1-p)^2 \times 0.1}{P(r)} = \frac{9}{640}\cdot\frac{1}{P(r)}$$
$$P(c_2|r) = \frac{P(r|c_2)\cdot P(c_2)}{P(r)} = \frac{(1-p)p^2 \times 0.9}{P(r)} = \frac{27}{640}\cdot\frac{1}{P(r)}$$

So, MED decodes r to c_2. But IMLD decodes r to c_1.

IMLD vs. MED

- IMLD maximizes $P(r|c)$. MED maximizes $P(c|r)$.
- (i) MED has the drawback that the decoding algorithm depends on the probability distribution of source messages.

  (ii) If all source messages are equally likely, then CMLD and MED are equivalent:

$$P(r|c_i) = P(c_i|r) \cdot P(c_i)/P(r) = P(c_i|r) \cdot \underbrace{\left[\frac{1}{M \cdot P(r)}\right]}_{\substack{\text{does not} \\ \text{depend on } c_i}}$$

  (iii) In practice IMLD (or CMLD) is used.
- In this course, we will use IMLD/CMLD.

1.3 Error Correcting & Detecting Capabilities of a Code

Detection Only

Strategy: If r is received, then accept r if and only if $r \in C$.

e-error detecting code

A code C is an **e-error detecting code** if the decoder always makes the correct decision if e or fewer errors per codeword are introduced by the channel.

Example:

Consider $C = \{000, 111\}$.

C is a 2-error detecting code.

C is not a 3-error detecting code.

Theorem 1.3

A code C of distance d is a $(d-1)$-error detecting code (but is not a d-error detecting code).

Proof:

Suppose $c \in C$ is sent.

If no errors occur, then c is received (and is accepted).

Suppose that # of errors is ≥ 1 and $\leq d-1$; let r be the received word. Then $1 \leq d(r,c) \leq d-1$, so $r \notin C$. Thus r is rejected. This proves that it is $(d-1)$-error detecting code.

Since $d(C) = d$, there exist $c_1, c_2 \in C$ with $d(c_1, c_2) = d$. If c_1 is sent and c_2 is received, then c_2 is accepted; the d errors go undetected. □

Correction

Strategy: IMLD/CMLD

e-error correcting code

A code C is an **e-error correcting code** if the decoder always makes the correct decision if e or fewer errors per codeword are introduced by the channel.

Example:

Consider $C = \{000, 111\}$.

C is a 1-error correcting code.

C is not a 2-error correcting code.

Theorem 1.4

A code C of distance d is an e-error correcting code, where $e = \lfloor \frac{d-1}{2} \rfloor$.

Proof:

Suppose that $c \in C$ is sent, at most $\frac{d-1}{2}$ errors are introduced, and r is received. Then $d(r, c) \leq \frac{d-1}{2}$.

On the other hand, if c_1 is any other codeword, then

$$\begin{aligned} d(r, c_1) &\geq d(c, c_1) - d(r, c) && \triangle \text{ ineq} \\ &\geq d - \frac{d-1}{2} && \text{since } d(C) = d \\ &= \frac{d+1}{2} \\ &> \frac{d-1}{2} \geq d(r, c) \end{aligned}$$

Hence c is the unique codeword at minimum distance from r, so the decoder correctly concludes that c was sent. □

Exercise:

Suppose $d(C) = d$, and let $e = \lfloor \frac{d-1}{2} \rfloor$. Show that C is *not* an $(e+1)$-error correcting code.

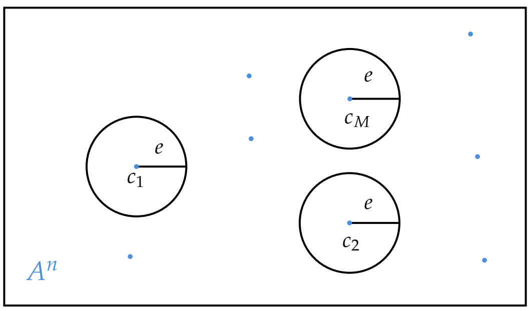
A natural question to ask is: given A, n, M, d, does there exist an $[n, M]$-code C over A of distance $\geq d$. This can be phrased as an equivalent sphere packing problem:

Sphere packing

Can we place M spheres of radius $e = \lfloor \frac{d-1}{2} \rfloor$ in A^n so that no two spheres overlap?

$C = \{c_1, \ldots, c_M\}$, $e = \lfloor \frac{d-1}{2} \rfloor$, S_c = sphere of radius e centered at c = all words within distance e of c.

We proved: if $c_1, c_2 \in C, c_1 \neq c_2$, then $S_{c_1} \cap S_{c_2} = \varnothing$.



Let $n = 128, q = 2, M = 2^{64}$. Does there exists a binary $[n, M]$-code with $d \geq 22$? If so, can encoding and decoding be done efficiently?

We'll view $\{0,1\}^{128}$ as a vector space of dimension 128 over $\mathbb{Z}_2$. We'll choose C to be a 64-dimensional subspace of this vector space. We will construct such a code at the end of the course. The main tools used will be linear algebra (over finite fields) and abstract algebra (rings and fields).

2

Introduction to Finite Fields

2.1 Definitions

ring

A **(commutative) ring** $(R, +, \cdot)$ consists of a set R and two operations $+ : R \times R \to R$ and $\cdot : R \times R \to R$, such that

1. $a + (b + c) = (a + b) + c \quad \forall a, b, c \in R.$
2. $a + b = b + a, \quad \forall a, b \in R.$
3. $\exists 0 \in R$ such that $a + 0 = a$, $\forall a \in R$.
4. $\forall a \in R$, $\exists - a \in R$ such that $a + (-a) = 0$.
5. $a \cdot (b \cdot c) = (a \cdot b) \cdot c, \quad \forall a, b, c \in R.$
6. $a \cdot b = b \cdot a, \qquad \forall a, b \in R.$
7. $\exists 1 \in R, 1 \neq 0$, such that $a \cdot 1 = a, \quad \forall a \in R.$
8. $a \cdot (b + c) = a \cdot b + b \cdot c, \qquad \forall a, b, c \in R.$

Notation We will denote $(R, +, \cdot)$ by R.

Example:
$\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}$ are commutative rings.

field

A **field** $(F, +, \cdot)$ is a commutative ring with the additional property:

9. $\forall a \in F, a \neq 0, \exists a^{-1} \in F$ such that $a \cdot a^{-1} = 1$.

Example:
$\mathbb{Q}, \mathbb{R}, \mathbb{C}$ are fields. $\mathbb{Z}$ is *not* a field.

infinite/finite field

A field $(F, +, \cdot)$ is a **finite field** if F is a finite set; otherwise it is an **infinite field**. If F is a finite field , its **order** is $|F|$.

Example:

$\mathbb{Q}, \mathbb{R}, \mathbb{C}$ are infinite fields.

For which integers $n \geq 2$ does there *exist* a finite field of order n? How does one *construct* such a field, i.e., what are the field elements, and how are the field operations performed?

The Integers Modulo n

Let $n \geq 2$. Recall that $\mathbb{Z}_n$ consists of the set of equivalence classes of integers modulo n, $\mathbb{Z}_n = \{[0], [1], [2], \ldots, [n-1]\}$, with addition and multiplication: $[a] + [b] = [a+b]$, $[a] \cdot [b] = [a \cdot b]$.

More simply, we write $\mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}$, and perform addition and multiplication modulo n.

Example:

$\mathbb{Z}_9 = \{0, 1, 2, \ldots, 8\}$. In $\mathbb{Z}_9$, $3 + 7 = 1$ and $3 \cdot 7 = 3$.

More precisely, $3 + 7 \equiv 1 \pmod 9$ and $3 \cdot 7 \equiv 3 \pmod 9$.

$\mathbb{Z}_n$ is a commutative ring (i.e., axioms 1-8 in the definition are satisfied).

When is $\mathbb{Z}_n$ is a field?

Theorem 2.1

$\mathbb{Z}_n$ is a field if and only if n is prime.

Proof:

$\Leftarrow$ Suppose n is prime. Let $a \in \mathbb{Z}_n$, $a \neq 0$ (so $1 \leq a \leq n-1$). Since n is prime, $\gcd(a, n) = 1$. Hence $\exists s, t \in \mathbb{Z}$ such that $as + nt = 1$. Reducing both sides modulo n gives $as \equiv 1 \pmod n$. Hence $a^{-1} = s$. Thus $\mathbb{Z}_n$ is a field.

$\Rightarrow$ Suppose n is composite, say $n = ab$ where $2 \leq a, b \leq n-1$.

Now, if a^{-1} exists, say $ac \equiv 1 \pmod n$, then $abc \equiv b \pmod n$, so $nc \equiv b \pmod n$. Thus $b \equiv 0 \pmod n$, so $n \mid b$ which is absurd since $2 \leq b \leq n-1$. Thus $\mathbb{Z}_n$ is not a field.

$\square$

We have established the existence of finite fields of order n, for each prime n. What about finite fields of order n, where n is composite? In particular, is there a field of order 4? Order 6?

characteristic

Let F be a field. The **characteristic** of F, denoted $\text{char}(F)$, is the smallest positive integer m such that $\underbrace{1 + \cdots + 1}_{m} = 0$. If no such m exists, then $\text{char}(F) = 0$.

Example:

$\mathbb{Q}, \mathbb{R}, \mathbb{C}$ have characteristic 0. $\mathbb{Z}_p$ (p prime) has characteristic p.

Theorem 2.2

If $\mathrm{char}(F) = 0$, then F is an infinite field.

Proof:
The elements $1, 1+1, 1+1+1, \ldots$ are distinct, because if $\underbrace{1+\cdots+1}_{a} = \underbrace{1+\cdots+1}_{b}$ where $a < b$, then $(\underbrace{1+\cdots+1}_{b}) - (\underbrace{1+\cdots+1}_{a}) = 1+\cdots+1_{b-a} = 0$, contradicting $\mathrm{char}(F) = 0$. $\square$

Theorem 2.3

Let F be a field with $\mathrm{char}(F) = m \neq 0$. Then m is prime.

Proof:
Suppose m is composite, say $m = ab$ where $2 \leq a, b \leq m-1$. Let $s = \underbrace{1+\cdots+1}_{a}$ and $t = \underbrace{1+\cdots+1}_{b}$; note that $s, t \neq 0$. Then $s \cdot t = (\underbrace{1+\cdots+1}_{a}) \cdot (\underbrace{1+\cdots+1}_{b}) = \underbrace{1+\cdots+1}_{ab=m} = 0$. Thus

$$s \cdot t \cdot t^{-1} = s \cdot 1 = s = 0,$$

a contradiction. We then conclude that m is prime. $\square$

Let F be a finite field of characteristic p. Consider the subset of elements of F:

$$E = \{0, 1, 1+1, 1+1, \ldots, \underbrace{1+\cdots+1}_{p-1}\}.$$

The elements of E are distinct. One can verify that E is a field, using the same operations as F. E is a **subfield** of F. If we identify the elements of E with the elements of $\mathbb{Z}_p$ in the natural way, then E is essentially the same field as $\mathbb{Z}_p$. We have proven:

Theorem 2.4

Let F be a finite field of char p. Then $\mathbb{Z}_p$ is a subfield of F.

Finite fields as vector spaces

Let F be a finite field of characteristic p. Identify:

$$\begin{array}{rcl} \text{vectors} & \leftrightarrow & \text{elements of } F \\ \text{scalars} & \leftrightarrow & \text{elements of } \mathbb{Z}_p \\ \text{vector addition} & \leftrightarrow & \text{addition of } F \\ \text{scalar multiplication} & \leftrightarrow & \text{multiplication of } F \end{array}$$

Then F is a vector space over $\mathbb{Z}_p$ (i.e., the axioms of what it means to be a vector space are satisfied).

2.2 Finite fields: Non-existence

Theorem 2.5

Let F be a finite field of characteristic p. Then the order of F is p^n, for some positive integer n.

Proof:

Let the dimension of F as a vector space over $\mathbb{Z}_p$ be n. Let $\alpha_1, \ldots, \alpha_n$ be a basis for F over $\mathbb{Z}_p$. Then each element $\beta \in F$ can be written uniquely in the form $\beta = c_1\alpha_1 + \cdots + c_n\alpha_n$, where $c_i \in \mathbb{Z}_p$. Thus $F = \left\{ \sum_{i=1}^{n} c_i\alpha_i : c_i \in \mathbb{Z}_p \right\}$, so $|F| = p^n$. $\square$

For example, there do not exist finite fields of order $6, 10, 12, 14, 15, \ldots$

Do finite fields of orders $4, 8, 9, 16, 25, 27, \ldots$ exist?

2.3 Existence of finite fields

Polynomial rings Let F be a field. $F[x]$ denotes the set of all polynomials in x with coefficients from F. Addition and multiplication of polynomials in $F[x]$ is done in the usual way, with coefficient arithmetic done in F.

Example:

In $\mathbb{Z}_5[x]$,

$$\begin{aligned}(3x^4 + 2x^3 + x + 4) + (x^5 + 2x^4 + x^2 + 2x + 3) &= x^5 + 2x^3 + x^2 + 3x + 2 \\ (3x^2 + 4x + 1) \cdot (2x^2 + x + 2) &= (x^4 + x^3 + 2x^2 + 4x + 2).\end{aligned}$$

Note that $F[x]$ is an infinite commutative ring.

Construction of finite fields: main idea

$$\begin{tikzcd} \mathbb{Z} \arrow[r, "\text{fix } n \geq 2", "a \equiv b \pmod{n}"'] & \mathbb{Z}_n \arrow[r, "n \text{ prime}"] & \mathbb{Z}_n \end{tikzcd}$$

infinite commutative ring | finite commutative ring | finite field of order n

$$\begin{tikzcd} \mathbb{Z}_p[x] \arrow[r, "{\text{fix } f \in \mathbb{Z}_p[x],\ \deg(f) = n \geq 1}", "g \equiv h \pmod{f}"'] & \mathbb{Z}_p[x]/(f) \arrow[r, "f \text{ irreducible}"] & \mathbb{Z}_p[x]/(f) \end{tikzcd}$$

infinite commutative ring | finite commutative ring | finite field of order p^n

Polynomial division

Let $f, g \in F[x]$, with $g \neq 0$. Then there exist unique polynomials $r, s \in F[x]$ such that $f = \underset{\substack{\uparrow \\ \text{quotient}}}{s}\, g + \underset{\substack{\uparrow \\ \text{remainder}}}{r}$, $\deg(r) < \deg(g)$. By convention, $\deg(0) = -\infty$.

Example:

Consider $f = 3x^4 + 2x^2 + x + 1, g = 2x^2 + 3x + 4 \in \mathbb{Z}_5[x]$.

$$\begin{array}{r|lllll} & 4x^2 & +3 & & & \\ \hline 2x^2+3x+4 & 3x^4 & +2x^3 & +2x^2 & +x & +1 \\ & 3x^4 & +2x^3 & +x^2 & & \\ \hline & & & x^2 & +x & +1 \\ & & & x^2 & +4x & +2 \\ \hline & & & & 2x & +4 \end{array}$$

So, $f = (4x^2 + 3)g + (2x + 4)$.

The ring $F[x]/(f)$

$g \equiv h \pmod f$

Let $f \in F[x]$ with $\deg(f) \geq 1$. Let $g, h \in F[x]$. Then g is congruent to h modulo f, written $g \equiv h \pmod f$, if $g - h = \ell f$ for some $\ell \in F[x]$ (equivalently, $f \mid (g - h)$, or g, h leave the same remainder upon division by f).

The relation $\equiv \pmod f$ is an equivalence relation, and partitions $F[x]$ into equivalence classes:

$$[g] = \{h \in F[x] : g \equiv g \pmod f\}.$$

Addition & multiplication: $[g] + [h] = [g + h], [g] \cdot [h] = [g \cdot h]$.

$F[x]/(f)$

The set of equivalence classes is denoted $F[x]/(f)$.

Theorem 2.6

$F[x]/(f)$ is a commutative ring.

Suppose now that $\deg(f) = n$. Let $g \in F[x]$. Then we can write $g = sf + r$, where $s, r \in F[x]$, and $\deg(r) < n$. Thus $g \equiv r \pmod f$, so $[g] = [r]$.

If $r_1, r_2 \in F[x], r_1 \neq r_2, \deg(r_1), \deg(r_2) < n$, then $f \nmid (r_1 - r_2)$, so $r_1 \not\equiv r_2 \pmod f$. Thus $[r_1] \neq [r_2]$.

Thus the polynomials in $F[x]$ of degree $< n$ are a complete set of representatives of the equivalence classes of $F[x]/(f)$.

Now, let $F = \mathbb{Z}_p$. Then $\mathbb{Z}_p[x]/(f) = \{[r] : r \in \mathbb{Z}_p[x], \deg(r) < n\}$. Thus $|\mathbb{Z}_p[x]/(f)| = p^n$, so $\mathbb{Z}_p[x]/(f)$ is a commutative ring of order p^n.

When is $F[x]/(f)$ a field?

irreducible over F

Let $f \in F[x]$, with $\deg(f) \geq 1$. Then **irreducible over** F if f cannot be written as $f = g \cdot h$, $g, h \in F[x]$, $\deg(g) \geq 1, \deg(h) \geq 1$.

Example:

$x^2 + 1$ is irreducible over $\mathbb{R}$, since it has no roots in $\mathbb{R}$.

$x^2 + 1$ is reducible over $\mathbb{C}$, since $x^2 + 1 = (x + i)(x - i)$.

$x^2 + 1$ is reducible over $\mathbb{Z}_2$, since $x^2 + 1 = (x + 1)(x + 1)$.

$x^2 + 1$ is irreducible over $\mathbb{Z}_3$, since it has no roots in $\mathbb{Z}_3$.

Theorem 2.7

$F[x]/(f)$ is a field if and only if f is irreducible over F.

Proof:
Analogous to the proof of the theorem: $\mathbb{Z}_n$ is a field if and only if n is prime. □

Now let's construct finite fields.

Theorem 2.8

Let $f \in \mathbb{Z}_p[x]$ be an irreducible polynomial of degree $n \geq 1$. Then $\mathbb{Z}_p[x]/(f)$ is a finite field of order p^n and characteristic p. The elements are the polynomials in $\mathbb{Z}_p[x]$ of degree $< n$.

Example: finite field of order $4 = 2^2$

Here $p = 2$ and $n = 2$. Let $f(x) = x^2 + x + 1 \in \mathbb{Z}_2[x]$. Then $f(0) = 1$, $f(1) = 1$, so f has no roots in $\mathbb{Z}_2$. Thus f is irreducible over $\mathbb{Z}_2$.

So, $F = \mathbb{Z}_2[x]/(x^2 + x + 1)$ is a finite field of order $2^2 = 4$. The elements are $\{0, 1, x, x + 1\}$ where $[\,]$ is omitted.

Example of addition: $x + (x + 1) = 1$

Example of multiplication: $x \cdot (x + 1) = x^2 + x = 1$

Example: finite field of order $2^3 = 8$

Here, $p = 2$ and $n = 3$. We need an irreducible polynomial. We need an irreducible polynomial of degree 3 over $\mathbb{Z}_2$.

Candidates: $x^3, x^3 + 1, x^3 + x, x^3 + x + 1, x^3 + x^2, x^3 + x^2 + 1, x^3 + x^2 + x, x^3 + x^2 + x + 1$

- Try $f(x) = x^3 + x + 1$.

  Since $f(0) = f(1) = 1$, f has no roots in $\mathbb{Z}_2$, and thus no linear factors in $\mathbb{Z}_2[x]$. Thus f is irreducible over $\mathbb{Z}_2$, and $F_1 = \mathbb{Z}_2[x]/(x^3 + x + 1)$ is a finite field of order $2^3 = 8$.

  The elements of F_1 are $\{0, 1, x, x + 1, x^2, x^2 + 1, x^2 + x, x^2 + x + 1\}$.

  Example of addition: $(x^2 + x) + (x^2 + x + 1) = 1$.

  Example of multiplication: $(x^2 + x) \cdot (x^2 + x + 1) = x^4 + x = x^2$.

  Example of inversion: $x^{-1} = x^2 + 1$, since $x \cdot (x^2 + 1) = 1$.

- $x^3 + x^2 + 1$ is irreducible over $\mathbb{Z}_2$, so $F_2 = \mathbb{Z}_2[x]/(x^3 + x^2 + 1)$ is a finite field of order 8. The elements of F_2 are $\{0, 1, x, x + 1, x^2, x^2 + 1, x^2 + x, x^2 + x + 1\}$.

Note that F_1 and F_2 are not the same field. For example, in F_1, $x \cdot x^2 = x + 1$, whereas in F_2, $x \cdot x^2 = x^2 + 1$. However, F_1 and F_2 are isomorphic (essentially the same). Formally, there is a bijection $\phi : F_1 \to F_2$ such that $\phi(a + b) = \phi(a) + \phi(b)$ and $\phi(a \cdot b) = \phi(a) \cdot \phi(b)$ $\forall a, b \in F_1$.

Existence and uniqueness of finite fields

Let p be prime and $n \geq 1$. Then there exists an irreducible polynomial of degree n over $\mathbb{Z}_p$.

Theorem 2.9

There exists a finite field of order q if and only if $q = p^n$ for some prime p and $n \geq 1$.

Actually, any two finite fields of the same order are isomorphic.

We will denote *the* finite field of order q by $\mathrm{GF}(q)$ "the Galois Field of order q".

In the previous example, we saw two ways of representing the finite field $\mathrm{GF}(2^3)$.

2.4 Properties of finite fields

Theorem 2.10: Frosh's dream

Let F be a finite field of characteristic p, and let $\alpha, \beta \in F$. Then $(\alpha+\beta)^{p^m} = \alpha^{p^m} + \beta^{p^m}$ $\forall m \geq 1$.

Proof ($m = 1$):
By the Binomial Theorem,

$$(\alpha+\beta)^p = \binom{p}{0}\alpha^p + \sum_{i=1}^{p-1}\binom{p}{i}\alpha^i\beta^{p-i} + \binom{p}{p}\beta^p.$$

Now for $1 \leq i \leq p-1$,

$$\binom{p}{i} = \frac{p(p-1)(p-2)\cdots(p-i+1)}{1\cdot 2\cdot 3\cdots i} \equiv 0 \pmod{p},$$

since p divides the numerator but not the denominator, and since $\binom{p}{i}$ is an integer. Thus

$$\binom{p}{i}\alpha^i\beta^{p-i} = \underbrace{\alpha^i\beta^{p-i} + \cdots + \alpha^i\beta^{p-i}}_{\binom{p}{i}} = (1+\cdots+1)\alpha^i\beta^{p-i} = 0.$$

Hence $(\alpha+\beta)^p = \alpha^p + \beta^p$. The statement for $m \geq 1$ can be proven by induction. □

The multiplicative group $\mathrm{GF}(q)^*$

multiplicative group of $\mathrm{GF}(q)$

The **multiplicative group of** $\mathrm{GF}(q)$ is $\mathrm{GF}(q)^* = \mathrm{GF}(q) \setminus \{0\}$.

Theorem 2.11

Let $\alpha \in \mathrm{GF}(q)^*$. Then $\alpha^{q-1} = 1$.

Note that if $\mathrm{GF}(q) = \mathbb{Z}_p$, this is Fermat's Little Theorem.

Proof:
Let the (distinct) elements of $\mathrm{GF}(q)^*$ be $\alpha_1, \alpha_2, \ldots, \alpha_{q-1}$. Consider the (nonzero) elements $\alpha\alpha_1, \alpha\alpha_2, \ldots, \alpha\alpha_{q-1}$. These elements are distinct because if $\alpha\alpha_i = \alpha\alpha_j$ for some $i \neq j$, then $\alpha^{-1}(\alpha\alpha_i) = \alpha^{-1}(\alpha\alpha_j)$, so $\alpha_i = \alpha_j$, a contradiction. Hence $\{\alpha\alpha_1, \alpha\alpha_2, \ldots, \alpha\alpha_{q-1}\} = \{\alpha_1, \alpha_2, \ldots, \alpha_{q-1}\}$, so

$$(\alpha\alpha_1)(\alpha\alpha_2)\cdots(\alpha\alpha_{q-1}) = \alpha_1\alpha_2\cdots\alpha_{q-1}.$$

Cancelling gives $\alpha^{q-1} = 1$. □

Corollary 2.12

Let $\alpha \in \mathrm{GF}(q)$. Then $\alpha^q = \alpha$.

Order of finite elements

order of α

Let $\alpha \in \mathrm{GF}(q)^*$. The **order of** α, denoted $\mathrm{ord}(\alpha)$, is the smallest positive integer t such that $\alpha^t = 1$.

Theorem 2.13

Let $\alpha \in \mathrm{GF}(q)^*$, $\mathrm{ord}(\alpha) = t$. Then $\alpha^s = 1$ if and only if $t \mid s$.

Proof:
Let $s \in \mathbb{Z}$. Then long division of s by t yields

$$s = \ell t + r, \quad \text{where } 0 \leq r < t.$$

Now, $\alpha^s = \alpha^{\ell t + r} = (\alpha^t)^\ell \cdot \alpha^r = \alpha^r$. Hence $\alpha^s = 1 \iff \alpha^r = 1 \iff r = 0 \iff t \mid s$. □

Corollary 2.14

Let $\alpha \in \mathrm{GF}(q)^*$. Then $\mathrm{ord}(\alpha) \mid (q-1)$.

Example:
There is only one element in $\mathrm{GF}(q)$ of order 1, namely the element 1.

Example:
Consider $\mathrm{GF}(2^3) = \mathbb{Z}_2[x]/(x^3 + x + 1)$. The order of $\alpha = x^2 + 1$ is 7.

Example:
Consider $\mathrm{GF}(2^4) = \mathbb{Z}_2[x]/(x^4 + x + 1)$.

$f(x) = x^4 + x + 1$ has no roots in $\mathbb{Z}_2$, thus no linear factors. Also, $f(x)$ has no irreducible quadratic factors, since $(x^2 + x + 1) \nmid f(x)$. Note here $x^2, x^2 + 1, x^2 + x$ are reducible quadratic polynomials. Thus f is irreducible over $\mathbb{Z}_2$.

Find $\mathrm{ord}(x)$ in $\mathrm{GF}(2^4)$.

Solution: We have $x^1 = x, x^2 = x^2, x^3 = x^3, x^4 = x + 1, x^5 = x^2 + x \neq 1$. Thus $\mathrm{ord}(x) \neq 1, 3, 5$. Since $\mathrm{ord}(x) \mid 15$, we must have $\mathrm{ord}(x) = 15$.

Let $\alpha \in \mathrm{GF}(q)^*$ with $\mathrm{ord}(\alpha) = t$. Then the elements $\alpha^0, \alpha^1, \alpha^2, \ldots, \alpha^{t-1}$ are distinct. In particular, if

$\mathrm{ord}(\alpha) = q-1$, then $\mathrm{GF}(q)^* = \{\alpha^0, \alpha^1, \alpha^2, \dots, \alpha^{q-2}\}$.

generator

A **generator** of $\mathrm{GF}(q)^*$ is an element of order $q-1$.

Example:

$\alpha = x$ is a generator of $\mathrm{GF}(2^4) = \mathbb{Z}_2[x]/(x^4+x+1)$ since $\mathrm{ord}(x) = 15$. Let's verify the above fact:

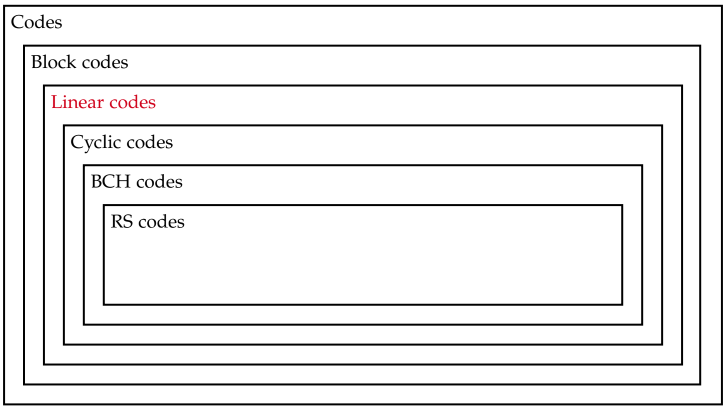
$$
\begin{array}{llll}
x^0 = 1, & x^1 = x, & x^2 = x^2, & x^3 = x^3, \\
x^4 = x+1, & x^5 + x^2 + x, & x^6 = x^3 + x^2, & x^7 = x^3 + x + 1, \\
x^8 = x^2 + 1, & x^9 = x^3 + x, & x^{10} = x^2 + x + 1, & x^{11} = x^3 + x^2 + x, \\
x^{12} = x^3 + x^2 + x + 1, & x^{13} = x^3 + x^2 + x + 1, & x^{14} = x^3 + 1, & x^{15} = 1.
\end{array}
$$

Theorem 2.15

Every finite field $\mathrm{GF}(q)$ has a generator.

3

Linear codes



3.1 Definition

Let $F = \mathrm{GF}(q)$. Let $V_n(F) = \underbrace{F \times \cdots \times F}_{n}$. $V_n(F)$ is an n-dimensional space over F. $|V_n(F)| = q^n$.

linear (n,k)-code over F

A **linear (n,k)-code over F** is a k-dimensional subspace of $V_n(F)$.

Recall a *subspace* S of a vector space V over F is non-empty subset $S \subseteq V$ such that:

$$\text{(i) } a, b \in S \implies a + b \in S, \text{ (ii) } a \in S, \lambda \in F \implies \lambda a \in S.$$

If S is a subspace of V, then S is itself a vector space over F; also $0 \in S$. A *basis* of S is a linearly independent, spanning subset of S. All bases of S have the same cardinality, called the *dimension* of S.

3.2 Properties of Linear Codes

Let C be an (n,k)-code over F, and let $v_1, v_2, \ldots, v_k$ be an ordered basis for C.

1. Number of codewords

The elements of C are precisely

$$c_1v_1 + c_2v_2 + \cdots + c_kv_k, \quad c_i \in F.$$

Thus, $|C| = M = q^k$.

2. Rate

The rate of C is $R = \frac{\log_q M}{n} = \frac{\log_q q^k}{n} = \frac{k}{n}$.

3. Weight

Hamming weight

The **Hamming weight** $w(v)$ of a vector $v \in V_n(F)$ is the number of nonzero coordinates in v. The **Hamming weight** of a linear code C is $w(C) = \min\{w(c) : c \in C, c \neq 0\}$.

Theorem 3.1

If C is a linear code, then $w(c) = d(C)$.

Proof:
We have

$$\begin{aligned} d(C) &= \min\{d(x,y) : x,y \in C, x \neq y\} \\ &= \min\{w(x-y) : x,y \in C, x \neq y\} && \text{since } d(x,y) = w(x-y) \\ &= \min\{w(c) : c \in C, c \neq 0\} && \text{since } C \text{ is linear }, x-y \in C \\ &= w(C). \end{aligned}$$

4. Encoding

Since there are q^k codewords, there are also q^k source messages. We shall assume that source messages are the elements of F^k. Then a convenient and natural bijection (i.e., *encoding rule*) between F^k and C is defined by:

$$\boxed{m = (m_1, m_2, \ldots, m_k) \mapsto c = m_1v_1 + m_2v_2 + \cdots + m_kv_k.}$$

Note that different ordered bases for C yield different encoding rules.

5. Generator matrix

A convenient way to represent C.

generator matrix

A **generator matrix** G for an (n,k)-code C is a $k \times n$ matrix whose rows form a basis for C:

$$G = \begin{bmatrix} v_1 \\ v_2 \\ \vdots \\ v_k \end{bmatrix}_{k \times n}.$$

Note that the encoding rule is $c = mG$.

Example: linear code

Consider the $(5,3)$-binary code:

$$C = \langle \underset{c_1}{10011}, \underset{c_2}{01001}, \underset{c_3}{00110} \rangle$$

and c_1, c_2, c_3 are linearly independent over $\mathrm{GF}(2)$.

A generator matrix for C is $G = \left[\begin{array}{ccc|cc} 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 \end{array}\right]_{3\times 5}$

The encoding rule (with respect to the ordered basis $\{c_1, c_2, c_3\}$) is $c = mG$.

$$\begin{array}{ccc@{\qquad}ccc} 000 & \to & 00000 & 100 & \to & 10011 \\ 001 & \to & 00110 & 101 & \to & 10101 \\ 010 & \to & 01001 & 110 & \to & 11010 \\ 011 & \to & 01111 & 111 & \to & 11100 \end{array}$$

Other properties: $M = |C| = 2^3 = 8$, $R = 3/5$, $d(C) = w(C) = 2$.

Standard form GM

standard form generator matrix

Let C be an (n,k)-code over F. A GM G for C of the form $G = [I_k | A]_{k\times n}$ is said to be in **standard form**.

systematic code

If C has a GM in standard form, then C is a **systematic code**.

Example: systematic/non-systematic code

$C = \langle 100011, 001001, 000110 \rangle$ is a *non-systematic* $(6,3)$-binary code.

But $C' = \langle 10011, 001001, 010010 \rangle$ is *systematic*. A GM for C' is

$$G = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 \end{bmatrix}$$

equivalent codes

Two codes C, C' over F are **equivalent** if C' can be obtained from C by choosing a permutation of the coordinate positions $\{1, 2, \ldots, n\}$, and then consistently rearranging every codeword of C according to this permutation.

Below are some facts of equivalent codes:

1. If C is linear, and C' is equivalent to C, then C' is linear.
2. Equivalent codes have the same length, dimension, distance.
3. Every linear code is equivalent to a systematic code.

3.3 The Dual Code

inner product

Let $x = (x_1, x_2, \ldots, x_n)$, $y = (y_1, y_2, \ldots, y_n) \in V_n(F)$. The **inner product** of x and y is

$$x \cdot y = \sum_{i=1}^{n} x_i y_i \in F$$

For all $x, y, z \in V_n(F)$ and $\lambda \in F$:

1. $x \cdot y = y \cdot x$.
2. $x \cdot (y + z) = x \cdot y + x \cdot z$.
3. $(\lambda x) \cdot y = \lambda(x \cdot y)$
4. $x \cdot x$ does *not* imply that $x = 0$.

Example:
Consider $x = 111100 \in V_6(\mathbb{Z}_2)$. Then $x \cdot x = 0$, but $x \neq 0$. More generally, if $x \in V_n(\mathbb{Z}_2)$, then $x \cdot x = 0$ if and only if $w(x)$ is even.

orthogonal vectors

Two vectors x, y are **orthogonal** if $x \cdot y = 0$.

dual code

Let C be an (n, k)-code over F. The **dual code** or **orthogonal code** of C is

$$C^\perp = \{x \in V_n(F) : x \cdot y = 0, \quad \forall y \in C\}.$$

Theorem 3.2

If C is an (n, k)-code over F, then $C^\perp$ is an $(n, n-k)$-code over F.

Proof:
Let G be a GM for C, and let the rows of G be $v_1, v_2, \ldots, v_k$.

Claim Let $x \in V_n(F)$. Then $x \in C^\perp$ if and only if $v_1 \cdot x = v_2 \cdot x = \cdots = v_k \cdot x = 0$.

Let's prove the claim.

($\Rightarrow$) is clear since $v_1, v_2, \ldots, v_k \in C$.

($\Leftarrow$) Suppose $v \in C$. Then we can write $v = \lambda_1 v_1 + \cdots + \lambda_k v_k$, where $\lambda_i \in F$. Then

$$v \cdots x = (\lambda_1 v_1 + \cdots + \lambda_k v_k) \cdot x = \lambda_1(v_1 \cdot x) + \cdots + \lambda_k(v_k \cdot x) = 0.$$

Thus, $C^\perp = \{x \in V_n(F) : Gx^T = 0\}$ = null space of G. Since G has rank k, $C^\perp$ is a subspace of $V_n(F)$ of dimension $n - k$. □

3.4 Parity-Check Matrix

Let G be a GM for a linear code C. Then $C^\perp$ = null space of G.

Theorem 3.3

If C is a linear code, then $(C^\perp)^\perp = C$.

Proof:
Let C be an (n, k)-code. Then $C^\perp$ is an $(n, n-k)$-code.

Furthermore, $(C^\perp)^\perp$ is an (n, k)-code, and $C \subseteq (C^\perp)^\perp$.

Since $\dim(C) = \dim\big((C^\perp)^\perp\big)$, it follows that $C = (C^\perp)^\perp$. □

parity-check matrix

If C is a linear code, then a generator matrix H for $C^\perp$ is called a **parity-check matrix** (PCM) for C.

Note:
H is an $(n-k) \times n$ matrix.

C has many PCMs.

Constructing a GM for $C^\perp$

Theorem 3.4

Let C be an (n, k)-code with GM $G = [I_k | A]$. Then $H = [-A^T | I_{n-k}]$ is a GM for $C^\perp$.

Note that A is $k \times (n-k)$ matrix.

Proof:
Since $\operatorname{rank}(H) = n - k$, H is a GM for an $(n, n-k)$-code $\overline{C}$. Also,

$$GH^T = [I_k | A] \left[\begin{array}{c} -A \\ \hline I_{n-k} \end{array}\right] = -A + A = 0.$$

Thus $\overline{C} \subseteq C^\perp$. Since $\dim(\overline{C}) = \dim(C^\perp)$, we have $\overline{C} = C^\perp$. Hence H is a GM for $C^\perp$. □

Example:

Consider the $(5, 2)$-code C over $\mathbb{Z}_3$ with GM $G = \begin{bmatrix} 2 & 0 & 2 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 \end{bmatrix}$. Find a PCM for C.

Solution Find a GM for C in standard form:

$$G \xrightarrow{R_1 \leftarrow 2R_1} \begin{bmatrix} 1 & 0 & 1 & 2 & 0 \\ 1 & 1 & 0 & 0 & 1 \end{bmatrix} \xrightarrow{R_2 \leftarrow R_2 - R_1} \left[\begin{array}{cc|ccc} 1 & 0 & 1 & 2 & 0 \\ 0 & 1 & 2 & 1 & 1 \end{array}\right].$$

So,

$$H = \left[\begin{array}{cc|ccc} 2 & 1 & 1 & 0 & 0 \\ 1 & 2 & 0 & 1 & 0 \\ 0 & 2 & 0 & 0 & 1 \end{array}\right]$$

is a PCM for C.

We have

$$C = \left\{ \begin{array}{lll} 00000, & 20210, & 10120, \\ 11001, & 22002, & 01211, \\ 02122, & 21121, & 12212 \end{array} \right\}$$

Thus $d(C) = w(C) = 3, R = 2/5$.

Notes on PCMs

Let C be an (n,k)-code over F with GM G.

1. An $(n-k) \times n$ matrix H over F is a PCM for C iff $GH^T = 0$ and $\operatorname{rank}(H) = n - k$.
2. G is a PCM for $C^\perp$ (since $(C^\perp)^\perp = C$).
3. $C = \operatorname{null}(H)$.
4. Let H be a PCM for C, and let $x \in V_n(F)$, then $x \in C$ iff $Hx^T = 0$.

V3c skipped for now. V3f

3.5 Syndrome Decoding

Let C be an (n,k)-code over $F = \mathrm{GF}(q)$ with PCM H.

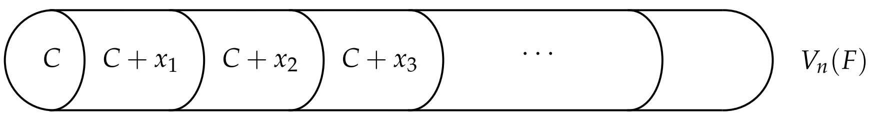
$x \equiv y \pmod{C}$

Let $x, y \in V_n(F)$. We write $x \equiv y \pmod{C}$ if $x - y \in C$.

Facts:

1. $\equiv \pmod{C}$ is an *equivalence relation*.
2. The set of equivalences classes partitions $V_n(F)$.
3. The equivalence class containing $x \in V_n(F)$ is called a **coset** of C. THis class is

$$C + x = \{y \in V_n(F) : y \equiv \pmod{C}\} = \{c + x : c \in C\}.$$



Example: Cosets

Consider a $(5,2)$-binary code C with GM

$$G = \begin{bmatrix} 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 0 \end{bmatrix}.$$

Find all cosets of C.

Solution The cosets of C are:

$$\begin{aligned} C = C + 00000 &= \{00000, 10111, 01110, 11001\} = C + 10111 = C + 01110 + C + 11001 \\ C + 10000 &= \{10000, 00111, 11110, 01001\} = C + 00111 = C + 11110 = C + 01001 \\ C + 01000 &= \{01000, 11111, 00110, 10001\} \\ C + 00100 &= \{00100, 10011, 01010, 11101\} \\ C + 00010 &= \{00010, 10101, 01100, 11011\} \\ C + 00001 &= \{00001, 10110, 01111, 11000\} \\ C + 10100 &= \{10100, 00011, 11010, 01101\} \\ C + 10010 &= \{10010, 00101, 11100, 01011\} \end{aligned}$$

Facts on cosets:

4

Golay codes

5

Cyclic codes

cyclic space

A subspace S of $V_n(F)$ is **cyclic** if $(a_0, a_1, \ldots, a_{n-1}) \in S \implies (a_{n-1}, a_0, a_1, \ldots, a_{n-2}) \in S$.

cyclic code

A **cyclic code** is a cyclic subspace of $V_n(F)$.

5.1 The Polynomial Ring $R = F[x]/(x^n - 1)$

Let $R = F[x]/(x^n - 1)$, where $F = \mathrm{GF}(q)$. Then R is a commutative ring (but not a field, since $x^n - 1$ is reducible over F).

We have the following bijection between $V_n(F)$ and R:

$$a = (a_0, a_1, a_2, \ldots, a_{n-1}) \longleftrightarrow a(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_{n-1} x^{n-1}.$$

Vector addition and scalar multiplication preserved.

$a \cdot b$

Let $a, b \in V_n(F)$. Then $a \cdot b = c \in V_n(F)$, where $c \leftrightarrow c(x) = a(x) \cdot b(x) \bmod (x^n - 1)$.

ideal

Let R be a (finite) commutative ring. A non-empty subset I of R is an **ideal** of R if

(i) $a, b \in I \implies a + b \in I$;

(ii) $a \in I, b \in R \implies a \cdot b \in I$.

Theorem 5.1: algebraic characterization of cyclic subspaces of $V_n(F)$

Let S be a non-empty subset of $V_n(F)$. Let I be the associated polynomials in $R = F[x]/(x^n - 1)$. Then S is a cyclic subspace of $V_n(F)$ if and only if I is an ideal of R.

5.2 Ideals of $R = F[x]/(x^n - 1)$

ideal generated by g

Let R be a (commutative) ring, and let $g \in R$. Let $\langle g \rangle = \{g \cdot r : r \in R\}$. Then $\langle g \rangle$ is an ideal of R, called the **ideal generated by** g.

principal ideal

An ideal I of R is said to be **principal** if $I = \langle g \rangle$ for some $g \in I$.

principal ideal ring

A ring R is a **principal ideal ring** if every ideal of R is principal.

Theorem 5.2

$R = F[x]/(x^n - 1)$ is a principal ideal ring.

generator polynomial

Let I be an ideal of $R = F[x]/(x^n - 1)$.

- If $I = \{0\}$, then $x^n - 1$ is the **generator polynomial** of I.
- If $I \neq \{0\}$, then *the* monic polynomial of smallest degree in I is called the **generator polynomial** of I.

Theorem 5.3

Let I be a nonzero ideal of $R = F[x]/(x^n - 1)$.

1) There is a unique monic polynomial $g(x)$ of smallest degree in I; $I = \langle g \rangle$.
2) $g(x) \mid (x^n - 1)$ in $F[x]$.

Theorem 5.4

Let $h(x)$ be a monic divisor of $x^n - 1$ in $F[x]$. Then $h(x)$ is *the* generator polynomial of $\langle h(x) \rangle$.

Corollary 5.5

There is a 1-1 correspondence between ideals of R and monic divisors of $x^n - 1$, and thus also a 1-1 correspondence between cyclic subspaces of $V_n(F)$ and monic divisors of $x^n - 1$.

5.3 Dimension of a Cyclic Code

Theorem 5.6

Let $g(x)$ be a monic divisor of $x^n - 1$ over F, where $F = \mathrm{GF}(q)$. Suppose $\deg(g) = n - k$. Then the cyclic subspace S of $V_n(F)$ generated by $g(x)$ has dimension k.

5.4 GM of a Cyclic Code

Theorem 5.7

Let $g(x)$ be the generator polynomial of an (n,k)-cyclic code C over F (so $g(x)$ is a monic divisor of $x^n - 1$ over F of degree $n - k$). Then a (non-standard) GM for C is

$$G = \begin{bmatrix} g(x) \\ xg(x) \\ x^2 g(x) \\ \vdots \\ x^{k-1} g(x) \end{bmatrix}_{k \times n} .$$

Encoding Source messages are the polynomials in $F[x]$ of degree $< k$. If $m(x) = m_0 + m_1 x + \cdots + m_{k-1} x^{k-1}$, then encoding of m with respect to G is

$$c = \begin{bmatrix} m_0 & m_1 & \cdots & m_{k-1} \end{bmatrix} G = m_0 g(x) + m_1 x g(x) + \cdots + m_{k-1} x^{k-1} g(x),$$

so $c(x) = m(x)g(x)$. Note that no reduction by $x^n - 1$ is needed.

5.5 The Dual Code of a Cyclic Code

Let C be an (n,k)-cyclic code over F with generator polynomial $g(x)$. Let

$$g(x) = \underset{\substack{\uparrow \\ \neq 0}}{g_0} + g_1 x + \cdots + \underset{\substack{\uparrow \\ = 1}}{g_{n-k}} x^{n-k} + \underbrace{g_{n-k+1} x^{n-k+1} + \cdots + g_{n-1} x^{n-1}}_{0} .$$

parity-check polynomial

The **parity-check polynomial** is $h(x) = (x^n - 1)/g(x)$.

Let

$$h(x) = \underset{\substack{\uparrow \\ \neq 0}}{h_0} + h_1 x + \cdots + \underset{\substack{\uparrow \\ = 1}}{h_k} x^k + \underbrace{h_{k+1} x^{k+1} + \cdots + h_{n-1} x^{n-1}}_{0}$$

Also define $h_j = h_{j \bmod n}$ for all $j \in \mathbb{Z}$.

Observe that $g = (g_0, \ldots, g_{n-1})$ is orthogonal to the vector $\overline{h} = (h_{n-1}, \ldots, h_0)$ and all its cyclic shifts.

6

BCH codes

6.1 Subfields and Extension fields

For any prime power q, $\mathrm{GF}(q)$ is a subfield of $\mathrm{GF}(q^m)$ and we can view $\mathrm{GF}(q^m)$ as an m-dimensional vector space over $\mathrm{GF}(q)$.

Example:

$\mathrm{GF}(2^{16})$ is a 16-dimensional vector space over $\mathrm{GF}(2)$.
$\mathrm{GF}(2^{16})$ is a 8-dimensional vector space over $\mathrm{GF}(2^2)$.
$\mathrm{GF}(2^{16})$ is a 4-dimensional vector space over $\mathrm{GF}(2^4)$.
$\mathrm{GF}(2^{16})$ is a 2-dimensional vector space over $\mathrm{GF}(2^8)$.
$\mathrm{GF}(2^{16})$ is a 1-dimensional vector space over $\mathrm{GF}(2^{16})$.

6.2 Minimal Polynomials

We call $\mathrm{GF}(q^m)$ the **extension field**, and $\mathrm{GF}(q)$ the subfield.

minimal polynomial of α over $\mathrm{GF}(q)$

Let $\alpha \in \mathrm{GF}(q^m)$. The **minimal polynomial of α over** $\mathrm{GF}(q)$, denoted $m_\alpha(y)$ is the monic polynomial of smallest degree in $\mathrm{GF}(q)[y]$ that α has a root.

Theorem 6.1

Let $\alpha \in \mathrm{GF}(q^m)$.

1. The minimal polynomial $m_\alpha(y)$ of α over $\mathrm{GF}(q)$ is unique.
2. $m_\alpha(y)$ is irreducible over $\mathrm{GF}(q)$.
3. $\deg(m_\alpha) \leq m$.
4. If $f \in \mathrm{GF}(q)[y]$, then $f(\alpha) = 0 \iff m_\alpha(y) \mid f(y)$.

6.3 Computing Minimal Polynomials

Theorem 6.2

Let $\alpha \in \mathrm{GF}(q^m)$. Then $\alpha \in \mathrm{GF}(q)$ if and only if $\alpha^q = \alpha$.

set of conjugates of α w.r.t. GF(q)

Let $\alpha \in \mathrm{GF}(q^m)$. Let t be the smallest positive integer such that $\alpha^{q^t} = \alpha$ (note: $t \leq m$). Then the **set of conjugates of α w.r.t.** GF(q) is $C(\alpha) = \{\alpha, \alpha^q, \alpha^{q^2}, \ldots, \alpha^{q^{t-1}}\}$.

The t elements in $C(\alpha)$ are distinct.

Theorem 6.3

Let $\alpha \in \mathrm{GF}(q^m)$. Then the minimal polynomial of α over GF(q) is

$$m(y) = \prod_{\beta \in C(\alpha)} (y - \beta)\,.$$

6.4 Factoring $x^n - 1$ over GF(q)

Preliminaries Let p be the characteristic of GF(q). If $\gcd(n, q) \neq 1$, then write $n = \overline{n} p^\ell$, where $\ell \geq 1$ and $\gcd(\overline{n}, p) = 1$. Then $x^n - 1 = (x^{\overline{n}} - 1)^{p^\ell}$. So, WLOG, we shall assume that $\gcd(n, q) = 1$.

Let m be the smallest integer such that $q^m \equiv 1 \pmod{n}$, i.e., $n \mid (q^m - 1)$. Note that such an m exists.

Let α be a generator of $\mathrm{GF}(q^m)^*$. Let $\beta = \alpha^{(q^m-1)/n}$; note that $\beta \in \mathrm{GF}(q^m)$.

Also note, $\mathrm{ord}(\beta) = n$, and $1, \beta, \beta^2, \ldots, \beta^{n-1}$ are distinct. Furthermore, $(\beta^i)^n = (\beta^n)^i = 1$ for each $i \in [0, n-1]$. Hence $1, \beta, \beta^2, \ldots, \beta^{n-1}$ are roots of $x^n - 1$; and there aren't any other roots. So,

$$x^n - 1 = (x-1)(x-\beta)(x-\beta^2)\cdots(x-\beta^{n-1})$$

is the complete factorization of $x^n - 1$ over GF(q^m).

However, we seek the factorization of $x^n - 1$ over GF(q).

Consider β^i, where $0 \leq i \leq n-1$. Since β^i is a root of $x^n - 1$, we have $m_{\beta^i}(x) \mid (x^n - 1)$. Also, the roots of $m_{\beta^i}(x)$ are $C(\beta^i) = \{\beta^i, \beta^{iq}, \beta^{iq^2}, \ldots, \beta^{iq^{t-1}}\}$, where t is the smallest positive integer such that $iq^t \equiv i \pmod{n}$.

cyclotomic coset of q (mod n) containing i

Suppose $\gcd(n, q) = 1$, and let $0 \leq i \leq n-1$. The **cyclotomic coset of** q (mod n) **containing** i is

$$C_i = \{i, \quad iq \bmod n, \quad iq^2 \bmod n, \quad \ldots, \quad iq^{t-1} \bmod n\},$$

where t is the smallest positive integer such that $iq^t \equiv i \pmod{n}$. Also $C = \{C_i : 0 \leq i \leq n-1\}$ is the **set of cyclotomic cosets of** q mod n.

Theorem 6.4

Suppose $\gcd(n, q) = 1$.

- The number of monic irreducible factors of $x^n - 1$ over $\mathrm{GF}(q)$ is equal to the number of (distinct) cyclotomic cosets of q mod n.
- The number of monic irreducible factors of degree d is equal to the number of (distinct) cyclotomic cosets of q mod n of size d.

Theorem 6.5

Suppose $\gcd(n, q) = 1$. Let m be the smallest positive integer such that $q^m \pmod n$, and let $\beta \in \mathrm{GF}(q^m)$ be an element of order n. Then the monic irreducible factor of $x^n - 1$ over $\mathrm{GF}(q)$ are $\{m_{\beta^i}(x) : 0 \le i \le n-1\}$, where

$$m_{\beta^i}(x) = \prod_{j \in C_i} (x - \beta^j) .$$

If $j \in C_i$, then $m_{\beta^j}(x) = m_{\beta^i}(x)$.

6.5 BCH Codes: Definition

BCH codes are cyclic codes that are constructed in such a way that a (useful) lower bound on their distance is known.

BCH code

A **BCH code** C over $\mathrm{GF}(q)$ of block length n and **designed distance** δ is a cyclic code generated by $g(x) = \mathrm{lcm}\,\{m_{\beta^i}(x) : a \le i \le a + \delta - 2\}$, for some integer a.

6.6 BCH Bound

Vanderdmonde matrix

A **Vanderdmonde matrix** over a field F is a matrix of the form

$$A(x_1, x_2, \ldots, x_t) = \begin{bmatrix} 1 & 1 & \cdots & 1 \\ x_1 & x_2 & \cdots & x_t \\ x_1^2 & x_2^2 & \cdots & x_t^2 \\ \vdots & \vdots & \vdots & \\ x_1^{t-1} & x_2^{t-1} & \cdots & x_t^{t-1} \end{bmatrix}_{t \times t} ,$$

where $x_1, x_2, \ldots, x_t \in F$.

Theorem 6.6

$\det(A(x_1, \ldots, x_t)) \neq 0$ if and only if $x_1, \ldots, x_t$ are distinct.

Corollary 6.7

A Vanderdmonde matrix $A(x_1, \ldots, x_t)$ is non-singular if and only if $x_1, x_2, \ldots, x_t$ are distinct.

Theorem 6.8: BCH bound

Let C be an (n, k)-BCH code over GF(q) with designed distance δ. Then $d(C) \geq \delta$.

6.7 BCH Decoding

Later, because not covered in A4.

Index

A

alphabet . . . 5

B

BCH code . . . 34
block code . . . 5

C

characteristic . . . 13
code . . . 5
codeword . . . 5
coset . . . 26
cyclic code . . . 29
cyclic space . . . 29
cyclotomic coset of $q \pmod{n}$ containing i . . . 33

D

designed distance δ . . . 34
dual code . . . 24

E

e-error correcting code . . . 10
e-error detecting code . . . 9
equivalent codes . . . 23
extension field . . . 32

F

field . . . 12
finite field . . . 13

G

generator . . . 20
generator matrix . . . 22
generator polynomial . . . 30

H

Hamming distance . . . 7
Hamming weight . . . 22

I

ideal . . . 29
ideal generated by g . . . 30
infinite field . . . 13
information rate . . . 6
inner product . . . 24
irreducible over F . . . 16

L

length . . . 5
linear (n, k)-code over F . . . 21

M

minimal polynomial of α over $\mathrm{GF}(q)$ . . . 32
multiplicative group of $\mathrm{GF}(q)$ . . . 18

O

order of α . . . 19

order of a field 13
orthogonal code 24
orthogonal vectors 24

P

parity-check matrix 25
parity-check polynomial 31
principal ideal 30
principal ideal ring 30

R

ring 12

S

set of conjugates of α w.r.t. $\mathrm{GF}(q)$ 33
set of cyclotomic cosets of q mod n 33
standard form generator matrix 23
subfield 14
symbol error probability 6
systematic code 23

V

Vanderdmonde matrix 34

W

word 5