CONTEMPORARY MATHEMATICS

225

Finite Fields: Theory, Applications, and Algorithms

Fourth International Conference on
Finite Fields: Theory, Applications, and Algorithms
August 12–15, 1997
University of Waterloo, Waterloo, Ontario, Canada

Ronald C. Mullin
Gary L. Mullen
Editors

American Mathematical Society

Selected Titles in This Series

225 **Ronald C. Mullin and Gary L. Mullen, Editors,** Finite fields: Theory, applications, and algorithms, 1999

224 **Sang Geun Hahn, Hyo Chul Myung, and Efim Zelmanov, Editors,** Recent progress in algebra, 1999

223 **Bernard Chazelle, Jacob E. Goodman, and Richard Pollack, Editors,** Advances in discrete and computational geometry, 1999

222 **Kang-Tae Kim and Steven G. Krantz, Editors,** Complex geometric analysis in Pohang, 1999

221 **J. Robert Dorroh, Giséle Ruiz Goldstein, Jerome A. Goldstein, and Michael Mudi Tom, Editors,** Applied analysis, 1999

220 **Mark Mahowald and Stewart Priddy, Editors,** Homotopy theory via algebraic geometry and group representations, 1998

219 **Marc Henneaux, Joseph Krasil'shchik, and Alexandre Vinogradov, Editors,** Secondary calculus and cohomological physics, 1998

218 **Jan Mandel, Charbel Farhat, and Xiao-Chuan Cai, Editors,** Domain decomposition methods 10, 1998

217 **Eric Carlen, Evans M. Harrell, and Michael Loss, Editors,** Advances in differential equations and mathematical physics, 1998

216 **Akram Aldroubi and EnBing Lin, Editors,** Wavelets, multiwavelets, and their applications, 1998

215 **M. G. Nerurkar, D. P. Dokken, and D. B. Ellis, Editors,** Topological dynamics and applications, 1998

214 **Lewis A. Coburn and Marc A. Rieffel, Editors,** Perspectives on quantization, 1998

213 **Farhad Jafari, Barbara D. MacCluer, Carl C. Cowen, and A. Duane Porter, Editors,** Studies on composition operators, 1998

212 **E. Ramírez de Arellano, N. Salinas, M. V. Shapiro, and N. L. Vasilevski, Editors,** Operator theory for complex and hypercomplex analysis, 1998

211 **Józef Dodziuk and Linda Keen, Editors,** Lipa's legacy: Proceedings from the Bers Colloquium, 1997

210 **V. Kumar Murty and Michel Waldschmidt, Editors,** Number theory, 1998

209 **Steven Cox and Irena Lasiecka, Editors,** Optimization methods in partial differential equations, 1997

208 **Michel L. Lapidus, Lawrence H. Harper, and Adolfo J. Rumbos, Editors,** Harmonic analysis and nonlinear differential equations: A volume in honor of Victor L. Shapiro, 1997

207 **Yujiro Kawamata and Vyacheslav V. Shokurov, Editors,** Birational algebraic geometry: A conference on algebraic geometry in memory of Wei-Liang Chow (1911–1995), 1997

206 **Adam Korányi, Editor,** Harmonic functions on trees and buildings, 1997

205 **Paulo D. Cordaro and Howard Jacobowitz, Editors,** Multidimensional complex analysis and partial differential equations: A collection of papers in honor of François Treves, 1997

204 **Yair Censor and Simeon Reich, Editors,** Recent developments in optimization theory and nonlinear analysis, 1997

203 **Hanna Nencka and Jean-Pierre Bourguignon, Editors,** Geometry and nature: In memory of W. K. Clifford, 1997

202 **Jean-Louis Loday, James D. Stasheff, and Alexander A. Voronov, Editors,** Operads: Proceedings of Renaissance Conferences, 1997

201 **J. R. Quine and Peter Sarnak, Editors,** Extremal Riemann surfaces, 1997

(*Continued in the back of this publication*)

This page intentionally left blank

Finite Fields: Theory, Applications, and Algorithms

This page intentionally left blank

CONTEMPORARY MATHEMATICS

225

Finite Fields: Theory, Applications, and Algorithms

Fourth International Conference on
Finite Fields: Theory, Applications, and Algorithms
August 12–15, 1997
University of Waterloo, Waterloo, Ontario, Canada

Ronald C. Mullin
Gary L. Mullen
Editors

American Mathematical Society
Providence, Rhode Island

Editorial Board

Dennis DeTurck, managing editor

Andreas Blass Andy R. Magid Michael Vogelius

This volume contains the referreed proceedings of the Fourth International Conference on Finite Fields: Theory, Applications and Algorithms held at the University of Waterloo, Waterloo, Ontario, Canada, August 12–15, 1997.

1991 *Mathematics Subject Classification.* Primary 11T02;
Secondary 05B05, 11Y16, 94S60, 94B05.

Library of Congress Cataloging-in-Publication Data

International Conference on Finite Fields: Theory, Applications, and Algorithms (4th : 1997 : University of Waterloo)

Finite fields : theory, applications, and algorithms : Fourth International Conference on Finite Fields, Theory, Applications, and Algorithms, August 12–15, 1997, University of Waterloo, Ontario, Canada / Ronald C. Mullin, Gary L. Mullen, editors.

p. cm. — (Contemporary mathematics ; 225)

Includes bibliographical references.

ISBN 0-8218-0817-6 (alk. paper)

1. Finite fields (Algebra)—Congresses. I. Mullin, Ronald C. (Ronald Cleveland), 1936– . II. Mullen, Gary L. III. Title. IV. Series: Contemporary mathematics (American Mathematical Society) ; v. 225.

QA247.3.I58 1997

512′.3—dc21 98-38826

CIP

Copying and reprinting. Material in this book may be reproduced by any means for educational and scientific purposes without fee or permission with the exception of reproduction by services that collect fees for delivery of documents and provided that the customary acknowledgment of the source is given. This consent does not extend to other kinds of copying for general distribution, for advertising or promotional purposes, or for resale. Requests for permission for commercial use of material should be addressed to the Assistant to the Publisher, American Mathematical Society, P. O. Box 6248, Providence, Rhode Island 02940-6248. Requests can also be made by e-mail to `reprint-permission@ams.org`.

Excluded from these provisions is material in articles for which the author holds copyright. In such cases, requests for permission to use or reprint should be addressed directly to the author(s). (Copyright ownership is indicated in the notice in the lower right-hand corner of the first page of each article.)

© 1999 by the American Mathematical Society. All rights reserved.
The American Mathematical Society retains all rights
except those granted to the United States Government.
Printed in the United States of America.

⊗ The paper used in this book is acid-free and falls within the guidelines
established to ensure permanence and durability.
Visit the AMS home page at URL: `http://www.ams.org/`

10 9 8 7 6 5 4 3 2 1 04 03 02 01 00 99

Contents

Preface

This volume contains the refereed proceedings of the Fourth International Conference on Finite Fields: Theory, Applications, and Algorithms held at the University of Waterloo, August 12-15, 1997. The Organizing Committee consisted of I.F. Blake, R.C. Mullin, C.L. Stewart, S.A. Vanstone (all of the University of Waterloo), and S.D. Cohen, (University of Glascow), G. L. Mullen,(The Pennsylvania State University), H. Niederreiter, (Austrian Academy of Sciences, Vienna).

Because of applications in so many diverse areas, finite fields continue to grow in importance in modern mathematics. In particular,they now play very important roles in number theory, algebra, and algebraic geometry, as well as in computer science, statistics, and engineering. Areas of application include, but certainly are not limited to, algebraic coding theory, cryptology, and combinatorial design theory. Computational and algorithmic aspects of finite field problems also continue to grow in importance.

We greatly acknowledge the very generous support of the conference by our sponsors, namely The University of Waterloo, The National Security Agency, The National Science Foundation, CERTICOM Corp., and the Institute for Combinatorics and its Applications. Without their support, we would not have been able to invite so many eminent researchers, or to partially support junior faculty members, postdocs and graduate students.

The purpose of the conference was to bring together workers in theoretical, applied, and algorithmic finite field theory. All papers in this volume have been refereed, and have been very loosely classified as theoretical and applied, and are listed alphabetically by contact author under these very general headings.

On behalf of all of the participants, we would like to thank the Faculty of Mathematics and the Department of Combinatorics and Optimization at the University of Waterloo for their hospitality and support. Special thanks are due to Kim Gingrich and Marg Feeney for their tireless efforts in attending to every detail of the conference.

We also express our thanks to the participants for a lively and successful conference. We would also like to thank the authors for contributing to this volume and the referees for their invaluable assistance. Thanks are also due to Barbara Baum and Frances Hannigan for their help in preparation of parts of this volume. We also express our appreciation to the American Mathematical Society for publishing this volume in their series Comtemporary Mathematics, and in particular to Christine Thivierge (Amer. Math. Soc.) for her patience, care, and great assistance in the preparation of this volume.

Because of the success of this conference, frequently referred to as Fq4, and its earlier incarnations, we are delighted to report that Prof. D. Jungnickel of Augsburg

University, Augsberg, Germany, has agreed to host Fq5 on August 2–6, 1999. We look forward to what we are sure will be another very successful conference. We hope to see you there.

Gary L. Mullen

Ronald C. Mullin

Contemporary Mathematics
Volume **225**, 1999

Computing Composed Products of Polynomials

Joel V. Brawley, Shuhong Gao, and Donald Mills

ABSTRACT. If $f(x)$ and $g(x)$ are polynomials in $F_q[x]$ of degrees m and n respectively, then the *composed sum* of f and g, denoted $f*g$, is the degree mn polynomial whose roots are all sums of roots of f with roots of g. Likewise, the *composed multiplication* of f and g, denoted $f \circ g$, is the degree mn polynomial whose roots are all products of roots of f with roots of g. In 1987, Brawley and Carlitz defined a more general notion of polynomial composition, denoted by $f \diamond g$, for which $f*g$ and $f \circ g$ are special cases. They prove that when f and g are irreducible with degrees m and n coprime, then $f \diamond g$ is irreducible of degree mn. This gives us a way to obtain irreducibles of relatively large degree using irreducibles of smaller degrees. In this paper, we describe several methods of computing polynomial compositions of the above form and compare their time complexities.

1. Introduction

Let F_q denote the finite field of order $q = p^m$, p a prime, and let $f(x)$ and $g(x)$ be monic polynomials in $F_q[x]$. The *composed sum* of f and g is the polynomial defined by

$$f * g = \prod_{\alpha} \prod_{\beta} (x - (\alpha + \beta)) \tag{1.1}$$

while the *composed multiplication* of f and g is the polynomial defined by

$$f \circ g = \prod_{\alpha} \prod_{\beta} (x - \alpha\beta). \tag{1.2}$$

In both cases the product runs through all roots α of f and β of g, including multiplicities.

In [1] these compositions are generalized as follows. Let G be a nonempty subset of the algebraic closure Γ_q of F_q with the property that G is invariant under the Frobenius automorphism $\alpha \to \sigma(\alpha) = \alpha^q$, and suppose there is defined on G a binary operation $\diamond$ satisfying

$$\sigma(\alpha \diamond \beta) = \sigma(\alpha) \diamond \sigma(\beta) \tag{1.3}$$

1991 *Mathematics Subject Classification.* Primary 12Y05; Secondary 68Q25.

© 1999 American Mathematical Society

for all $\alpha, \beta \in G$. Then for monic polynomials f and g whose coefficients are in F_q and whose roots lie in G, the *composed product*, denoted $f \diamond g$, is the polynomial defined by

$$f \diamond g = \prod_{\alpha} \prod_{\beta} (x - (\alpha \diamond \beta)), \tag{1.4}$$

where again the products are over all roots α of f and β of g. It is clear that

$$deg\ f \diamond g = (deg\ f)(deg\ g),$$

and it is also clear that when $G = \Gamma_q$ and $\diamond$ is the usual addition (respectively, the usual multiplication) on Γ_q, then (1.4) becomes (1.1) (respectively (1.2)).

While the roots of f and g are in G and not necessarily in F_q, it is easy to prove that (1.3) implies that the composed product (1.4) has its coefficients in F_q [**1**]. Further, under the additional assumption that G is a group under $\diamond$, the composition (1.4) has the following property which allows for the construction of irreducibles over F_q of a relatively large degree from irreducibles over F_q of relatively small degrees.

THEOREM 1.1 ([**1**]). *Let $(G, \diamond)$ be a σ-invariant group satisfying (1.3) and let f, g be monic polynomials in $F_q[x]$ with roots in G. If* deg $f = m$ *and* deg $g = n$, *then the composed product $f \diamond g$ is irreducible in $F_q[x]$ if and only if f and g are irreducible in $F_q[x]$ and* $\gcd(m, n) = 1$.

The proof of Theorem 1.1 uses among other things the following property: If f and g factor as $f = f_1 f_2 \cdots f_r$ and $g = g_1 g_2 \cdots g_s$ where the f_i and g_j are irreducible in $F_q[x]$, then

$$(\prod_{i=1}^{r} f_i) \diamond (\prod_{j=1}^{s} g_j) = \prod_{i=1}^{r} \prod_{j=1}^{s} (f_i \diamond g_j). \tag{1.5}$$

Our main goal is to show how to compute $f \diamond g$ efficiently. In lieu of this, (1.5) shows that given the factorization of f and g, to find $f \diamond g$ one needs only to compute the compositions of the individual irreducible factors. Consequently, we shall focus on methods of computing compositions of irreducible polynomials.

In Section 2, we discuss the representation of the $\diamond$ operation, as well as show a connection between elliptic curve groups and the composed product. In Section 3, we show how to efficiently compute the general composed product. In Section 4, we specialize to $f * g$ and $f \circ g$. We first determine how to efficiently compute them using (1.1) and (1.2) directly, and then give formulas for $f * g$ and $f \circ g$ which are defined as determinants of matrices whose entries are polynomials. For these, we demonstrate how to find $f * g$ and $f \circ g$ efficiently using fast interpolation. We also show how to compute $f * g$ and $f \circ g$ using linear recurring sequences. We conclude with a brief summary.

Recall that if $h(x), k(x) \in F_q[x]$ with degrees at most n, then the number of F_q-operations needed to compute $h + k$ or $h - k$ is $O(n)$, while the time needed to multiply h by k is $O(M(n))$. Here $M(n) = n^2$ for classical multiplication and $nL(n)$ for fast multiplication (Schönhage & Strassen 1971, Schönhage 1977, and Cantor & Kaltofen 1991), where we use $L(n)$ in place of $\log n \log\log n$, as used by Shoup [**13**]. If we operate in the ring $F_q[x]/ < f(x) >$ (and so reduce the product

of h and k modulo f, where $deg\ f = n$), then the number of F_q-operations needed is $O(M_r(n))$. For classical multiplication, $M_r(n) = n^2$; for fast multiplication, $M_r(n) = nL(n)\log n$. The additional $\log n$ term is needed when using fast multiplication because the time needed to do long division of f into hk is $O(nL(n)\log n)$. In this paper, if we are given two polynomials f and g of degrees m and n respectively, we will always assume (for ease of exposition) that $m \sim n$ when discussing the running times.

2. Properties of the Diamond Binary Operation

2.1. Representations of the Binary Operation on G. We consider the form of the operation $\diamond$ defined on G. The following is stated in [1] but not proved.

THEOREM 2.1. *Suppose G is a finite σ-invariant subset of Γ_q on which there is defined a binary operation $\diamond$ satisfying (1.3). Then $\diamond$ can be represented by a polynomial $h(x,y) \in F_q[x,y]$ such that $h(\alpha,\beta) = \alpha \diamond \beta$ for all $\alpha, \beta \in G$.*

PROOF. Suppose $G = \{\alpha_1, \alpha_2, ..., \alpha_t\}$ where $t = |G|$. By Lagrange interpolation, define

$$h(x,y) = \sum_{1 \le i,j \le t} (\alpha_i \diamond \alpha_j) \frac{S_i(x)}{W_i} \frac{S_j(y)}{W_j}$$

where S_i and W_i are defined as

$$S_i(x) = \prod_{\alpha \in G, \alpha \neq \alpha_i} (x - \alpha),\ W_i = \prod_{\alpha \in G, \alpha \neq \alpha_i} (\alpha_i - \alpha).$$

It is clear that $h(\alpha,\beta) = \alpha \diamond \beta$ for all $\alpha, \beta \in G$. We need to prove that $h(x,y) \in F_q[x,y]$. Since G is σ-invariant, σ induces a permutation on the elements in G. Hence

$$\begin{aligned}
[h(x,y)]^q &= \sum_{(i,j)} \left((\alpha_i \diamond \alpha_j) \frac{S_i(x)}{W_i} \frac{S_j(y)}{W_j} \right)^q \\
&= \sum_{(i,j)} (\alpha_i \diamond \alpha_j)^q \frac{(S_i(x))^q}{W_i^q} \frac{(S_j(y))^q}{W_j^q} \\
&= \sum_{(i,j)} (\alpha_{\sigma(i)} \diamond \alpha_{\sigma(j)}) \frac{S_{\sigma(i)}(x^q)}{W_{\sigma(i)}} \frac{S_{\sigma(j)}(y^q)}{W_{\sigma(j)}}
\end{aligned}$$

where $\alpha_i^q = \alpha_{\sigma(i)}$ and $\alpha_j^q = \alpha_{\sigma(j)}$. But since σ induces a permutation on the elements in G, and since the sum is taken over all (i,j), we have

$$[h(x,y)]^q = \sum_{(i,j)} (\alpha_i \diamond \alpha_j) \frac{S_i(x^q)}{W_i} \frac{S_j(y^q)}{W_j} = h(x^q, y^q).$$

So each coefficient of $h(x,y)$ belongs to F_q. □

Note that G does not have to be finite in order for us to represent composed products as polynomials in $F_q[x,y]$, as seen in Section 1 for $f * g$ and $f \circ g$. Also note that if G is not finite, the operation $\diamond$ may not have a polynomial representation [3].

In this paper we are concerned only with polynomial representations of composed products.

We can also go the other way; that is, if we are given $h(x,y) \in F_q[x,y]$, we can use $h(x,y)$ to define a $\diamond$ operation on a suitable subset G of the closure, where by "suitable" we mean that G is closed under $\diamond$.

THEOREM 2.2. *For every $h(x,y) \in F_q[x,y]$ and every nonempty subset S of Γ_q, there exists a smallest subset G containing S such that*

- *G is σ-invariant and*
- *The operation defined by $\alpha \diamond \beta = h(\alpha,\beta)$ is a binary operation on G satisfying (1.3).*

Moreover, if S is finite then so is G.

PROOF. Put $S_0 = \{\alpha^{q^i} : \alpha \in S, i \geq 0\}$. By definition, we see that S_0 is σ-invariant. Now for $i = 0, 1, 2, \ldots$ define S_{i+1} by

$$S_{i+1} = \{h(\alpha,\beta) : \alpha, \beta \in S_i\} \bigcup S_i.$$

This produces a nested sequence of sets $S_0 \subseteq S_1 \subseteq \cdots \subseteq S_i \subseteq \cdots$. Note that each S_i is σ-invariant, and $\sigma(\alpha \diamond \beta) = \sigma(\alpha) \diamond \sigma(\beta)$ for each S_i. Moreover, for each $i \geq 1$, $\alpha \diamond \beta \in S_i$ for all $\alpha, \beta \in S_{i-1}$.

Now let $G = \bigcup_{i \geq 0} S_i$. Then G is closed under $\diamond$. If S is finite, then there is an extension of F_q, say F_{q^m} for some m such that $S \subseteq F_{q^m}$. Obviously, $S_i \subseteq F_{q^m}$ for all i, so that $G \subseteq F_{q^m}$. □

2.2. Elliptic Curve Groups: A Special Case. We show that almost any elliptic curve group is isomorphic to a finite σ-invariant subset G of Γ_q, with an appropriate binary operation $\diamond$ satisfying (1.3). For a brief introduction to elliptic curves over finite fields, see [**8**].

THEOREM 2.3. *If $(E,+)$ is an elliptic curve group over the field F_q (consisting of F_q-rational points), $q > 3$ odd, then there exists a finite σ-invariant subset G of Γ_q and a group operation $\diamond$ on G such that $(G,\diamond)$ is isomorphic to $(E,+)$ and σ is an automorphism of $(G,\diamond)$.*

PROOF. Let $E = \{(x,y)\} \bigcup \{[0]\}$ denote the points on an elliptic curve over F_q, $q > 3$ odd, and let $a \in F_q$ be a quadratic nonresidue. Then $(x^2 - a) \in F_q[x]$ is irreducible and if $\alpha \in F_{q^2}$ is a root of $x^2 - a$, then α satisfies $\alpha^q = -\alpha$. Let $e \in F_q$ have the property that the point $(e,0)$ is not on the curve. Such a point must exist since at most three points on E have the form $(x,0)$. Consider the mapping $\nu : E \to F_{q^2}$ defined as follows:

$$\nu(P) = \begin{cases} e & \text{if } P = [0] \\ x + y\alpha & \text{if } P = (x,y). \end{cases}$$

Clearly ν is a one-to-one correspondence between E and a subset G of Γ_q, and further, the elliptic curve addition induces an operation $\diamond$ on G which makes G isomorphic to E; namely,

$$\nu(P) \diamond \nu(Q) = \nu(P + Q). \tag{2.1}$$

It remains to show that G is σ-invariant and that σ is an automorphism of $(G, \diamond)$.

Now if $P = (x, y)$ is on E, then so is its negative, $-P = (x, -y)$. Thus, we may write

$$(\nu(P))^q = (x + y\alpha)^q = x + y\alpha^q = x + y(-\alpha) = x - y\alpha = \nu(-P).$$

Also, by choice of e, the relation

$$(\nu(P))^q = \nu(-P) \tag{2.2}$$

holds when $P = [0]$ so (2.2) is valid for all P on E, implying that G is σ-invariant.

Using both (2.1) and (2.2), we have $\sigma(\nu(P)) \diamond \sigma(\nu(Q)) = \nu(-P) \diamond \nu(-Q) = \nu(-(P+Q))$ which by (2.2) is $(\nu(P+Q))^q$. But then (2.1) gives us $(\nu(P+Q))^q = (\nu(P) \diamond \nu(Q))^q = \sigma(\nu(P) \diamond \nu(Q))$, which shows that σ is an automorphism of the group G. □

3. Computing the General Composed Product

Suppose that $f \diamond g$ is defined as in (1.4), and suppose the diamond product is represented by $h(x, y) \in F_q[x, y]$, i.e. $\alpha \diamond \beta = h(\alpha, \beta)$ for all $\alpha, \beta \in G$. Our goal is to compute $f \diamond g$ efficiently. We assume by (1.5) that f and g are irreducible of degrees m and n respectively. By the definition (1.4), one needs to construct an extension field of F_q that contains the roots of f and g. When $\gcd(m, n) = 1$, the smallest such field is $F_{q^{mn}}$, and it can be constructed as $F_{q^m}[y]/ < g(y) >$ where $F_{q^m} = F_q[x]/ < f(x) >$. In other words, $F_{q^{mn}} \simeq R = F_q[x, y]/I$ where $I =< f(x), g(y) >$ is the ideal in $F_q[x, y]$ generated by $f(x)$ and $g(y)$. Let $\bar{x}$ represent the class of x and $\bar{y}$ the class of y in R. Then the roots of $f(z)$ are $\bar{x}^{q^i}$, $0 \le i \le m-1$, and the roots of $g(z)$ are $\bar{y}^{q^j}$, $0 \le j \le n-1$. When computing in R, one always reduces powers of x modulo $f(x)$ and powers of y modulo $g(y)$. The composition $f \diamond g$ can be computed by Algorithm 3.1 below.

When $\gcd(m, n) > 1$, the smallest field that contains the roots of f and g is $F_{q^{mn/d}}$ where $d = \gcd(m, n)$. One can still construct $F_{q^m} = F_q[x]/ < f(x) >$, but $F_{q^m}[y]/ < g(y) >$ is no longer a field. In fact, $g(y)$ factors over F_{q^m} as a product of d irreducibles of degree n/d. We will prove below that factoring is not necessary, and the same algorithm that is used for the case where $\gcd(m, n) = 1$ works for all m and n.

ALGORITHM 3.1. *Computing $f \diamond g$.*

INPUT: $f, g \in F_q[x]$ *of degrees m and n respectively;*
$h(x, y) = \sum_{(i,j)} c_{ij} x^i y^j \in F_q[x, y]$.

OUTPUT: $f \diamond g$.

Step 0: *Form the ring $R = F_q[x, y]/I$, where $I =< f(x), g(y) >$ and each class is represented by a unique polynomial of degree $\le m-1$ in x and degree $\le n-1$ in y.*

Step 1: *Compute the polynomials $u_i \equiv x^{q^i} \bmod f(x)$, $0 \le i \le m-1$*

and $v_j \equiv y^{q^j} \bmod g(y)$, $0 \le j \le n-1$.

Step 2: *In* R, *compute* $h_{ij} = h(u_i, v_j)$, $0 \le i \le m-1$ *and* $0 \le j \le n-1$.

Step 3: *In* $R[z]$, *compute and output the polynomial* $\prod_{i=0}^{m-1} \prod_{j=0}^{n-1} (z - h_{ij})$.

END.

THEOREM 3.2. *Algorithm 3.1 computes* $f \diamond g$ *correctly, and when* $m \sim n$, *it uses*

$$O(nM_r(n) \log q + n^2 M_r(n) T \log E + n^4 M_r^2(n))$$

F_q*-operations, where* E *is the largest degree of* x *or* y *in* $h(x, y)$ *and* T *is the number of nonzero terms in* $h(x, y)$.

PROOF. The correctness follows from Lemma 3.4 below. We give the time needed to compute $f \diamond g$. In Step 1, u_i and v_j can be computed iteratively by raising to the q^{th} power using $O(nM_r(n) \log q)$ F_q-operations. In Step 2, the h_{ij} are computed using $O(n^2 M_r(n) T \log E)$ F_q-operations. In Step 3, the product polynomial can be computed iteratively. At the k^{th} iteration, we multiply $(z - h_{ij})$ by a degree k polynomial in $R[z]$ with $O(k)$ multiplications in R. Hence the total number of R-operations used to compute the product polynomial is $O(\sum_{k=1}^{mn-1} k) = O(n^4)$. Now each multiplication in R can be done with $O(M_r(m)M_r(n)) = O(M_r^2(n))$ operations in F_q by viewing R as $F_{q^m}[y]/ < g(y) >$ where $F_{q^m} = F_q[x]/ < f(x) >$. So the total time for Step 3 is $O(n^4 M_r^2(n))$ operations in F_q. Hence the total time for Algorithm 3.1 is as stated in the theorem. □

Using classical multiplication, the time for Algorithm 3.1 is

$$O(n^3 \log q + n^4 T \log E + n^8);$$

using fast multiplication, the time is

$$O(n^2 L(n) \log n \log q + T n^3 L(n) \log n \log E + n^6 (L(n))^2 (\log n)^2),$$

where $L(n) = \log n \log\log n$.

COROLLARY 3.3. *Algorithm 3.1 computes* $f * g$ *and* $f \circ g$ *correctly using*

$$O(nM_r(n) \log q + n^4 M_r^2(n))$$

F_q*-operations.*

LEMMA 3.4. *Let* $f(x) \in F_q[x]$, $g(y) \in F_q[y]$ *be irreducible of degrees* m *and* n *respectively. Define the algebra* $R = F_q[x, y]/ < f(x), g(y) >$ *with* $\bar{x} = x + < f(x), g(y) >$ *and* $\bar{y} = y + < f(x), g(y) >$. *Then the polynomial*

$$s(z) = \prod_{k=0}^{m-1} \prod_{l=0}^{n-1} \left(z - \bar{x}^{q^k} \diamond \bar{y}^{q^l} \right) \in R[z] \tag{3.1}$$

equals $(f \diamond g)(z)$, *which is viewed as a polynomial over* R *by the natural embedding of* F_q *in* R.

PROOF. Let K represent any extension field of F_q over which f and g split completely, say

$$f(x) = \prod_{i=1}^{m}(x - \alpha_i), \quad g(y) = \prod_{j=1}^{n}(y - \beta_j).$$

Define the algebra $W = K[x, y]/ < f(x), g(y) >$. Note that $K \subset W$ and $F_q \subset R \subset W$ by means of natural embeddings. The polynomials $s(z)$ and $(f \diamond g)(z)$ are viewed as polynomials over W; we prove that they are equal over W and thus equal over R. Define in W

$$\epsilon_i = \frac{\prod_{l \neq i}(\bar{x} - \alpha_l)}{\prod_{l \neq i}(\alpha_i - \alpha_l)}, \quad \nu_j = \frac{\prod_{l \neq j}(\bar{y} - \beta_l)}{\prod_{l \neq j}(\beta_j - \beta_l)},$$

where $1 \leq i \leq m$ and $1 \leq j \leq n$. Note that $\sum_{i=1}^{m} \epsilon_i = 1$, $\epsilon_i \epsilon_j = 0$ for $i \neq j$ and $\epsilon_i^2 = \epsilon_i$ for $1 \leq i \leq m$; similar statements can be made for the ν_j. Also, $\bar{x} = \sum_{i=1}^{m} \alpha_i \epsilon_i$ and $\bar{y} = \sum_{j=1}^{n} \beta_j \nu_j$.

The elements $\{\epsilon_i \nu_j\}$, $1 \leq i \leq m$ and $1 \leq j \leq n$, are primitive idempotents in W and form an orthogonal basis for W over K. Denote $\eta_{ij} = \epsilon_i \nu_j$ for each i and j. We have $\sum_{(i,j)} \eta_{ij} = 1$, $\bar{x} = \sum_{(i,j)} \alpha_i \eta_{ij}$ and $\bar{y} = \sum_{(i,j)} \beta_j \eta_{ij}$. Also $W = K\eta_{11} \oplus K\eta_{12} \oplus \cdots \oplus K\eta_{mn}$.

Since the η_{ij} are orthogonal idempotents, we have $\bar{x} \diamond \bar{y} = \sum_{(i,j)} \eta_{ij}(\alpha_i \diamond \beta_j)$ and $z = \sum_{(i,j)} z\eta_{ij}$. Hence

$$\begin{aligned}
s(z) = \prod_{(k,l)}(z - \bar{x}^{q^k} \diamond \bar{y}^{q^l}) &= \prod_{(k,l)} \left(z - \sum_{(i,j)} \eta_{ij}(\alpha_i^{q^k} \diamond \beta_j^{q^l}) \right) \\
&= \prod_{(k,l)} \left(\sum_{(i,j)} \eta_{ij}(z - \alpha_i^{q^k} \diamond \beta_j^{q^l}) \right) \\
&= \sum_{(i,j)} \eta_{ij} \prod_{(k,l)} (z - \alpha_i^{q^k} \diamond \beta_j^{q^l}) \\
&= \sum_{(i,j)} \eta_{ij}(f \diamond g)(z) \\
&= (f \diamond g)(z).
\end{aligned}$$

This proves the lemma. □

4. Computing $f * g$ and $f \circ g$

In this section, we explore alternate methods of computing (1.1) and (1.2), and improve the running times given in Corollary 3.3.

4.1. Computing $f * g$ and $f \circ g$ via the Definitions.

Note that

$$f * g = \prod_{\alpha,\beta}(x - (\alpha + \beta)) = \prod_{\alpha} \prod_{\beta}((x - \alpha) - \beta) = \prod_{\alpha} g(x - \alpha)$$

and

$$f \circ g = \prod_{\alpha,\beta}(x - \alpha\beta) = \prod_{\alpha} \prod_{\beta} \alpha((x/\alpha) - \beta) = \prod_{\alpha} \alpha^n g(x/\alpha).$$

Similarly, $f * g = \prod_{\beta} f(x - \beta)$ and $f \circ g = \prod_{\beta} \beta^m f(x/\beta)$. The products are taken over all roots α of f and β of g.

We discuss the number of F_q-operations needed to find $f*g$. Let $F_{q^n} = F_q[y]/ < g(y) >$. Then the roots of g are $\beta_j \equiv y^{q^j} \mod g(y)$ for $0 \leq j \leq n-1$. To compute $f * g$, we first compute $f(x - \beta_j)$, $0 \leq j \leq n-1$, and then multiply them as follows: pair the factors $f(x - \beta_j)$ together and calculate the product of each pair; then pair these results and repeat the process until all factors are combined. Note that β_j, $0 \leq j \leq n-1$, can be computed by repeatedly raising to the q^{th} power using $O(nM_r(n) \log q)$ F_q-operations. For each j, $f(x - \beta_j)$ can be computed via its Taylor series at $x = 0$:

$$f(x - \beta_j) = f(-\beta_j) + f'(-\beta_j)x + \frac{f''(-\beta_j)}{2!}x^2 + \cdots + \frac{f^{(m)}(-\beta_j)}{m!}x^m.$$

Note that each coefficient $\dfrac{f^{(k)}(-\beta_j)}{k!}$ is just a linear combination of the elements $1, \beta_j, \beta_j^2, ..., \beta_j^m$ with scalars in F_q. We compute $1, \beta_j, \beta_j^2, ..., \beta_j^m$ using $O(mM_r(n))$ F_q-operations. Each coefficient of $f(x-\beta_j)$ can be computed in $O(n^2)$ F_q-operations, and so each $f(x - \beta_j)$ can be computed in time $O(mn^2) = O(n^3)$. Hence all the $f(x - \beta_j)$ can be computed in time $O(n^4)$. Note that the $f(x - \beta_j)$ can also be computed by Horner's Rule; however, the cost is greater, even if one uses fast multiplication.

To multiply the $f(x - \beta_j)$, $0 \leq j \leq n-1$, we require $\log n$ iterations. At the k^{th} iteration ($0 \leq k \leq \lceil \log n \rceil - 1$), we multiply $(n/2^{k+1})$ pairs of polynomials in $F_{q^n}[x]$, each of degree at most $2^k m$. The k^{th} iteration needs $O((n/2^{k+1})M_r(2^k m)) = O(M_r(mn)) = O(M_r(n^2))$ F_{q^n}-operations. All the iterations need $O(M_r(n^2) \log n)$ F_{q^n}-operations, or $O(M_r(n^2)M_r(n) \log n)$ F_q-operations. The total time needed to find $f * g$ is stated in Theorem 4.1. We can compute $f \circ g$ similarly by pairing factors, but each factor $\beta^m f(x/\beta)$ can be found directly, without using Taylor series. The number of F_q-operations needed to find all the $\beta_j^m f(x/\beta_j)$ is $O(mnM_r(n)) = O(n^2 M_r(n))$.

THEOREM 4.1. *The composed sum $f * g$ can be computed with the formula $f * g = \prod_{\beta} f(x - \beta)$ using*

$$O(n^4 + M_r(n)M_r(n^2) \log n + nM_r(n) \log q)$$

F_q-operations. Likewise, the composed multiplication $f \circ g$ can be computed with the formula $f \circ g = \prod_{\beta} \beta^m f(x/\beta)$ using

$$O(M_r(n)M_r(n^2) \log n + nM_r(n) \log q)$$

F_q-operations.

Using classical multiplication, the time given in Theorem 4.1 is $O(n^6 \log n + n^3 \log q)$ for both $f * g$ and $f \circ g$; using fast multiplication, the time is $O(n^4 + n^3 L(n)L(n^2)(\log n)^3 + n^2 L(n) \log n \log q)$ for $f * g$, and $O(n^3 L(n)L(n^2)(\log n)^3 + n^2 L(n) \log n \log q)$ for $f \circ g$. These times improve upon the time given in Corollary 3.3.

4.2. Matrix Methods. The methods below are matrix-oriented, and stem from the use of the tensor, or Kronecker, product operation to calculate $f \diamond g$ [1]. We will specialize to $f * g$ and $f \circ g$ following a presentation of the general approach.

Recall that if A and B are square matrices over F_q of sizes m and n respectively, then the Kronecker product of A and B is the square matrix over F_q of size mn given by $A \otimes B = (a_{ij}B)$ [1]. The eigenvalues of $A \otimes B$ are of the form $\alpha\beta$ [6] where α and β range over the eigenvalues for A and B, respectively, so that

$$\det(xI - A \otimes B) = \prod_{\alpha} \prod_{\beta} (x - \alpha\beta).$$

From this we conclude that if f and g are monic nonconstant polynomials over F_q with companion matrices A and B, respectively, then

$$f \circ g = \det(xI - A \otimes B).$$

More generally, we consider the case where G is a σ-invariant subset of Γ_q, and we define a binary operation $\diamond$ on G where $x \diamond y = h(x, y) = \sum_{(i,j)} c_{ij} x^i y^j \in F_q[x, y]$ [1]. For square matrices A and B over F_q, define a binary operation $H(A; B)$ where

$$H(A; B) = \sum_{(i,j)} c_{ij}(A^i \otimes B^j),$$

and the exponents i, j for A and B denote ordinary, as opposed to tensor, matrix products. These exponents correspond to the ones given in the above equation for $x \diamond y$. The eigenvalues of $H(A; B)$ are the numbers $h(\alpha, \beta)$ [6], where α and β range over the eigenvalues for A and B, respectively. Hence

$$\det\left(xI - H(A; B)\right) = \prod_{\alpha} \prod_{\beta} (x - h(\alpha, \beta)),$$

so that if f and g are any two polynomials over F_q with degrees m and n respectively and with companion matrices A and B, respectively, then from [1] we have

$$f \diamond g = \det\left(xI - H(A; B)\right).$$

For the case where $H(\alpha, \beta) = \alpha + \beta$, we have

$$f * g = \det\left(xI_{mn} - (A \otimes I_n + I_m \otimes B)\right),$$

where I_n denotes the n-square identity matrix.

While we now have the advantage of working in F_q, the sizes of the tensor product matrices can quickly become huge, so we prefer to use a method that employs matrices of smaller size. The formulas presented below accomplish this by building on the formulas given above, using matrix theory and symmetric function theory to obtain better formulas for $f \circ g$ and $f * g$.

THEOREM 4.2 ([8]). *Let* $f(x) = \sum_{i=0}^{m} a_i x^i$ *and* $g(x) = \sum_{j=0}^{n} b_j x^j$ *be two monic polynomials over* F_q *of degrees* m *and* n*, respectively, each having distinct roots. Let* A *and* B *be their respective companion matrices. Then*

$$f \circ g = \det\left(\sum_{j=0}^{n} b_j x^j A^{n-j}\right) = \det\left(\sum_{i=0}^{m} a_i x^i B^{m-i}\right) \tag{4.1}$$

and

$$f * g = \det\left(\sum_{j=0}^{n} b_j (xI_m - A)^j\right) = \det\left(\sum_{i=0}^{m} a_i (xI_n - B)^i\right) \tag{4.2}$$

are both polynomials over F_q of degree mn.

Since f and g are each devoid of repeated roots, their companion matrices are each similar to a diagonal matrix whose nonzero entries contain the polynomial's roots. A proof for (4.1) is given below. The proof that follows is similar to the proof of (4.2) given in [**8**], and is given for sake of completeness.

PROOF. Use the facts that, for matrices A, B, C, and D of appropriate sizes, $(A \otimes B)(C \otimes D) = (AC) \otimes (BD)$ and $(A \otimes B)^{-1} = A^{-1} \otimes B^{-1}$ (provided A^{-1} and B^{-1} exist). Let the eigenvalues of A, which are the roots of f, be represented by $\alpha_1, ..., \alpha_m$ and let D be the diagonal matrix whose nonzero entries are the α_i. Then there is an invertible matrix P (whose elements lie in some extension field of F_q) such that $A = PDP^{-1}$. Hence

$$\begin{aligned}
f \circ g = \det(xI_{mn} - A \otimes B) &= \det(xI_{mn} - (PDP^{-1}) \otimes B) \\
&= \det(x(P \otimes I_n)(P^{-1} \otimes I_n) - (PDP^{-1}) \otimes B) \\
&= \det((P \otimes I_n)(xI_{mn} - D \otimes B)(P^{-1} \otimes I_n)) \\
&= \det(xI_{mn} - D \otimes B) \\
&= \det(diag(xI_n - \alpha_i B)) \\
&= \prod_{i=1}^{m} \det(xI_n - \alpha_i B) \\
&= \det\left(\prod_{i=1}^{m} (xI_n - \alpha_i B)\right) \\
&= \det\left(\sum_{i=0}^{m} a_i x^i B^{m-i}\right).
\end{aligned}$$

□

In order to compute $f * g$ and $f \circ g$ efficiently using (4.1) and (4.2), we use Newton's interpolation method (see [**4**] for details). This involves choosing $mn + 1$ distinct points c_i, $i = 0, 1, ..., mn$, from an extension field of F_q of sufficient size, and evaluating $f * g$ and $f \circ g$ at these points. These values are then used to recover the polynomials, which have degree mn. Note that an extension field of sufficient size is F_{q^e} where $e = O(\log_q mn)$. Also, we choose the points c_i so that fast interpolation can be done (as in FFT).

Now to the implementation, where for convenience we let

$$J(x) = \det\left(\sum_{i=0}^{m} a_i x^i B^{m-i}\right)$$

and

$$K(x) = \det\left(\sum_{i=0}^{m} a_i (xI_n - B)^i\right).$$

Note that the field F_{q^e} can be constructed in negligible time for our application (see [**12**] and [**13**] for details). The number of F_{q^e}-operations required to find $J(c_i)$ (similarly, $K(c_i)$) for any i is $O(n^3)$; here we use Horner's Rule and the sparseness of the companion matrix B. Hence all the values $\det[J(c_i)]$ (similarly, $\det[K(c_i)]$) are found in time $O(n^5)$. Using fast interpolation, the number of F_{q^e}-operations needed to find the coefficients of $f * g$ (similarly, $f \circ g$) is $O(n^2 \log n^2)$ (again, we refer the reader to Schönhage & Strassen 1971, Schönhage 1977, and Cantor & Kaltofen 1991). The total number of F_{q^e}-operations needed to find $f * g$ (similarly, $f \circ g$) is $O(n^5)$, or $O(n^5 M_r(e))$ F_q-operations. While this method costs more than the one given in Section 4.1 for fast multiplication, it is not dependent upon the size of q.

The polynomials $f * g$ and $f \circ g$ can also be written as variants of the resultant of $f(x)$ and $g(x)$. To be specific, we use the fact [**4**] that the resultant of f and g can be written as $\prod_{i=1}^{m} \prod_{j=1}^{n} (\alpha_i - \beta_j)$ (assuming that f and g are monic). If we introduce a new variable z, then

$$f * g = res_z(f(x - z), g(z)) = res_z(g(x - z), f(z)), \tag{4.3}$$

where res denotes the resultant. Likewise we have

$$f \circ g = (-1)^{mn} res_z \left(z^n g\left(\frac{x}{z}\right), f(z) \right). \tag{4.4}$$

Use Schwartz's algorithm [**11**] for fast resultant calculation to compute $(f * g)(c_i) = res_z(f(c_i - z), g(z))$ in $O(n \log^2 n)$ F_{q^e}-operations, where c_i has the same meaning as above. Then the number of F_{q^e}-operations needed to find the values $(f*g)(c_i)$ (similarly, $(f \circ g)(c_i)$) is $O(mn(n \log^2 n)) = O(n^3 \log^2 n)$. The time needed to recover the polynomial is absorbed into the above running time, so that the time needed to find $f * g$ and $f \circ g$ using F_q-operations is $O((n^3 \log^2 n) M_r(e))$, the best of the times given yet. As with the method which uses (4.1) and (4.2), its time is independent of the size of q. We summarize these results in the next theorem.

THEOREM 4.3. *The composed products $f \circ g$ and $f * g$ can be computed with formulas (4.1) and (4.2), respectively, using $O(n^5 M_r(e))$ F_q-operations. If (4.3) and (4.4) are used instead, the number of F_q-operations required to compute $f * g$ and $f \circ g$ is $O((n^3 \log^2 n) M_r(e))$. In both cases, $e = O(\log_q n)$.*

Note in closing that the method used to find (4.1) and (4.2) can be extended to the case where either α or β is linear in the polynomial representation of $\alpha \diamond \beta$. Let $\alpha_1, \ldots, \alpha_m$ represent the roots of f, where f is defined as in Theorem 4.2. We have

$$\begin{aligned} f \diamond g &= \det \left[\prod_{k=1}^{m} h(B)[h^{-1}(B)(xI_n - t(B)) - \alpha_k I_n] \right] \\ &= \det(h^m(B) f(Y)) \\ &= \det \left(\sum_{k=0}^{m} a_k (xI_n - t(B))^k h^{m-k}(B) \right) \end{aligned}$$

where $Y = h^{-1}(B)(xI_n - t(B))$, and $h(B)$ and $t(B)$ are polynomials in B. In particular, $h(B)$ is associated with those terms in the polynomial representation of

$\alpha \diamond \beta$ in which the exponent of α is one, and $t(B)$ corresponds to the remainder of the terms.

4.3. Linear Recursive Sequences and Composed Products. A method of computing $f*g$ and $f \circ g$ which allows us to work entirely within F_q is to use linear recursive sequences (LRS) and the Berlekamp-Massey Algorithm. The method for finding $f \circ g$ using LRS's was described to us by John Brillhart [**2**], who attributed the method to D.H. Lehmer. We derive a formula for the kth term of the sequence whose minimal polynomial is $f * g$, and use this to compute $f * g$.

Recall that a *linear recursive sequence* $\{a_j\}$ is generated by a polynomial $f(x) = x^m + \sum_{k=0}^{m-1} f_k x^k \in F[x]$, F a field, if $a_j = -\sum_{k=1}^{m} f_{m-k} a_{j-k}$ for $j = m, m+1, \ldots$. Such a polynomial of smallest degree is called the minimal polynomial of the sequence.

We first show how to find $f \circ g$ via LRS's. Suppose (nonzero) LRS's $\{a_k\}$ and $\{b_k\}$ have minimal polynomials $f(x), g(x) \in F_q[x]$, respectively. Suppose further that $f(x)$ and $g(x)$ have distinct roots $\alpha_1, \ldots, \alpha_m$ and $\beta_1, \ldots, \beta_n$, respectively. Then there exist elements A_i and B_j in some extension of F_q so that for all $k \geq 0$,

$$a_k = \sum_{i=1}^{m} A_i \alpha_i^k \qquad \text{and} \qquad b_k = \sum_{j=1}^{n} B_j \beta_j^k.$$

Then the kth element of the product sequence $\{a_k b_k\}$ is given by

$$a_k b_k = \sum_{i=1}^{m} \sum_{j=1}^{n} A_i B_j (\alpha_i \beta_j)^k.$$

Hence the products $\alpha_i \beta_j$, $1 \leq i \leq m$ and $1 \leq j \leq n$, are all the candidates for the roots of the minimal polynomial of $\{a_k b_k\}$. If all the $\alpha_i \beta_j$ are distinct, then the minimal polynomial is indeed $f \circ g$. For our purposes, if f and g are irreducible and of coprime degrees (so that the products of their roots are distinct), then $f \circ g$ is the minimal polynomial of the corresponding product sequence.

It is well known that the minimum number of elements of $\{c_k\} = \{a_k b_k\}$ needed to determine $f \circ g$ is $2mn$. Given a_0 through a_{2mn-1} and b_0 through b_{2mn-1} we compute c_0 through c_{2mn-1}; this new sequence provides the input for the Berlekamp-Massey Algorithm, which outputs $f \circ g$ (see [**7**] and [**9**] for details).

The steps taken to find $f \circ g$ are as follows. First we select nonzero starting states for $\{a_k\}$ and $\{b_k\}$; the simplest such states are ones with zeros for the first $m-1$ terms ($n-1$, respectively), and with a one for the mth term of the sequence (nth term, respectively). We use these starting states to generate a_m through a_{2mn-1} and b_n through b_{2mn-1} (via f and g respectively) using $O(mn(m+n)) = O(n^3)$ F_q-operations. The number of F_q-operations needed to find the subsequence $c_0, \ldots, c_{2mn-1}$ using componentwise multiplication is $O(n^2)$. The number of F_q-operations required for the Berlekamp-Massey Algorithm is $O((mn)^2) = O(n^4)$ [**9**]. So the total time needed to find $f \circ g$ is $O(n^4)$ F_q-operations. This time, while slower than the running time given in Section 4.1 (using fast multiplication), does not depend upon the value of q. It is also slower than the resultant-based interpolation method. The advantage in using this method, though, is that we work entirely in the ground field F_q.

We turn our attention to finding a linear recursive sequence whose minimal polynomial is $f * g$, where $f, g \in F_q[x]$ are irreducible and of coprime degree.

THEOREM 4.4. *Suppose $\{a_k\}$ and $\{b_k\}$ are (nonzero) linear recursive sequences having irreducible minimal polynomials $f(x)$ and $g(x)$ in $F_q[x]$, respectively. Suppose further that the degrees of f and g are relatively prime. Then $f * g$ is the minimal polynomial of the sequence $\{c_k\}$ whose k^{th} term is given by*

$$c_k = \sum_{i=0}^{k} \binom{k}{i} a_i b_{k-i}. \tag{4.5}$$

To prove this, we show that the elements of any nonzero LRS of a given polynomial can be written in terms of the trace function (this was stated in [**10**] but not proven), and then use the fact that the degrees of f and g are coprime to obtain (4.5).

LEMMA 4.5 ([**5**]). *Let $A = \{\alpha_0, \alpha_1, ..., \alpha_{m-1}\}$ and $B = \{\gamma_0, \gamma_1, ..., \gamma_{m-1}\}$ be a pair of dual bases of F_{q^m}/F_q, and let ψ be any element of F_{q^m}. Then the coordinate x_i of α_i in $\psi = x_0\alpha_0 + x_1\alpha_1 + \cdots + x_{m-1}\alpha_{m-1}$ equals $Tr(\psi\gamma_i)$, and likewise the coordinate a_i of γ_i in $\psi = a_0\gamma_0 + a_1\gamma_1 + \cdots + a_{m-1}\gamma_{m-1}$ equals $Tr(\psi\alpha_i)$.*

LEMMA 4.6. *Let $f = x^m + \sum_{k=0}^{m-1} f_k x^k$ be irreducible, and let α represent a root of f. Then a nonzero sequence $\{a_k\}$ is generated by $f(x)$ iff there exists a $\psi \in F_{q^m}$ such that $a_i = Tr(\psi\alpha^i)$ for all $i \geq 0$.*

PROOF. Suppose $a_i = Tr(\psi\alpha^i)$ for all $i \geq 0$. Since $\{\alpha^i\}$ is generated by $f(x)$ (because α is a root of $f(x)$) and since the trace function is linear, $\{a_i\}$ is also generated by $f(x)$.

Now let $\{\gamma_0, \gamma_1, ..., \gamma_{m-1}\}$ represent the dual basis for $\{1, \alpha, ..., \alpha^{m-1}\}$. Take $\psi = \sum_{i=0}^{m-1} a_i\gamma_i \in F_{q^m}$. Then $a_i = Tr(\psi\alpha^i)$ for $i = 0, 1, ..., m-1$. Suppose $a_i = Tr(\psi\alpha^i)$ for $0 \leq i \leq k-1$ where $k \geq m$. Then

$$\begin{aligned} Tr(\psi\alpha^k) = Tr\left(-\psi \sum_{i=1}^{m} f_{m-i}\alpha^{k-i}\right) &= \left(-\sum_{i=1}^{m} f_{m-i} Tr(\psi\alpha^{k-i})\right) \\ &= \left(-\sum_{i=1}^{m} f_{m-i} a_{k-i}\right) \\ &= a_k. \end{aligned}$$

The lemma follows by induction on k. □

So under the conditions set forward for f, we can generate *any* nonzero LRS by using the trace function on an appropriate multiple of the elements of the basis corresponding to f. Similar statements can be made for the irreducible g of degree n over F_q mentioned above. For this polynomial, we use the notation β for its roots, $\{b_k\}$ for its associated nonzero LRS, and let $\rho \in F_{q^n}$ play the same role as ψ above.

We require one more result before proving Theorem 4.4.

LEMMA 4.7 ([**5**]). *Let $A = \{\alpha_0, \alpha_1, ..., \alpha_{m-1}\}$ and $B = \{\beta_0, \beta_1, ..., \beta_{n-1}\}$ be bases for $K = F_{q^m}$ and $L = F_{q^n}$ over $F = F_q$, respectively, and assume that m and n are coprime. Then one has the following results, where we write $E = F_{q^{mn}}$.*

- $C = \{\alpha_i\beta_j : i = 0, ..., m-1 \ ; \ j = 0, ..., n-1\}$ *is a basis for* E/F.
- $Tr_{E/F}(\kappa\lambda) = Tr_{K/F}(\kappa)Tr_{L/F}(\lambda)$ *for all* $\kappa \in K$ *and all* $\lambda \in L$.

PROOF OF THEOREM 4.4. Apply Lemma 4.6 to f and g. Thus there exist elements $\psi \in F_{q^m}$ and $\rho \in F_{q^n}$ such that $a_k = Tr(\psi\alpha^k)$ and $b_k = Tr(\rho\beta^k)$ for each k. Since f and g are irreducible and of coprime degree, $f * g$ is irreducible. Let $c_k = Tr(\psi\rho(\alpha+\beta)^k)$. Then by Lemma 4.6, $\{c_k\}$ is generated by $f * g$. Since $f * g$ is irreducible, it is the minimal polynomial of $\{c_k\}$. Note that

$$\begin{aligned} c_k = Tr[\psi\rho(\alpha+\beta)^k] &= Tr\left[\sum_{i=0}^{k}\binom{k}{i}\psi\rho\alpha^i\beta^{k-i}\right] \\ &= \sum_{i=0}^{k}\binom{k}{i}Tr(\psi\rho\alpha^i\beta^{k-i}) \\ &= \sum_{i=0}^{k}\binom{k}{i}Tr(\psi\alpha^i)Tr(\rho\beta^{k-i}) \\ &= \sum_{i=0}^{k}\binom{k}{i}a_i b_{k-i} \end{aligned}$$

where we use Lemma 4.7 in the third line. We have proved the theorem. □

Using the formula $\binom{k}{i} = \binom{k-1}{i} + \binom{k-1}{i-1}$, one can compute all the $\binom{k}{i}$ and thus the c_k, $k \le 2n^2$, in time $O((mn)^2) = O(n^4)$. So the total time needed to find $f * g$ is again $O(n^4)$ F_q-operations.

The results of this portion of the paper are summarized in the following theorem.

THEOREM 4.8. *Suppose that* $\{a_k\}$, $\{b_k\}$ *are nonzero linear recurring sequences whose elements come from* F_q, *with irreducible minimal polynomials* $f(x), g(x) \in F_q[x]$ *respectively. Suppose further that the degrees of* f *and* g *are relatively prime. Then the composed products* $f \circ g$ *and* $f * g$ *can be computed with the sequences* $\{a_k\}$ *and* $\{b_k\}$ *using* $O(n^4)$ F_q*-operations.*

5. Summary

We have shown that a general composition $f \diamond g$ can be computed in

$$O(nM_r(n)\log q + n^2 M_r(n) T \log E + n^4 M_r^2(n))$$

F_q-operations. In the special cases of $f \circ g$ and $f * g$, we presented several fast methods for computing them. All of the methods given in Section 4 were shown to be faster than the general method in Section 3. The fastest method is the interpolation method as applied to (4.3) and (4.4), with the running time being

$$O((n^3 \log^2 n) M_r(e))$$

F_q-operations, where $e = O(\log_q mn) = O(\log_q n)$. While the LRS method costs more (it requires $O(n^4)$ F_q-operations), it is better than the resultant method in that we operate entirely within the ground field F_q. The resultant method requires us to work in an appropriate extension of F_q so that fast interpolation can be done.

Recall that the running time for the method of Section 4.1 (as applied to $f \circ g$) is

$$O(n^3 L(n) L(n^2)(\log n)^3 + n^2 L(n) \log n \log q)$$

when fast multiplication is used. This method is inefficient for large q (in comparison with the LRS method, the Section 4.1 method is inefficient for values of q such that $\log q \geq n^2$). We conclude that the most efficient methods for computing $f * g$ and $f \circ g$ are the resultant-based interpolation method and the LRS method.

References

[1] Brawley, J.V. and Carlitz, L. *Irreducibles and the Composed Product for Polynomials Over a Finite Field.* North-Holland, Amsterdam; Discrete Mathematics 65 (1987), 115-139.

[2] Brillhart, John. Private Communication.

[3] Brown, David D. *Iterated Presentations and Module Polynomials Over Finite Fields.* Ph.D. Thesis, Clemson University, 1990.

[4] Geddes, Keith O.; Czapor, Stephen R.; Labahn, George. *Algorithms for Computer Algebra.* Kluwer, Boston, 1992.

[5] Jungnickel, Dieter. *Finite Fields: Structure and Arithmetics.* Wissenschaftsverlag, Mannheim, 1993.

[6] MacDuffee, C.C. *The Theory of Matrices.* Chelsea, New York, 1946.

[7] Massey, J.L. *Shift-Register Synthesis and BCH Decoding.* IEEE Transactions on Information Theory, vol. IT-15, January 1969, 122-127.

[8] Menezes, Alfred J. (editor); Blake, Ian F.; Gao, XuHong; Mullin, Ronald C.; Vanstone, Scott A.; Yaghoobian, Tomik. *Applications of Finite Fields.* Kluwer, Boston, 1993.

[9] Menezes, Alfred J.; van Oorschot, Paul C.; Vanstone, Scott A. *Handbook of Applied Cryptography.* CRC Press, Boca Raton, FL, 1997.

[10] Rueppel, Rainer A. and Staffelbach, Othmar J. *Products of Linear Recurring Sequences with Maximum Complexity.* IEEE Transactions on Information Theory, vol. IT-33, no. 1, January, 1987, 124-131.

[11] Schwartz, J.T. *Fast Probabilistic Algorithms for Verification of Polynomial Identities.* J. Assoc. Comput. Mach. 27 (1980), no. 4, 701-717.

[12] Shoup, Victor. *New Algorithms for Finding Irreducible Polynomials Over Finite Fields.* Math. Comp. 54 (1990), no. 189, 435-447.

[13] Shoup, Victor. *Fast Construction of Irreducible Polynomials Over Finite Fields.* J. Symbolic Comput. 17 (1994), no. 5, 371-391.

Department of Mathematical Sciences, Clemson University, Clemson, South Carolina 29634

E-mail address: jvbrw@clemson.edu, sgao@math.clemson.edu, ddmills@math.clemson.edu

This page intentionally left blank

Contemporary Mathematics
Volume **225**, 1999

Actions of Linearized Polynomials on the Algebraic Closure of a Finite Field

By *Stephen D. Cohen*[1]
and *Dirk Hachenberger*[2]

Abstract. Let g and h be monic polynomials in $F[x]$, where F is the finite field of order q. We define a dynamical system by letting the q-linearized polynomial associated with g act on equivalence classes of a certain F-subspace of the algebraic closure $\bar{F}$ of F in which related elements of $\bar{F}$ lie in the same orbit under the action of the q-linearized polynomial associated with h. When $h = x$, this is equivalent to the system in which the dynamic polynomial g acts on irreducible polynomials over F as discussed in [CH], where a conjecture of Morton [M] was proved as regards linearized polynomials. A generalization of that result is proved here. This states that when g and h are non-constant relatively prime polynomials, then there are infinitely many classes with prescribed preperiod and primitive period in the (g, h)-dynamical system.

Mathematics Subject Classification. 11T30, 11T99, 58F22.

Acknowledgements. Parts of this research were done while the second author was a visitor of the first author at the University of Glasgow. He thanks the Deutsche Forschungsgemeinschaft for supporting this visit through a Forschungsstipendium. He also thanks the Department of Mathematics of the University of Glasgow for its kind hospitality. This paper expands the invited talk of the first author at the 4th International Conference on Finite Fields and Applications at the University of Waterloo, Canada, 12-15 August, 1997. He gratefully acknowledges support from the conference.

[1]Department of Mathematics, University of Glasgow, Glasgow G12 8QW, Scotland, sdc@maths.gla.ac.uk

[2]Institut für Mathematik, Universität Augsburg, 86159 Augsburg, Germany, Hachenberger@math.uni-augsburg.de

© 1999 American Mathematical Society

1. Introduction

Let $F = \mathrm{GF}(q)$ and $\bar{F}$ be the algebraic closure of F. For any polynomial $f = \sum_i f_i x^i$ in $F[x]$, let $A_q(f)$ be the associated (additive) *q-linearized polynomial* (or simply *q-polynomial*) $\sum_i f_i x^{q^i}$ and set

$$x^f := A_q(f)(x). \tag{1.1}$$

By these means we obtain the set A_F of all q-polynomials. Moreover, A_F acquires a ring structure through addition and *polynomial composition.* Indeed, the association $f \to A_q(f)$ yields a ring isomorphism from $F[x]$ to A_F (see [O] or [LN]).

By the *dynamics* of a mapping γ on a set S is meant all that pertains to the orbits of elements of S under iterates of γ. For $i \geq 0$ let $\gamma^{(i)}$ denote the ith iterate of γ (with $\gamma^{(0)}$ being the identity on S). An element $s \in S$ is called *periodic*, if its orbit $\{\gamma^{(i)}(s) \mid i \geq 0\}$ is finite. If s is periodic and $k \geq 0$ and $n \geq 1$ are minimial such that $\gamma^{(k)}(s) = \gamma^{(k+n)}(s)$, then k is called the *preperiod of* s, while n is called the *primitive period* of s. A periodic element is called *purely periodic* if its preperiod is zero. The *backward orbit* of $s \in S$ is the set of all $t \in S$ for which there exists an $i \geq 0$ such that $\gamma^{(i)}(t) = s$, excluding the members of the orbit of s different from s, if s is purely periodic. We refer to (S, γ) as a *dynamical system.*

In this paper γ will be induced by a monic q-polynomial $A_q(g)$ in which event the above mentioned isomorphism reduces the study of iterates and composites of dynamical mappings to that of powers and products of ordinary polynomials, respectively. For the set S we may, in the first instance, choose $S = \bar{F}$. If $A_q(g)$ acts naturally on S (i.e., by evaluation), it is clear that every element is periodic. Moreover, if g is non-constant, then, given n, there are at most finitely many purely periodic elements of primitive period n: this is because $A_q(g^n - 1)$ is a nonzero polynomial and thus has only finitely many roots. Studies delineating those primitive periods (and preperiods) that can be realized in the dynamical system $(\bar{F}, A_q(g))$ and on other questions relating the dynamical structure to the polynomial and field structures have been undertaken by Batra and Morton [BM1, BM2] and Chou and Cohen [CC] and will not be discussed here in detail.

Nevertheless we elaborate on one aspect of the system just introduced. The subset V_g of $\bar{F}$ comprising the purely periodic elements of $(\bar{F}, A_q(g))$ can be partitioned into equivalence classes under the relation ρ_g defined by the rule that $(\alpha, \beta) \in \rho_g$ if and only if α and β lie in the same orbit under $A_q(g)$ (evidently, this can be done for every dynamical system (S, γ)). For example, if $g = x$ (so that $A_q(x)$ is the Frobenius automorphism $w \to w^q$

on $\bar{F}$), then $V_x = \bar{F}$ and $(\alpha, \beta) \in \rho_x$ if and only if α and β have the same minimal polynomial over F. In fact, if μ_α denotes the minimal polynomial of α over F, then $\alpha \to \mu_\alpha$ induces a bijection between the set V_x/ρ_x of equivalence classes of ρ_x and the set I_F of monic *irreducible* polynomials in $F[x]$. Observe that each $n \geq 1$ occurs as a primitive period. Another case in which $V_g = \bar{F}$ is the trivial one when $g = 1$, i.e., when $A_q(g)$ is the identity map: then V_1/ρ_1 essentially is the same as the set $\bar{F}$. Section 2 will include a more explicit description of the set V_g in general: it is always an F-subspace of $\bar{F}$ which is invariant under the Frobenius automorphism.

For a more general dynamical system, yet one that retains $A_q(g)$ as the dynamical polynomial, let h be another monic polynomial in $F[x]$ and take S to be the set V_h/ρ_h. Since $(\alpha^g)^h = (\alpha^h)^g$, there is a natural action of $A_q(g)$ on V_h/ρ_h: if $\rho_h(\alpha)$ denotes the equivalence class of α, then

$$A_q(g)(\rho_h(\alpha)) := \rho_h(A_q(g)(\alpha)) = \rho_h(\alpha^g) \tag{1.2}$$

is well-defined. In particular, if $h = 1$ we recover the situation discussed above and if $h = x$, then, from the previous paragraph we obtain a system equivalent to that in which the linearized polynomial $G := A_q(g)$ acts on I_F by defining

$$G(\mu_\alpha) := \mu_{\alpha^g}.$$

Such dynamical systems (I_F, G) (in a more general context in which the dynamic polynomial G need not be additive) were introduced by Vivaldi [V]. They were studied more intensively by Batra and Morton [BM1], [BM2], by Morton [M] and by Cohen and Hachenberger [CH]. For these systems the dynamics is richer because, potentially, there are *infinitely* many purely periodic elements of *any* given period. Indeed, in [CH], in establishing a conjecture of Morton [M] in the case of q-polynomials, it was shown that, for g not of the form x^l ($l \geq 0$ an integer), the system $(I_F, A_q(g))$, equivalently $(V_x/\rho_x, A_q(g))$, contains infinitely many elements having prescribed primitive period n (≥ 1) and preperiod k (≥ 0).

In the present paper we consider the general situation with arbitrary monic q-polynomials g and h. For simplicity, we refer to $(V_h/\rho_h, A_q(g))$ as the (g, h)-*(dynamical) system.* In order to extend the above mentioned result of [CH], necessarily, we except those polynomials satisfying a relation of the form $g^r = h^s$ where $r, s \geq 0$ are integers. In particular, we suppose that g and h are non-constant polynomials. In fact, since $A_q(h^i)$ ($i \geq 0$) induces the identity mapping on V_h/ρ_h, the (gh^i, h)-system has the same dynamics as the (g, h)-system. Consequently, we may assume that h does not divide g. Additionally, we impose the further constraint that g and h

are relatively prime, which however may not be altogether necessary. The result is as follows.

Theorem 1.1 *Let g and h be monic and relatively prime non-constant polynomials in $F[x]$. Let $n \geq 1$ and $k \geq 0$ be integers. Then there exist infinitely many classes $\lambda \in V_h/\rho_h$ which, with respect to the action of $A_q(g)$ definied in (1.2), have primitive period n and preperiod k.*

To complete this introduction we mention a simplification. If $g = g_0^l$ ($l \geq 2$), the existence of an element λ in V_h/ρ_h with primitive period ln and preperiod lk with respect to the (g_0, h)-system guarantees that λ has primitive period n and preperiod k in the (g, h)-system. Hence, we may assume that g is a *non-power*, i.e., g is different from g_0^l for $l \geq 2$, an integer.

2. Additive order and its uses

The notion of the additive order or F-order of an element $\alpha \in \bar{F}$ is fundamental to our study. References relevant to the present context are [H1], [CH].

By Section 1, $\bar{F}$ can be interpreted as an $F[x]$-module wherein the action of $f \in F[x]$ on $\alpha \in \bar{F}$ is given by $\alpha^f := A_q(f)(\alpha)$ (see (1.1)). Let $\mathcal{P}_F$ denote the set of all monic polynomials of $F[x]$ which are indivisible by x. The finite $F[x]$-submodules of $\bar{F}$ correspond bijectively to the members of $\mathcal{P}_F$: $f \in \mathcal{P}_F$ corresponds to the set of roots of $A_q(f)$ in $\bar{F}$. Moreover, every finite $F[x]$-submodule is cyclic, i.e., free on one generator. For any $\alpha \in \bar{F}$, the *F-order* or *additive order* of α (denoted by $\mathrm{Ord}_F(\alpha)$) is the polynomial $f \in \mathcal{P}_F$ of least degree for which $\alpha^f = 0$. In particular $\mathrm{Ord}_F(0) = 1$. The generators of the submodule corresponding to $f \in \mathcal{P}_F$ are exactly the elements $\alpha \in \bar{F}$ such that $\mathrm{Ord}_F(\alpha) = f$. There are precisely $\Phi_q(f)$ (> 0) such generators, where Φ_q denotes the finite field Euler function. For more details about $F[x]$-submodules, we refer to [H1, H2].

We state some simple properties of additive orders. For $\alpha, \beta \in \bar{F}$, $\mathrm{Ord}_F(\alpha + \beta)$ is a divisor of $\mathrm{Ord}_F(\alpha) \cdot \mathrm{Ord}_F(\beta)$ with equality if $\mathrm{Ord}_F(\alpha)$ and $\mathrm{Ord}_F(\beta)$ are coprime. A crucial result for the dynamics of linearized polynomials is the following.

Lemma 2.1 *Let $\alpha \in \bar{F}$. If $\mathrm{Ord}_F(\alpha) = f$ and $g \in F[x]$, then $\mathrm{Ord}_F(\alpha^g) = f/\gcd(g, f)$ (where* gcd *denotes the greatest common (monic) divisor).* □

Let $h \in F[x]$ be monic. We are now prepared to deduce a description of the subset V_h of $\bar{F}$ comprising exactly the purely periodic elements of the dynamical system $(\bar{F}, A_q(h))$ (see Section 1).

Proposition 2.2 *For any polynomial $h \in F[x]$,*

$$V_h = \{\alpha \in \bar{F} \mid \gcd(\mathrm{Ord}_F(\alpha), h) = 1\}. \tag{2.1}$$

Moreover, V_h is an $F[x]$- submodule of $\bar{F}$.

Proof. Let C_h be the right hand side of (2.1), i.e., the set of all elements $\alpha \in \bar{F}$ whose F-order is coprime to h. If $\alpha \in \bar{F}$ and $f \in F[x]$ then, by Lemma 2.1, the F-order of α^f is a divisor of $\mathrm{Ord}_F(\alpha)$. Thus, C_h is invariant under the action of $A_q(f)$ for all $f \in F[x]$. Now, if $\alpha \in V_h$, then $\alpha^{h^n} = \alpha$ for some integer $n \geq 1$. Thus, a further application of Lemma 2.1 shows that $\alpha \in C_h$. Conversely, if $\alpha \in C_h$, let l be the *multiplicative order of h modulo* $\mathrm{Ord}_F(\alpha)$, i.e., $l \geq 1$ is the least integer such that $h^l - 1$ is divisible by $\mathrm{Ord}_F(\alpha)$. Then $\alpha^{h^l} = \alpha$, whence $\alpha \in V_h$. □

For simplicity, throughout let $M_h := V_h/\rho_h$. As in the proof of Proposition 2.2, Lemma 2.1 shows that, for $\alpha, \beta \in V_h$, $\mathrm{Ord}_F(\alpha) = \mathrm{Ord}_F(\beta)$ whenever $\alpha \in \rho_h(\beta)$. Hence, for any $\lambda \in M_h$, we may define

$$\mathrm{Ord}_F(\lambda) := \mathrm{Ord}_F(\alpha), \text{ where } \alpha \in \lambda. \tag{2.2}$$

This shows that each member of M_h is periodic. We next proceed to demonstrate the pre-eminence of additive order for the preperiod and primitive periods of elements of M_h in the (g, h)-dynamical system for arbitrary polynomials g and h. Clearly, $\lambda = \rho_h(\alpha)$ $(\alpha \in V_h)$ is *purely periodic* if and only if $\alpha^{g^n} = \alpha^{h^l}$ for some integers $n \geq 1$ and $l \geq 0$. In this case the primitive period of λ is the minimal such value of n, denoted by $\pi_{g,h}\{\lambda\}$. Then, clearly,

$$\pi_{g,h}\{\lambda\} = \min\{n \mid \mathrm{Ord}_F(\lambda) \text{ divides } g^n - h^l \text{ for some } l \geq 0\}. \tag{2.3}$$

Combining (2.2) and Lemma 2.1, similarly to the proof of Proposition 2.2, we derive a description of the set $\mathcal{P}_{g,h}$ of purely periodic elements in the (g, h)-system.

Proposition 2.3 *Let $P_{g,h}$ be the set of purely periodic elements of M_h in the (g, h)-system and let $V_{g,h}$ be the union of all $\lambda \in P_{g,h}$ (regarding each such λ as a subset of V_h). Then $V_{g,h} = V_g \cap V_h = V_{gh}$, i.e., $V_{g,h}$ is the set of all $\alpha \in \bar{F}$ whose F-order is coprime to gh.* □

Following Proposition 2.3, for any $n \geq 1$, we define $P_{g,h}(n)$ as the subset of $P_{g,h}$ comprising all elements of primitive period n. From (2.3), if $\lambda \in$

$P_{g,h}(n)$, then all $\rho \in M_h$ with $\mathrm{Ord}_F(\rho) = \mathrm{Ord}_F(\lambda)$ are in $P_{g,h}(n)$. We can therefore, for $f \in \mathcal{P}_F$, define

$$\pi_{g,h}(f) := \pi_{g,h}\{\lambda\} \text{ for all } \lambda \in M_h \text{ with } \mathrm{Ord}_F(\lambda) = f. \tag{2.4}$$

Observe that, if g and h are simply related in the sense that $g^r = h^s$ $(r \geq 1, s \geq 0)$, then $\pi_{g,h}(f) \leq r$ for any $f \in \mathcal{P}_F$ which is coprime to gh. Such a pair (g,h) is excluded by the assumption from Theorem 1.1. It is an open problem whether the assertion of Theorem 1.1 concerning the primitive periods can be strengthened by replacing the relative primeness of g and h with the above mentioned trivial necessary condition.

As far as the preperiods are concerned, we will finally show that the additive order also leads to a satisfactory classification of the preperiodic structure in M_h in an arbitrary (g,h)-system. Let U_g be the (unique) complementary $F[x]$-submodule of V_g in $\bar{F}$. Then U_g consists of all elements α such that $\nu(\mathrm{Ord}_F(\alpha))$ divides g, where $\nu(f)$ denotes the square-free part of a polynomial f, i.e., the product of all distinct irreducible monic factors of f. Let $U_{g,h}$ be the intersection of U_g with V_h. Then V_h is equal to the direct sum of $V_{g,h} = V_{gh}$ with $U_{g,h}$. Since $U_{g,h}$ is an $F[x]$-submodule of $\bar{F}$, it is a union of members of M_h: let $Q_{g,h}$ be the subset of M_h corresponding to $U_{g,h}$. Then, essentially by Lemma 2.1, $Q_{g,h}$ is the backward orbit of $\rho_h(0) \in P_{g,h}(1)$ in the (g,h)-system. More generally, since $V_{g,h}$ is a complete system of coset representatives of $U_{g,h}$ in V_h, for any purely periodic element λ, the backward orbit of λ comprises exactly those classes in M_h whose union is equal to $\lambda + U_{g,h}$. Consequently, most of the information about the preperiodic structure of the (g,h)-system is contained in $U_{g,h}$.

By definition, $\alpha \in U_{g,h}$ if and only if $f = \mathrm{Ord}_F(\alpha)$ is relatively prime to h and satisfies $\nu(f)$ divides $\nu(g)$. Thus, if $\nu(g)$ divides $\nu(h)$, then $f = 1$ and $U_{g,h} = \{0\}$ which means that every member of M_h is purely periodic. On the other hand, if a is an irreducible divisor of g which does not divide h, then $U_{g,h}$ contains infinitely many elements. In fact, by considering the $F[x]$-submodule U_a of $U_{g,h}$, one can already show that the preperiods of each purely periodic member of M_h can achieve each value $k \geq 0$. Assume that $\lambda \in M_h$ has F-order f coprime to gh and let $\alpha \in \lambda$. Assume further that $k \geq 0$. Let a^m $(m \geq 1)$ be the largest power of a dividing g. Then, again by Lemma 2.1, any element of M_h of order $a^{km}f$ has preperiod k and primitive period equal to that of λ. Moreover, see [H2], there exists a $\beta \in \bar{F}$ with $\mathrm{Ord}_F(\beta) = a^{km}f$ and $\beta^{g^k} = \alpha$, whence $A_q(g)^{(k)}(\rho_h(\beta)) = \lambda$. Summarizing, we have that the part of Theorem 1.1 relating to preperiods is a consequence of the rest.

Theorem 2.4 *Let $g, h \in F[x]$ be monic non-constant polynomials. Then the following hold.*

(1) *If $\nu(g)$ divides h, then $\mathcal{P}_{g,h} = M_h$.*

(2) *If $\nu(g)$ does not divide h, then for each $\lambda \in \mathcal{P}_{g,h}$ and each integer $k \geq 0$, there exists an $\eta \in M_h$ which has preperiod k and satisfies $A_q(g)^{(k)}(\eta) = \lambda$.* □

From now on we shall only consider purely periodic elements and therefore assume that all additive orders f are co-prime to gh. Because of (2.4) we tend to work with F-orders rather than members of $P_{g,h}$.

We finally remark that for the $(g,1)$-system (with $M_1 = \bar{F}$), Chou and Cohen [CC] further classify the preperiodic structure. Similar details can certainly be set down for the general (g,h)-system.

3. Infinitely many F-orders f with $\pi_{g,h}(f) = n$ from one

Consider a (g,h)-system, where g and h are non-constant monic polynomials over F. Following Section 2, define $\mathcal{P}_{g,h}(n)$ as the set of all F-orders $f \in \mathcal{P}_F$ prime to gh such that $\pi_{g,h}(f) = n$. The aim of this section is to show that, under the assumption of Theorem 1.1, $\mathcal{P}_{g,h}(n)$ is infinite provided it is non-empty.

Observe first that (2.3) and (2.4) can be recast to yield

$$\pi_{g,h}(f) = \min\{n |\, f \text{ divides } g^n - h^l \text{ for some } l \geq 0\}. \tag{3.1}$$

Thus, $\pi_{g,h}(f)$ can be interpreted as the group order of $g + fF[x]$ in the group of units $U_f^\times$ modulo f factorized by the subgroup $[h]$ generated by $h + fF[x]$. In fact, our main problem concerning the primitive periods in the (g,h)-system can be formulated as follows.

Given polynomials g, h over F and $n \geq 1$ an integer, do there exist infinitely many $f \in \mathcal{P}_F$, relatively prime to gh, such that the group order of $g + fF[x]$ in $U_f^\times/[h]$ is equal to n?

Lemma 3.1 *Assume that $f, f^* \in \mathcal{P}_F$ are relatively prime to gh. Let $n \geq 1$ and $m \geq 0$ be integers. Then the following hold.*

(1) *f divides $g^n - h^l$ if and only if $\pi_{g,h}(f)$ divides n.*

(2) *If f divides f^*, then $\pi_{g,h}(f)$ divides $\pi_{g,h}(f^*)$.* □

We are now prepared to prove the main result of this section. Note that it is convenient to assume that g and h are coprime.

Theorem 3.2 *Let g, h be monic non-constant polynomials in $F[x]$ which are relatively prime. Assume that f is a polynomial in $\mathcal{P}_F$ relatively prime to gh. If $\pi_{g,h}(f) = n$, then $\mathcal{P}_{g,h}(n)$ is infinite.*

Proof. Because $\pi_{g,h}(f) = n$, by (2.3) there exists $m \geq 0$ such that f divides $f_0 := g^n - h^m$. Since g and h are relatively prime, f_0 is prime to gh and therefore a member of $\mathcal{P}_{g,h}$. Moreover, from Lemma 3.1, $\pi_{g,h}(f_0) = n$. Let d be the multiplicative order of h modulo f. For $l \geq 0$, let $f_l := g^n - h^{m+ld}$ (relatively prime to gh). Since f divides both $g^n - h^m$ and $h^d - 1$, it also divides $f_l = g^n - h^m - h^m(h^{ld} - 1)$. Thus, again by Lemma 3.1, $\pi_{g,h}(f_l) = n$ for all l. Since the f_i are all distinct ($i \geq 0$), we conclude that $\mathcal{P}_{g,h}(n)$ is infinite. □

We remark that it follows from Theorem 3.2 that $\mathcal{P}_{g,h}(1)$ is infinite because $\{0\}$ is a member.

4. Irreducible F-orders with primitive period coprime to p

Let p be the characteristic of $F = \mathrm{GF}(q)$. In this section we consider again the (g, h)-system with g and h non-constant and relatively prime as in the statement of Theorem 1.1. Further, without loss of generality (as noted at the end of Section 1), we suppose that g is a *non-power*. The polynomial h, however, may be a power and we define m to be the maximal integer indivisible by p such that $h = h_0^m$ for some $h_0 \in F[x]$. Note that, additionally, h may be a p^eth power for some $e \geq 0$. If $m = 1$ we shall say that h is *at most a p-power*.

Given any n (≥ 1) indivisibe by p we prove directly that $\mathcal{P}_{g,h}(n)$ is infinite (and so certainly non-empty, cf. Theorem 3.2). To accomplish this goal, we seek to enumerate those F-orders f with $\pi_{g,h}(f) = n$ for which f is an *irreducible* polynomial over F of degree d, where n is a divisor of $q^d - 1$ and f is coprime to gh. Let $N_n^*(d)$ be the number of such f. We can take d to be any integer such that the least common multiple of m and n is a divisor of $q^d - 1$.

Suppose f is irreducible of degree d and θ is a root of f. Then $F(\theta) = \mathrm{GF}(q^d) =: F_d$, say. Moreover, by (3.1) we have

$$\pi_{g,h}(f) = \min\{n |\, g^n(\theta) = h^l(\theta) \text{ for some } l \geq 0\}. \tag{4.1}$$

Now, for the next part, suppose that h is at most a p-power. We shall indicate later modifications which treat the general case. Introducing yet one further notion of order - this time the multiplicative order $\mathrm{ord}(w)$ of non-zero elements w of $\bar{F}$ - we consider the relationship to (4.1) of the following conditions involving an element θ of F_d; namely

$$\mathrm{ord}(h(\theta)) = \frac{q^d - 1}{n}, \quad h(\theta) \neq 0 \tag{4.2}$$

$$\gcd(\frac{q^d-1}{\mathrm{ord}(g(\theta))}, n) = 1, \ g(\theta) \neq 0. \tag{4.3}$$

Assume that (4.2) and (4.3) hold for $\theta \in F_d$. Suppose, in fact, that $\theta \in F_{d_0}$, where d_0 divides d. Then $g(\theta), h(\theta) \in F_{d_0}$ and $\mathrm{ord}(g(\theta))$ and $\mathrm{ord}(h(\theta))$ are divisors of $q^{d_0}-1$. Hence, from (4.2), n is a multiple of $\frac{q^d-1}{q^{d_0}-1}$, whereas, from (4.3), n is relatively prime to this number. Hence $d = d_0$ and $F_d = F(\theta)$. Consequently, f is irreducible of degree d. Furthermore, (4.2) implies that $h(\theta)$ is a generator of the (cyclic) group of nth powers in F_d^*. Hence $g^n(\theta) = h^l(\theta)$ for some $l \geq 0$. Moreover, (4.3) guarantees that $g(\theta)$ is *not any kind of nth power* in F_d, i.e., $g(\theta) = \beta^e$ for e dividing n implies $e = 1$. Thus, (4.1) holds and $\pi_{g,h}(f) = n$. We conclude that if $N_n(d)$ denotes the cardinality of the subset of F_d satisfying (4.2) and (4.3) then, clearly,

$$N_n^*(d) \geq \frac{1}{d} \cdot N_n(d),$$

and it suffices to show that $N_n(d)$ is positive.

To state our results we repeat some notation from [CH]. Define n_1 as the part of n involving primes common to n and $\frac{q^d-1}{n}$. More precisely, write $n = n_1 n_2$, where n_1 and n_2 are relatively prime, the squarefree part $\nu(n_1)$ of n_1 is equal to the squarefree part of $\gcd(\frac{q^d-1}{n}, n)$ and $\gcd(\frac{q^d-1}{n}, n_2) = 1$.

In this section φ and μ are the regular Euler and Möbius functions, respectively, and, if $\omega(k)$ is the number of distinct prime factors of k, then $W(k) := 2^{\omega(k)}$ is the number of squarefree factors of k.

The crucial result is the following.

Proposition 4.1 *Let g and h be non-constant monic polynomials in $F[x]$, where $F = \mathrm{GF}(q)$. Assume that g and h are relatively prime and that g is a non-power and h at most a p-power. Then, for any integers n (≥ 1) indivisible by the characteristic p of F and d such that n divides $q^d - 1$, we have*

$$N_n(d) = \frac{\varphi(\frac{q^d-1}{n_1})\varphi(n_1)}{(q^d-1)n} \cdot (q^d + R), \tag{4.4}$$

where

$$|R| \leq nMq^{d/2}W(q^d-1)W(n_1) \tag{4.5}$$

and $M = \deg(g) + \deg(h) - 1$. (The trivial case $Mq^d = 2$ is excluded.)

Proof. Employing the characteristic functions E_1 and E_2 for the sets of elements of F_d satisfying (4.3) and (4.2), respectively, we obtain

$$N_n(d) = \sum_{\alpha \in F_d} E_1(\alpha) E_2(\alpha).$$

Here, see e.g., [Co],

$$E_1(\alpha) = \frac{\varphi(n)}{n} \sum_{r|n} \frac{\mu(r)}{\varphi(r)} \sum_{\mathrm{ord}(\chi)=r} \chi(g(\alpha)), \tag{4.6}$$

where the sum over χ is over all $\varphi(r)$ multiplicative characters of F_d of order r. The sum $E_2(\alpha)$ (associated with (4.2)) is rather more awkward but has the shape (taken from Lemma 2 of Carlitz [C]) given by

$$E_2(\alpha) = \frac{\varphi(\frac{q^d-1}{n})}{q^d-1} \sum_{s|q-1} \frac{\mu(s^*)}{\varphi(s^*)} \sum_{\mathrm{ord}(\eta)=s} \eta(h(\alpha)), \tag{4.7}$$

where the sum over η is over all multiplicative characters of order s and

$$s^* = \frac{s}{\gcd(s,n)}.$$

Accordingly,

$$N_n(d) = \frac{\varphi(n)}{n} \frac{\varphi(\frac{q^d-1}{n})}{(q^d-1)} \sum_{r|n} \sum_{s|q^d-1} \frac{\mu(r)}{\varphi(r)} \frac{\mu(s^*)}{\varphi(s^*)} \sum_{\mathrm{ord}(\chi)=r} \sum_{\mathrm{ord}(\eta)=s} S(\chi,\eta), \tag{4.8}$$

where $S(\chi,\eta)$ denotes the character sum

$$S(\chi,\eta) = \sum_{\alpha \in F_d} \chi(g(\alpha))\eta(h(\alpha)).$$

Because n_2 and $\frac{q^d-1}{n}$ are relatively prime, it is easy to see that, in (4.8), n_1 may replace n in $\varphi(n)\varphi(\frac{q^d-1}{n})$. But the important step is to estimate the character sums $S(\chi,\eta)$ for the characters which appear in (4.8). Clearly, if $\chi = \chi_0$ and $\eta = \eta_0$ are the trivial characters (of order 1), then

$$S(\chi,\eta) = q^d - M_0, \tag{4.9}$$

where $M_0 \leq M+1$ is the number of zeros of gh in F_d. Otherwise, by Weil's Theorem, see [L] (Chapter 6, Theorem 3, part (1)),

$$|S(\chi,\eta)| \leq Mq^{d/2}. \tag{4.10}$$

At this point it must be emphasized that (4.10) need not be valid for all relevant characters χ, η (not both trivial) if the conditions g, h relatively

prime, or h at most a p-power, were to be relaxed and a discussion of the general situation has to overcome such difficulties.

We deduce from (4.8) to (4.10) that $N_n(d)$ has the form (4.4), where

$$q^{-d/2}|R| \le M \sum_{r|n} \sum_{s|q^d-1} \frac{\lambda(r)}{\varphi(r)} \frac{\lambda(s^*)}{\varphi(s^*)} \varphi(r)\varphi(s) =: T_1 \tag{4.11}$$

and $\lambda = \mu^2$ here denotes Liouville's function. Evidently,

$$T_1 = MW(n)T_2,$$

where

$$T_2 = \sum_{s|q^d-1} \frac{\lambda(s^*)\varphi(s)}{\varphi(s^*)}. \tag{4.12}$$

Now, let Q be the part of $q^d - 1$ prime to n. Then, by the multiplicativity of the functions involved, T_2 can be expressed as

$$T_2 = \sum_{t|Q} \lambda(t) \cdot \sum_{u|q^d-1,\, \nu(u)|\nu(n)} \frac{\lambda(u^*)\varphi(u)}{\varphi(u^*)} = W(Q)T_3,$$

where the definition of u^* is analogous to that of s^* and where

$$T_3 = \sum_{u|n\nu(n_1)} \frac{\lambda(u^*)\varphi(u)}{\varphi(u^*)},$$

since $\lambda(u^*) = 0$ unless u divides $n\nu(n_1)$. Somewhat surprisingly perhaps, T_3 can be evaluated exactly (see [CH]) as

$$T_3 = nW(n_1),$$

leading to a precise evaluation of T_1. Using the fact that $W(n)W(Q) = W(q^d - 1)$ we deduce the bound (4.5) for $|R|$. □

By means of Proposition 4.1 and the explicit bound $W(k) \le 5k^{1/4}$ (see Lemma 3.3 of [CH]) we obtain the following result which establishes Theorem 1.1 for n indivisible by p and h at most a p-power (because we can choose any value of d larger than the stated bound to guarantee that $\mathcal{P}_{g,h}(n)$ is infinite).

Theorem 4.2 *Let g and h be non-constant monic polynomials in $F[x]$, where $F = \mathrm{GF}(q)$. Assume that g and h are relatively prime and that g is a non-power and h at most a p-power. Then, for any integer n (≥ 1)*

indivisible by the characteristic p of F and any integer d such that n divides $q^d - 1$ and

$$d \geq \frac{4\log(25n^{\frac{5}{4}}M)}{\log(q)}$$

(where $M = \deg(g) + \deg(h) - 1$), we have that $N_n(d)$ and $N_n^*(d)$ are positive. □

To complete this section we outline the modifications to the above discussion when h is a power. Assume $h = h_0^m$ with m indivisible by p as described at the beginning of the section. The other assumed conditions remain in force. In particular, we suppose that $q^d - 1$ is divisible by the least common multiple L of m and n. Let $l := \gcd(n, m)$, then $n' := n/l$ and $m' := m/l$ are relatively prime. We claim that the following extensions of (4.2) and (4.3) guarantee that $\theta \in F_d$ is the root of an irreducible polynomial f of degree d such that (4.1) holds (so that $\pi_{g,h}(f) = n$), they are

$$\operatorname{ord}(h_0(\theta)) = \frac{q^d - 1}{n'}, \ h_0(\theta) \neq 0, \tag{4.13}$$

$$\operatorname{ord}(g(\theta)) \text{ divides } \tfrac{q^d-1}{m'}, \ \gcd(\tfrac{q^d-1}{m'\operatorname{ord}(g(\theta))}, m'n') = 1, \ g(\theta) \neq 0. \tag{4.14}$$

Observe that (4.13) means that $h(\theta)$ generates the Lth powers of F_d^*. Further, (4.14) implies that $g(\theta)$ is an m'th power but no higher power which is a divisor of L. Note that h_0 is at most a p-power and we could carry out a calculation similar to that of Proposition 4.1 to yield a satisfactory estimate for the cardinality of the subset of F_d satisfying (4.13) and (4.14).

An alternative to the above procedure is to replace (4.14) by the more stringent condition

$$\operatorname{ord}(g(\theta)) = \frac{q^d - 1}{m'} \tag{4.15}$$

and employ some of the estimates used in Proposition 4.1.

To illustrate the above, take $n = 12$ and $m = 8$; thus $q^d - 1$ is divisible by $L = 24$. Further $n' = 3$ and $m' = 2$. Also (4.13) means that $h_0(\theta)$ is the cube of a primitive element of F_d. On the other hand, (4.14) implies that $g(\theta)$ is a square but neither a cube nor a 4th power, whereas (4.15) simply means that $g(\theta)$ is the square of a primitive element.

Denote by $N_n'(d)$ the cardinality of the subset of F_d satisfying (4.13) and (4.15). Then, by following the proof of Proposition 4.1, but using a further analogue of (4.12) for T_1 as well as T_2, we obtain an expression for $N_n'(d)$ of the form

$$N'_n(d) = c(q^d + R),\ c > 0,$$

where

$$|R| \leq mnMq^{d/2}W(\frac{q^d-1}{n})W(\frac{q^d-1}{m}).$$

Though this is not the best possible lower bound for $N_n(d)$, it leads to a satisfactory extension of Theorem 4.2 that suffices to establish that $\mathcal{P}_{g,h}(n)$ is infinite for n indivisible by p.

5. Generating F-orders with primitive period divisible by p

Once more consider the (g,h)-system where g and h are non-constant and relatively prime. We know from Sections 3 and 4 that $\mathcal{P}_{g,h}(n)$ is infinite whenever n is indivisible by the characteristic p of $F = \mathrm{GF}(q)$. Given n not divisible by p, we shall show in this section that from any $f \in \mathcal{P}_{g,h}(n)$ can be derived a distinct F-order f_l in $\mathcal{P}_{g,h}(np^l)$ for each $l \geq 1$. As a consequence of this, Theorem 1.1 is completely proved. Assume throughout that f and gh are relatively prime.

First, some remarks are offered on where to look for F-orders with primitive periods divisible by p. In Section 4, for any n indivisible by p, we found *irreducible* polynomials f in $\mathcal{P}_{g,h}(n)$. Although this is far from a comprehensive treatment, it is the case that, in broad terms, such periods are associated with square-free F-orders f.

On the one hand, $\pi_{g,h}(f) = n$ is indivisible by p whenever f is square-free. To justify this, suppose p divides n. Let N be the multiplicative order of g modulo f. Then f divides $g^N - 1$ and so, by the definition of n and Lemma 3.1 (1), n divides N. Consequently, p divides N and f divides $g^{N/p} - 1$ (since f is square-free). This contradicts the definition of N.

On the other hand, if p does not divide n and $f \in \mathcal{P}_{g,h}(n)$, we claim that the square-free part $\nu(f)$ of f also lies in $\mathcal{P}_{g,h}(n)$. To justify this, let $\pi_{g,h}(\nu(f)) = k$ and let f divide $\nu(f)^{p^l}$, where $l \geq 0$. Then $\nu(f)$ divides $g^k - h^m$, say, and so $\nu(f)^{p^l}$ divides $g^{kp^l} - h^{mp^l}$. It follows from Lemma 3.1 that $n = \pi_{g,h}(f)$ divides $\pi_{g,h}(\nu(f)^{p^l})$ and the latter divides kp^l. Since n is indivisible by p we conclude that $k = n$.

The above argument also reveals that, if $f \in \mathcal{P}_{g,h}(n)$ and $j \geq 0$ is an integer, then $\pi_{g,h}(f^{p^j})$ is of the form np^{l_j} with $(l_j)_{j\geq 0}$ being an increasing sequence of nonnegative integers. Thus it is sensible to search for members of $\mathcal{P}_{g,h}(np^l)$ of the form f^{p^j}. The key result is as follows.

Proposition 5.1 *Let g and h be relatively prime and monic polynomials in $F[x]$ of degree at least 1. Let $n \geq 1$ be an integer and assume that $\pi_{g,h}(f)$ divides n where $f \in \mathcal{P}_f$ is relatively prime to gh. Then there exists a power $P > 1$ of the characteristic p of F such that $\pi_{g,h}(f^P)$ does not divide n.*

Proof. Observe first that by (1) of Lemma 3.1, if $k = \pi_{g,h}(f)$ divides n, then f divides $g^n - h^m$ for some $m \geq 0$. Now assume by way of contradiction that $\pi_{g,h}(f^P)$ divides n for each power $P \geq 1$ of p. Let $h^m = h_0^{m_0}$, where h_0 is a divisor of h which is not a pth power and analogously let $g^n = g_0^{n_0}$, where g_0 divides g and is not a pth power. Then $\pi_{g_0,h_0}(f^P)$ divides n_0 for each power $P \geq 1$ of p, and therefore the assumption of the proposition is satisfied for the (g_0, h_0)-system, f and $n_0 \geq 1$. From now on, we assume that g and h are not pth powers and shall derive a contradiction.

For a power $P \geq 1$ of p, let $m(P)$ be the unique nonnegative integer bounded by the multiplicative order of h modulo f^P such that $g^n - h^{m(P)}$ is divisible by f^P. Let $r = r(P)$ be the largest power of p dividing $\gcd(n, m(P))$ and write $N := N(P) = n/r$, $M(P) := m(P)/r$. Observe that r is bounded since n is fixed. Moreover, N or $M(P)$ is not divisible by p. We assume that r divides P and let $Q := P/r$. Then f^Q divides $g^N - h^{M(P)}$ as well as $g^{nQ} - h^{m(1)Q}$. Consequently, letting for simplicity $M = M(P)$ and $m = m(1)$, f^Q divides

$$A = A(P) := -(g^N - h^M)g^{nQ-N} + g^{nQ} - h^{mQ} = h^M g^{nQ-N} - h^{mQ}.$$

If $a \in F[x]$ is such that $A = af^Q$ and Q is larger than 1, then the formal derivative A' of A is equal to

$$A' = a'f^Q = h^{M-1}g^{nQ-N-1}(Mh'g - Ng'h).$$

If $B(P) := Mh'g - Ng'h \neq 0$ then $A' \neq 0$, whence the relative primeness of f and gh implies that f^Q divides $B(P)$. Since the degree of $B(P)$ is bounded for all P, this gives a contradiction for sufficiently large P (and Q). Thus, $B(P) = 0$ for large P, which we now assume. If $M \equiv 0 \bmod p$ then p does not divide N and therefore $g'h = 0$, whence $g' = 0$. This is a contradiction to the assumptions that $\deg(g) \geq 1$ and that g is not a pth power. Similarly, if $N \equiv 0 \bmod p$, then p does not divide M and therefore $h'g = 0$, whence $h' = 0$. Again, this is a contradiction. We deduce that p does not divide NM and therefore $h'g = \gamma g'h$ for some nonzero $\gamma \in F$. But this cannot happen, as g and h are assumed to be relatively prime and neither g' nor h' is zero. This completes the proof of Proposition 5.1. □

We now resume the discussion of the (g, h)-system described at the beginning of the section. Assume from now on that $f \in \mathcal{P}_{g,h}(n)$ for a given $n \geq 1$

(we know the existence of f when n is indivisible by p). An application of Proposition 5.1 shows that there exists an integer $j \geq 1$ such that $\pi_{g,h}(f^{p^j})$ does not divide n. In fact, $\pi_{g,h}(f^{p^j}) = np^l$ for some $l \geq 1$. Now let $\kappa(f)$ be the *p-index of* f, i.e., the least integer $k \geq 1$ such that np divides $\pi_{g,h}(f^{p^k})$. Then it is clear that $f_1 := f^{\kappa(f)} \in \mathcal{P}_{g,h}(np)$. If, by induction, $f_i \in \mathcal{P}_{g,h}(np^i)$ for some $i \geq 1$, then $f_{i+1} := f_i^{\kappa(f_i)} \in \mathcal{P}_{g,h}(np^{i+1})$. This finally completes the proof of Theorem 1.1, since $\mathcal{P}_{g,h}(n)$ is known to be nonempty (in fact infinite) if p does not divide n.

Nevertheless for h not a pth power, we give a final result representing a more precise version of the above. There is also a small restriction of f, namely that its degree be at least that of h.

Theorem 5.2 *Let g and h be monic non-constant polynomials over F which are relatively prime. Assume that h is not a pth power. Assume further that, for a given n, $f \in \mathcal{P}_{g,h}(n)$ and $\deg(f) \geq \deg(h)$. Let $\kappa := \kappa(f)$ be the p-index of f. Then*

$$\pi_{g,h}(f^{p^{\kappa+l}}) = np^{l+1} \text{ for all } l \geq 0. \tag{5.1}$$

Proof. The condition on h means that h' is non-zero. By the definition of κ, (5.1) is valid for $l = 0$. Assume by induction that the assertion holds for all $j \leq l$ and some $l \geq 0$. Assume further that, for some $c \in F[x]$ and some $m \geq 0$,

$$cf^{p^{\kappa+l+1}} = g^{np^{l+1}} - h^m.$$

Differentiating, we obtain that $f^{p^{\kappa+l}}$ divides $mh^{m-1}h'$. Using the facts that f and h are relatively prime and $\deg(f) \geq \deg(h)$, we deduce that m is divisible by p. Thus, $f^{p^{\kappa+l}}$ divides $g^{np^l} - h^{m/p}$, a contradiction to $\pi_{g,h}(f^{\kappa+l}) = np^{l+1}$. This completes the proof. □

References

[BM1] *A. Batra* and *P. Morton*, Algebraic dynamics of polynomial maps on the algebraic closure of a finite field, I, Rocky Mountain J. Math. **24** (1994), 453-481.

[BM2] *A. Batra* and *P. Morton*, Algebraic dynamics of polynomial maps on the algebraic closure of a finite field, II, Rocky Mountain J. Math. **24** (1994), 905-932.

[C] *L. Carlitz*, Sets of primitive roots, Compos. Math. **13** (1956), 65-70.

[CC] *W. S. Chou* and *S. D. Cohen*, The dynamics of linearized and sublinearized polynomials on finite fields, Preprint 97/47, University of Glasgow (1997).

[Co] *S. D. Cohen*, Primitive roots and powers among values of polynomials over finite fields, J. reine angew. Math. **350** (1984), 137-151.

[CH] *S. D. Cohen* and *D. Hachenberger*, The dynamics of linearized polynomials, Preprint 97/21, University of Glasgow (1997).

[H1] *D. Hachenberger*, "Finite Fields: Normal Bases and Completely Free Elements", Kluwer Academic Publishers, Boston, 1997.

[H2] *D. Hachenberger*, Finite fields: algebraic closure and module structures, Forschungsbericht, Deutsche Forschungsgemeinschaft (1997).

[L] *W. C. W. Li*, "Number Theory with Applications", World Scientific, 1996.

[LN] *R. Lidl* and *H. Niederreiter*, "Finite Fields", Addison-Wesley, Reading, Massachusetts, 1983.

[M] *P. Morton*, Periods of maps on irreducible polynomials over finite fields, Finite Fields and Their Applications **3** (1997), 11-24.

[O] *O. Ore*, Contributions to the theory of finite fields, Trans. Amer. Math. Soc. **36** (1934), 243-274.

[V] *F. Vivaldi*, Dynamics over irreducible polynomials, Nonlinearity **5** (1992), 941-960.

Contemporary Mathematics
Volume **225**, 1999

ON DEGREE BOUNDS FOR INVARIANT RINGS OF FINITE GROUPS OVER FINITE FIELDS

PETER FLEISCHMANN AND WOLFGANG LEMPKEN

ABSTRACT. Let G be a finite group acting on $A := \mathbb{F}[X_1, \ldots, X_n]$ by algebra automorphisms. If $\mathbb{F}$ is a field of characteristic zero, then, due to classical results of Emmy Noether one knows that the invariant ring A^G can be generated in degrees less or equal to $|G|$. If $\mathbb{F}$ an arbitrary commutative ring (e.g. a finite field), the situation is much less satisfying. In this paper we give an outline on known results (with some new proofs) on degree bounds for arbitrary rings and arbitary finite groups. It turns out that for the finite field $\mathbb{F}_q$ with $q = p^s$, A^G can be constructed explicitly from A^P, if P is a Sylow - p group of G. We also present some new results on the range of finite fields over which Noether's bound holds for subgroups of classical groups.

1. INTRODUCTION

Let R be a commutative ring, A a finitely generated (unitary) commutative R -algebra and G a group acting on A as R - algebra automorphisms. Then the **invariant ring** A^G is defined to be the R - algebra of fixed points

$$A^G := \{a \in A \mid g(a) = a\}.$$

For example R can be the field of complex numbers and A the polynomial ring $\mathbb{C}[X_1, \ldots, X_n]$ where the G - action on A is derived from a linear action on the space $V := \langle X_1, \ldots, X_n \rangle_{\mathbb{C}}$ of homogeneous polynomials with degree one. This situation had been considered by Hilbert in his famous address on occasion of the first International Congress of Mathematics 1900 in Paris. There he posed the problem to prove or disprove that $\mathbb{C}[V]^G$ is finitely generated for arbitrary G. Today this is known as **Hilbert's** 14^{th} **problem**. By that time a positive answer was already known for $G = SL_2$ by explicit work of Gordan on binary forms and for GL_n by Hilbert himself, as an important application of his famous 'basis theorem'. These results could later be extended by Hermann Weyl who proved finite generation for the invariant rings of what are known today as 'linearly reductive' groups, i.e. groups G whose category of finite - dimensional $\mathbb{C}G$ - modules is semisimple.

1991 *Mathematics Subject Classification.* Primary 20C20.

© 1999 American Mathematical Society

In general the answer to Hilbert's 14^{th} problem is **'no'**: In (1958) a counterexample consisting of a group $G \cong (\mathbb{C}^+)^m$ was given by Nagata. This cannot occur if G is a finite group because of the following fundamental result of Emmy Noether

Theorem 1.1. (Emmy Noether, 1926 [9]) If G is a finite group, R a Noetherian ring and A a finitely generated R - algebra, then A^G is finitely generated.

Noether's proof of this result uses the fact that A is integral over the subalgebra $B \leq A^G$, generated by the coefficients of all the polynomials

$$f_i(T) := \prod_{g \in G} (T - g(a_i)) \in A^G[T],$$

where the a_i are chosen such that $A = R[a_1, \ldots, a_n]$ and G acts on $\sum_{i=1}^n Ra_i$. By Hilbert's basis theorem B is a Noetherian ring and by finite integrality, A is a Noetherian B - module, containing A^G as a submodule. Since submodules of finitely generated modules over a Noetherian ring are again finitely generated, A^G is a finitely generated B - module and, a fortiori, finitely generated as an A - algebra.
Notice that, although we can easily describe a finite set of algebra generators for B, the above argument does not indicate any constructive method of choosing the 'missing' module generators for A^G over B.

Throughout the paper $\mathbf{N}_0$ denotes the set of nonnegative integers; for $n \in \mathbf{N}$, $\underline{n}$ denotes the set $\{1, 2, \cdots, n\}$ and $\mathbf{N}_0^{\underline{n}}$ denotes the set of functions from $\underline{n}$ to $\mathbf{N}_0$.

Definition 1.2. Let R, A and G be as above and let $RG - mod$ denote the category of finitely generated RG - modules which are free over R. With R^* we denote the group of units of R. For $n \in \mathbf{N}$, $a_1, \ldots, a_n \in A$ and $\alpha \in \mathbf{N}_0^{\underline{n}}$ we denote with $\underline{a}^\alpha$ the element $a_1^{\alpha_1} a_2^{\alpha_2} \ldots a_n^{\alpha_n} \in A$ and with $\mathcal{M}_k(\underline{(a_i)})$ the R - span $\langle \underline{a}^\alpha \mid |\alpha| := \sum_{i=1}^n \alpha_i \leq k \rangle$.
Suppose that $A = R[a_i, i = 1, \ldots, n]$ for some $n \in \mathbf{N}$ such that G acts linearly on $\sum_{i=1}^n Ra_i$.
We define the **degree bound** $\beta(A^G, (a_1, \ldots, a_n))$ to be the infimum of the set of all $k \in \mathbf{N}$ satisfying $A^G = R[b_1, \ldots, b_m]$ with $\{b_1, \ldots, b_m\} \subseteq \mathcal{M}_k(\underline{(a_i)})$. Notice that $\beta(A^G, (a_1, \ldots, a_n)) \in \mathbb{Z} \cup \{\infty\}$.
If $A = R[X_1, \ldots, X_n]$ is a polynomial ring with R - linear action of G on $V := \oplus_{i=1}^n RX_i$ then we also write $A = R[V]$ and call $\beta(R[V]^G) := \beta(R[V], (X_1, \ldots, X_n))$ a **local degree bound** of the pair (G, V). The supremum

$$\beta_R(G) := \sup\{\beta(R[V]^G) \mid V \in RG - mod\} \in \mathbb{Z} \cup \infty$$

will be called the **global (linear) degree bound** of the pair (R, G).

Remark 1.3. (i) Suppose that G is finite and $A = R[a_1, \ldots, a_n]$ as above. Extending $\{a_i\}$, if necessary, we can assume that G permutes this set of generators. Consider $W := \oplus_{i=1}^n RX_i$ as a G - permutation module where G permutes the X_i in the same way as the a_i. Then the epimorphism $c : R[W] \to A$, $X_i \mapsto a_i$ is G - equivariant, i.e. c commutes with the G - actions on $R[W]$ and A. If $|G|$ is invertible in R, then the restriction $c_| : R[W]^G \to A^G$ is easily seen to be surjective as well, since

$f = c(h) \in A^G$ with $h \in R[W]$ implies that

$$f = |G|^{-1} \sum_{g \in G} gf = c(|G|^{-1} \sum_{g \in G} gh) \in c(R[W]^G).$$

We see that $\beta(A^G, (a_1, \ldots, a_n)) \leq \beta(R[W]^G)$ (notice that the 'additional a_i's ' can be linearly expressed in the 'original' ones). The argument above shows

$$\beta_R(A^G, (a_1, \ldots, a_n)) \leq \beta_R(G),$$

whenever $|G| \in R^*$. It also shows that if $|G|$ is invertible, a 'global' degree bound **for permutation modules** is a global degree bound for invariant rings of arbitrary modules.
(ii) By 1.1, $\beta := \beta(A^G, (a_1, \ldots, a_n)) < \infty$ if R is Noetherian, but the proof does not give any bound for β.

The significance of degree bounds for constructive invariant theory has the following reason:
Let $G := \langle g_1, \ldots, g_m \rangle$ with generators g_i and $A := R[V] = R[X_1, \ldots, X_n]$. If $\beta(A^G)$ is a known finite number, then the following 'linear algebra' - procedure leads to a system of algebra generators of A^G:

Procedure 1.4. (Constructing algebra generators of $R[V]^G$)

(1) For $i = 1, 2, \ldots, \beta := \beta(R[V]^G)$ do
(2) find all homogeneous $f \in R[V]$ of degree i with $g_\ell(f) = f$ for all $\ell = 1, \ldots, m$;
(3) od;

Denoting the i - th homogeneous component of $R[V]$ by $R[V]_i$ we have

$$R[V]_i = \oplus_{\alpha \in \mathbb{N}^n, |\alpha| = i} \underline{X}^\alpha$$

for $i \in \mathbf{N}$; hence step (2) consists of the solution of the following system of linear equations over R:

$$\Sigma_{\alpha \in \mathbb{N}^n, |\alpha| = i} \, c_\alpha (g_\ell(\underline{X}^\alpha) - \underline{X}^\alpha) = 0, \ \ell = 1, \ldots, m$$

of format $m \times \begin{pmatrix} n+i-1 \\ i \end{pmatrix} \times \begin{pmatrix} n+i-1 \\ i \end{pmatrix}$. If $R = \mathbb{F}$ is a field, the complexity of this procedure will be $\mathcal{O}(m \cdot n^{3\beta})$ in elementary $\mathbb{F}$ - operations.

In 1916 Emmy Noether had already given two constructive proofs for the fact that for a finite group and a field $\mathbb{F}$ of characteristic zero, $\beta_{\mathbb{F}}(G) \leq |G|$. This is usually referred to as 'Noether's bound'. Unfortunately, both of these proofs fail in positive characteristics. In fact both proofs have two different steps where the characteristic of $\mathbb{F}$ comes into play: in one of these steps one needs that $|G|$ is invertible in $\mathbb{F}$ whereas in the other step one even needs that $|G|!$ is invertible in $\mathbb{F}$.
As we see soon Noether's bound does not hold in general if $|G|$ is not invertible in R. If $|G|$ is invertible in R, Noether's bound holds for solvable groups. This has been

proved by L. Smith in 1995 for the case that R is a field [12] and by D. Richman in 1990 for arbitrary R with $|G| \in R^*$ (see [10] which appeared posthumously).

In [5] a constructive proof has been given for

$$\beta(R[V]^G) \leq max\{|G|,\ rank_R(V)(|G|-1)\}$$

whenever there is a subgroup $H \leq G$ such that the index $|G:H|$ is invertible in R and the restriction $V_{|H}$ is a permutation module (i.e. H permutes an R - basis of V.) In [4] a degree bound has been given for so called 'vector invariants' of symmetric groups over arbitrary commutative rings. Each of these results give as a corollary the degree bound

$$\beta(R[V]^G) \leq max\{|G|,\ rank_R(V)(|G|-1)\} \quad (*)$$

for finite groups having a group order $|G|$ which is invertible in the ring R. Recently A. Broer proved the bound (*) to hold if R is field and $R[V]^G$ is a Cohen-Macaulay ring [2].
In case V is a permutation module of rank n over an arbitrary commutative ring R, M. Goebel ([6]) proved

$$\beta(R[V]^G) \leq \frac{n(n-1}{2}.$$

Moreover, a result of Richman ([11]) shows that $\beta_F(G) = \infty$ whenever the characteristic of the field F divides the order of G.

In this paper we use the result of [4] to extend the idea of Emmy Noether's first proof in [8] to arbitrary rings and in particular finite fields. In general this will not give a degree bound as good as Noether's bound for arbitrary finite groups with invertible order; but for special groups we will either obtain Noether's bound globally or at least significantly extend the range of rings where Noether's bound holds. In any case the proofs will be constructive, which means that they will provide a method to find a generating system of invariants within the given bound.

2. Constructing generators

From now on all groups considered will be assumed to be finite!

Let $R[X(n,k)]$ be the polynomial ring $R[X_{11},...,X_{n1},...,X_{1k},...,X_{nk}]$ in $n \times k$ variables and define the action of Σ_n on $R[X(n,k)]$ by extending the permutation action $\sigma(X_{ij}) := X_{\sigma(i)j}$ on $X(n,k) := \sum_{ij}^{\oplus} RX_{ij}$. Let $\underline{Y} := (Y_1,\ldots,Y_k)$ be a 'vector of variables'; then the multivariate polynomial

$$G(\underline{X}_1,\ldots,\underline{X}_n;\underline{Y}) := \prod_{i=1}^{n}(1+\sum_{j=1}^{k} X_{i,j}Y_j) \in R[X(n,k)]^{\Sigma_n}[Y_1,\ldots,Y_k]$$

is called **Galois - resolvent**. In the famous book 'Classical groups' of Hermann Weyl [14] one can find a proof of the following

Theorem 2.1. (Weyl) If $\mathbf{Q} \subseteq R$ then $R[X(n,k)]^{\Sigma_n}$ is generated by the coefficients of the Galois - resolvent $G(\underline{X}_1, \ldots, \underline{X}_n; \underline{Y})$. All of these have total degree $\leq n$, so $\beta(R(n,k)^{\Sigma_n}) \leq n$.

The analogue of Weyl's theorem is false if $R = \mathbf{Z}$ or a field of characteristic $p \leq n$. Already in the smallest nontrivial case $n = 2$ and $R = \mathbb{F}_2$ it is an easy exercise to show that the invariant $X_{11}X_{12}\ldots X_{1k} + X_{21}X_{22}\ldots X_{2k}$ is indecomposable, i.e. cannot be written as a sum of products of invariants with degrees less than k. Hence $\beta(\mathbb{F}_2(X(2,k)))^{\Sigma_2} \geq k$ and $\beta_{\mathbb{F}_2}(\Sigma_2) \geq \lim_{k\to\infty} k = \infty$. In particular, this shows that Noether's bound does not hold in the case of finite fields in general.
In [10] it was proved by D. Richman, that the analogue of Weyl's theorem holds if $n!$ is invertible in R. For arbitrary R the following has been shown in [4]

Theorem 2.2. $\beta(R[X(n,k)]^{\Sigma_n}) \leq max\{n, k \cdot (n-1)\}$. with equality if $n = p^s$ and *char* $R = p$.

Now let $H \leq G$ with $n := |G : H|$ and $G/H := \{H := g_1H, g_2G, \ldots, g_nH\}$ the set of H cosets in G. Consider the Cayley - homomorphism $c : G \to \Sigma_n, g \mapsto (g_iH \mapsto g_jH := gg_iH)$. Suppose that $A := R[a_1, \ldots, a_m]$ with $G(\sum_{i=1}^m Ra_i) \subseteq \sum_{i=1}^m Ra_i$ and $A^H = R[b_1, \ldots, b_k]$ with $b_i \in \mathcal{M}_b(\underline{(a_i)})$. Then

$$\nu : R[X(n,k)] \to A, X_{i\ell} \mapsto g_i(b_\ell)$$

is a G - equivariant R - algebra morphism. In fact, it does not depend on the choice of the g_i and

$$\nu(g(X_{i\ell})) = \nu(X_{j\ell}) = g_j(b_\ell) = gg_ih(b_\ell) = gg_i(b_\ell) = g\nu(X_{i\ell}),$$

because $gg_i = g_jh^{-1}$ for a suitable $h \in H$. The map ν (for $H = 1$) had been used in Noether's original 1916 - proof. We can use her original argument to show that that the restriction

$$\nu_| : R[X(n,k)]^{\Sigma_n} \to A^G$$

is surjective, whenever n is invertible in R: In this case, for any $f = f(b_1, \ldots, b_k) \in A^G \leq A^H$ we can define

$F := \frac{1}{n}(f(X_{11}, X_{12}, \ldots, X_{1k}) + \cdots + f(X_{n1}, X_{n2}, \ldots, X_{nk})) \in R[X(n,k)]^{\Sigma_n}$ and get

$$\nu(F) = \frac{1}{n}(f(g_1(b_1), g_1(b_2), \ldots, g_1(b_k)) + \cdots + f(g_n(b_1), g_n(b_2), \ldots, g_n(b_k))$$

$= \frac{1}{n}(g_1f(b_1, b_2, \ldots, b_k) + \cdots + g_nf(b_1, b_2, \ldots, b_k)) = f$. Let $\beta(n,k) := \beta(R[X(n,k)]^{\Sigma_n})$ then $R[X(n,k)^{\Sigma_n}] = R[F_1, \ldots, F_s]$ with $F_i \in \mathcal{M}_{\beta(n,k)}(\underline{(X_{ij})})^{\Sigma_n}$ and hence $A^G = R[\nu(F_1), \ldots, \nu(F_s)]$ with $\nu(F_i) \in \mathcal{M}_{\beta(n,k)}(\underline{(g_i(b_j))})^G \leq \mathcal{M}_{\beta(n,k)b}(\underline{(a_i)})^G$. So $|G : H| \in R^*$ implies

$$\beta(A^G) \leq \beta(n,k)\beta(A^H).$$

On the other hand, since $c(G) = G/\cap_{g\in G}^g H \leq \Sigma_n$, we have $R[X(n,k)]^{\Sigma_n} \subseteq R[X(n,k)]^{c(G)}$, hence

$$\beta(A^G) \leq \beta(R[X(n,k)]^{c(G)}\beta(A^H).$$

Together with 2.1 (or [10]) and 2.2 we get:

Theorem 2.3. Let A be an R - algebra as above and $H \leq G$ with $|G : H|$ invertible in R and $A^H = R[b_1, \ldots, b_k]$ with $b_i \in A^H \cap \mathcal{M}_b(\underline{(a_i)})$. Then

$$\beta(A^G, (a_1, \ldots, a_m)) \leq max\{|G : H|, k \cdot (|G : H| - 1)\}\beta(A^H, (a_1, \ldots, a_m)), \text{ and}$$
$$\beta(A^G, (a_1, \ldots, a_m)) \leq \beta_R(c(G))\beta(A^H, (a_1, \ldots, a_m)), \text{ and.}$$

In particular, if A^H is finitely generated then so is A^G. If moreover $|G : H|!$ is invertible in R, then

$$\beta(A^G, (a_1, \ldots, a_m)) \leq |G : H|\beta(A^H, (b_1, \ldots, b_\ell)).$$

In the case $H = 1$ and $|G|$ invertible we recover the bound (*) above and if $|G|!$ is invertible, we get Noether's bound.
If $R = \mathbb{F}_q$ is the finite field of order $q = p^s$, then we can take $H = P$, a Sylow - p group of G. Since the index $|G : P|$ is invertible in $\mathbb{F}$, we can apply 2.3 and construct $\mathbb{F}[V]^G$ from $\mathbb{F}[V]^P$ via vector invariants. So in modular invariant theory the most serious problem is to construct invariant rings of p - groups in characteristic $p > 0$. For this task there are algorithms available due to Gregor Kemper (see [7]).

By an obvious induction we get from 2.3:

Corollary 2.4. Let $G = H_0 > H_1 > H_2 > \cdots > H_m$ with $|G|$ and $(|H_{i-1} : H_i|)! \in R^*$ for $i = 1, \ldots, m$. Then

$$\beta_R(G) \leq \beta_R(H_m) \cdot |G : H_m|.$$

Recall that a subgroup $G \leq \Sigma_n$ is called k - **fold transitive** (for $1 \leq k \leq n$), if the induced action $g(\alpha) = g \circ \alpha$ of G on the set $Inj(\underline{n}^{\underline{k}})$ of injective maps $\underline{k} \to \underline{n}$ is transitive. If $G \leq \Sigma_n$ is k - fold transitive, then the stabilizer $G_{i_1,i_2,\ldots,i_\ell} \leq \Sigma_{\underline{n}\setminus i_1,i_2,\ldots,i_\ell}$ of any $\ell \leq k$ ciphers is $k - \ell$ - fold transitive. Consider the chain of subgroups

$$G > G_{i_1} > G_{i_1,i_2} > \cdots > G_{i_1,i_2,\ldots,i_\ell}$$

then $n,\ n-1,\ \ldots,\ n-\ell+1$ is the corresponding sequence of indices and we get from 2.4:

Corollary 2.5. Let $G \leq \Sigma_n$ be k - fold transitive and $n! \in R^*$ then for any $\ell \leq k$ ciphers of $\underline{n}$:

$$\beta_R(G) \leq \beta_R(G_{i_1,i_2,\ldots,i_\ell}) \cdot \frac{n!}{(n-k)!} = \beta_R(G_{i_1,i_2,\ldots,i_\ell}) \cdot |G : G_{i_1,i_2,\ldots,i_\ell}|.$$

From the well known theorem of symmetric polynomials one knows that the local degree bound $\beta(R[V]^{\Sigma_n}) \leq n$ holds for the 'natural permutation module' $V \in R\Sigma_n - mod$; ($R[V]^{\Sigma_n}$ is generated by the elementary symmetric polynomials). Since $n < n!$ (for $n > 2$) this is much better than Noether's bound. But using 2.5 we obtain Noether's bound globally for the symmetric and alternating groups whenever the group order is invertible in R.

Corollary 2.6. Let $G \in \{\Sigma_n, Alt_n\}$ and $|G| \in R^*$ then $\beta_R(G) \leq |G|$.

Proof: The groups Σ_n and Alt_n are n - fold and $n-2$ - fold transitive on $\underline{n}$ respectively, with trivial n and $n-2$ - fold stabilisers. Now the claim follows immediately from 2.5.

3. Normal subgroups and Factor groups

Theorem 3.1. Let $N \lhd G$, $|G/N|$ invertible in R. Then

$$\beta_R(A^G, (a_1, \ldots, a_n)) \leq \beta_R(A^N, (a_1, \ldots, a_n)) \cdot \beta_R(G/N).$$

Proof: If $N \lhd G$, then the image $c(G)$ of the Cayley homomorphism is isomorphic to G/N and the result follows immediately from 2.3. ∘

If $|G|$ is invertible in R and we know a global degree bound for any composition factor of G, then 3.1 yields a global degree bound for G. Thus a proof of the Noether bound (for invertible $|G|$) is in principle reduced to simple groups. For the simple groups of a prime order which is invertible in R, the Noether bound holds due to a result of Richman:

Theorem 3.2. (Richman,[10]) Let $A = R[a_1, \ldots, a_n]$ with $G(\sum_{i=1}^n Ra_i) \subseteq \sum_{i=1}^n Ra_i$. Assume that $|G|$ is a prime and is invertible in R. Then A^G is generated as an R - algebra by

$$\{\sum_{g \in G} g(\underline{a}^\gamma) \mid \gamma \in \mathbf{N}_0^k,\ |\gamma| \leq |G|\}.$$

The following theorem can be viewed as a further motivation to prove Noether's bound in general for groups with invertible order:

Theorem 3.3. Let $\mathcal{K} := \{\mathbb{Z}/n\mathbb{Z}, Alt_n \mid n \in \mathbb{N}\}$ be the class consisting of cyclic and alternating groups. If G is a finite group with all composition factors isomorphic to an element of $\mathcal{K}$ and assume that $|G|$ is invertible in R. Then $\beta(A^G, (a_1, \ldots, a_n)) \leq |G|$; in particular

$$\beta_R(G) \leq |G|.$$

Proof: By 3.1, 2.6 and 3.2 a minimal counterexample cannot exist. ∘

Remark 3.4. We have been informed that this result has also been obtained by Mingchang Kang, but we do not have any further details.

As a corollary we get:

Corollary 3.5. (D. Richman ([10]) , L. Smith ([12])) If G is solvable and $|G| \in R^*$, then $\beta_R(G) \leq |G|$.

Examples 3.6. i) The simple Mathieu group M_{11} has order $2^4 \cdot 3^2 \cdot 5 \cdot 11$ and contains a maximal subgroup $H \cong M_{10} := A_6.2$ of index 11. If we define $\tilde{\mathcal{K}} := \mathcal{K} \cup \{M_{11}\}$, then similar to 3.3 one can prove Noether's bound for all groups with composition factors in $\tilde{\mathcal{K}}$, as long as R is a field of characterisic $p \neq 7$ and not dividing $|G|$.

ii) As another example consider $G = SL_2(7)$, which has order $6 \cdot 7 \cdot 8 = 336$. From 2.3 we know that Noether's bound holds for G over any field of characteristic $p > 336$. But for classical groups like G we can do much better. In fact we will see that in case of $SL_2(7)$ Noether's bound already holds for $p > 7$.

So let us now consider the finite Chevalley groups of classical type $G(q)$, which are defined over finite fields $\mathbb{F}_q$. For details on these groups refer to [3]

The orders of these groups are given by polynomials in q of the following form

$$|G(q)| = |B(q)| \prod_{i=1}^{\ell} \frac{q^{d_i} - 1}{q - 1}$$

with $2 \leq d_1 \leq d_2 \leq \cdots \leq d_\ell \in \mathbf{N}$. The numbers $d_i - 1$ are the degrees of the fundamental invariants in the 'reflection representation' of the 'Weyl group' associated with $G(q)$, ℓ is the so called 'semisimple rank' of $G(q)$ and $B(q) \leq G(q)$ is the 'Borel subgroup' which is solvable. Let $d(G(q)) := max\{d_i \mid i = 1, \ldots, \ell\}$.
Then $d((G(q)) = \ell$ for quasisimple $G(q)$ of Dynkin type $A_{\ell-1}$, e.g. $GL_\ell(q), SL_\ell(q)$ or $PGL_\ell(q)$; $d((G(q)) = 2\ell$ for quasisimple $G(q)$ of Dynkin type B_ℓ, e.g. $Sp_{2\ell}(q)$ or $SO_{2\ell+1}(q)$ and $d((G(q)) = 2(\ell - 1)$ for quasisimple $G(q)$ of Dynkin type D_ℓ, e.g. $SO^{\pm}_{2\ell}(q)$.

Theorem 3.7. Suppose that $(\frac{q^{d(G(q))}-1}{q-1})!$ is invertible in R (e.g. R is a field of characteristic $p > \frac{q^{d(G(q))}-1}{q-1}$), then Noether's bound $\beta_R(G) \leq |G|$ holds for every $G \leq G(q)$.

Proof: From the order formulae for $|G(q)|$ we see immediately that all prime divisors of $|G(q)|$ are less or equal to $\frac{q^{d(G(q))}-1}{q-1}$, so $|G(q)|$ is invertible in R. Let $(G, G(q))$ be a counterexample with $|G| + |G(q)|$ minimal. Then we can assume that $G(q)$ is quasisimple:
Indeed otherwise $G(q) = G_1(q) * G_2(q)$ with $|G_i(q)| < |G(q)|$ and $d(G_i(q)) \leq d(G(q))$. Consider the short exact sequence $1 \to G \cap G_2(q) \to G \to H \to 1$ with $H \cong GG_2(q)/G_2(q) \leq G_1(q)/Z$ and Z a central subgroup of $G_1(q)$. Since $G_1(q)/Z$ is a again a Chevalley group of classical type, the induction hypotheses together with 3.1 yield a contradiction.
It is well known, that $G(q)$ contains a maximal parabolic subgroup $P(q)$ which can be written as a semidirect product $UL(q)$, where $U := O_r(P(q))$ with $q = r^s$, r a prime and $L(q) < G(q)$ a Chevalley group of classical type. Moreover $P(q)$ can be chosen such that $|G(q) : P(q)|$ divides $\frac{q^{d(G(q))}-1}{q-1}$ and $d(L(q)) \leq d(G(q))$. Since $|G : G \cap P(q)|$ divides $|G(q) : P(q)|$, its factorial is in R^* and we get from 2.4:

$$\beta_R(G) \leq |G : G \cap P(q)| \beta_R(G \cap P(q)). \quad (*)$$

Now $G \cap U \triangleleft G \cap P(q)$ and $G \cap P(q)/G \cap U \leq P(q)/U \cong L(q)$. Since $G \cap U$ is solvable we get $\beta_R(G \cap P(q)) \leq |G \cap U| \cdot |G \cap P(q)/G \cap U| = |G \cap P(q)|$. Together with $(*)$ this gives the final contradiction. $\circ$

Corollary 3.8. If $n > 1$ and $\mathbb{F}$ is a field of characteristic $p > \frac{q^n-1}{q-1}$, then

$$\beta_{\mathbb{F}}(G) \leq |G|$$

for each $G \leq GL_n(q)$.

References

[1] D. Benson, *Representations and cohomology I*, Cambridge Univ. Press 1991.

[2] A. Broer, *Remarks on Invariant Theory of Finite Groups*, preprint, Université de Montréal, 1997.

[3] R.W.Carter *Finite Groups of Lie Type*, J.Wiley and Sons, (1985)

[4] P. Fleischmann, *A new degree bound for Vector Invariants of Symmetric Groups*, Trans. Amer. Math. Soc. **350** (1998), 1703-1712.

[5] P. Fleischmann, W. Lempken, *On generators of modular invariant rings of finite groups*, Bull. London Math. Soc. **29** (1997), 585-591.

[6] M. Goebel, *Computing bases for rings of permutation- invariant polynomials*, J. Symb. Comp. **19** (1995), 285-291.

[7] G. Kemper, *Calculating Invariant Rings of Finite Groups over Arbitrary Fields*, J.Symbolic Computation, **21** (1996), 351–366.

[8] E. Noether, *Der Endlichkeitssatz der Invarianten endlicher Gruppen*, Math. Ann. **77** (1916), 89-92.

[9] E. Noether, *Der Endlichkeitssatz der Invarianten endlicher linearer Gruppen der Charakteristik p*, Nachr. Ges. Wiss. Göttingen (1926), 28-35, in 'Collected Papers', pp.485-492, Springer Verlag, Berlin (1983).

[10] D. Richman, *Explicit generators of the invariants of finite groups*, Adv. Math. **124** (1996), 49-76.

[11] D. Richman, *Invariants of finite groups over fields of charact eristic p*, Adv. Math. **124** (1996), 25-48.

[12] L. Smith, *E. Noether's bound in the invariant theory of finite groups*, Arch. Math. **66** (1995), 89-92.

[13] L. Smith, *Polynomial Invariants of Finite Groups*, A.K. Peters Ltd., (1995).

[14] H. Weyl, *The Classical Groups*, 2^{nd} Edition, Princeton Univ. Press, Princeton (1953).

Institute for Experimental Mathematics, University of Essen, Ellernstr. 29, 45326 Essen, G ermany

E-mail address: peter@exp-math.uni-essen.de

Institute for Experimental Mathematics, University of Essen, Ellernstr. 29, 45326 Essen, Germany

E-mail address: lempken@exp-math.uni-essen.de

This page intentionally left blank

Contemporary Mathematics
Volume **225**, 1999

IRREDUCIBLE POLYNOMIALS OF GIVEN FORMS

SHUHONG GAO, JASON HOWELL, AND DANIEL PANARIO

ABSTRACT. We survey under a unified approach on the number of irreducible polynomials of given forms: $x^n + g(x)$ where the coefficient vector of g comes from an affine algebraic variety over $\mathbb{F}_q$. For instance, all but $2 \log n$ coefficients of $g(x)$ are prefixed. The known results are mostly for large q and little is know when q is small or fixed. We present computer experiments on several classes of polynomials over $\mathbb{F}_2$ and compare our data with the results that hold for large q. We also mention some related applications and problems of (irreducible) polynomials with special forms.

1. THE GENERAL PROBLEM AND KNOWN RESULTS

Let $\mathbb{F}_q$ denote a finite field with q elements and V an affine algebraic variety over $\mathbb{F}_q$, say defined by r polynomials $f_1, \ldots, f_r \in \mathbb{F}_q[x_1, \cdots, x_n]$. Let V_q be the $\mathbb{F}_q$-rational points in V, i.e.

$$V_q = \{(t_1, \cdots, t_n) \in \mathbb{F}_q^n : f_i(t_1, \cdots, t_n) = 0, 1 \leq i \leq r\}. \tag{1}$$

We define $I_n(V_q)$ to be the number of points $(t_1, \cdots, t_n) \in V_q$ such that

$$F(x) = x^n + t_1 x^{n-1} + \cdots + t_{n-1} x + t_n \tag{2}$$

is irreducible in $\mathbb{F}_q[x]$. We also denote by $P(V_q)$ the set of all polynomials in (2) with $(t_1, \cdots, t_n) \in V_q$. For example, when the polynomials $f_1, \ldots, f_r$ are linear in $x_1, \ldots, x_n$, V is a coset of a linear subspace. If the linear subspace has dimension m then V is called a linear variety of dimension m. For a linear variety V of dimension m, $P(V_q)$ can be rewritten as

$$P(V_q) = \{x^n + g_0(x) + a_1 g_1(x) + \cdots + a_m g_m(x) : (a_1, \ldots, a_m) \in \mathbb{F}_q^m\}, \tag{3}$$

where $g_i \in \mathbb{F}_q[x]$ has degree at most $n-1$ for $0 \leq i \leq m$, and $g_1, \ldots, g_m$ are linearly independent over $\mathbb{F}_q$.

Problem 1.1. *Let V be an affine variety over $\mathbb{F}_q$. Determine $I_n(V_q)$.*

When V is a linear variety, we require that not all the constants in $g_0(x)$, $g_1(x), \ldots, g_m(x)$ are zero and that the polynomials $x^n + g_0(x), g_1(x), \ldots, g_m(x)$ are relatively prime; otherwise $I_n(V_q) = 0$ trivially.

When $V_q = \mathbb{F}_q^n$, $I_n(V_q)$ is just the number of monic irreducible polynomials of degree n in $\mathbb{F}_q[x]$ and there is a well–known formula for it. Generally one would not expect to find an explicit formula for $I_n(V_q)$. In practice, it often suffices to have a good lower bound or an asymptotic formula for it. We are most interested in the asymptotic behaviour of $I_n(V_q)$. We note that counting the number of points in V_q

Date: June 16, 1998 (revised).
1991 *Mathematics Subject Classification.* Primary 11T55; Secondary 12Y05.
Key words and phrases. Finite fields, irreducible polynomials, affine algebraic varieties, smooth polynomials.

© 1999 American Mathematical Society

itself is already a difficult problem; the reader is referred to Wan's paper [39] for more information.

When V is a linear affine variety, $I_n(V_q)$ has been studied by several people. Suppose that $a(x) \in \mathbb{F}_q[x]$ has degree $r < n-1$ and $b(x) \in \mathbb{F}_q[x]$ has degree $\leq n-1$. Artin [1] studies $I_n(V_q)$ for $g_0 = b(x)$ and $g_i(x) = a(x)x^{i-1}$ for $1 \leq i \leq n-r$; here $I_n(V_q)$ is the number of monic irreducible polynomials $F(x)$ in $\mathbb{F}_q[x]$ of degree n that are congruent to $b(x)$ modulo $a(x)$. Hayes [23] generalizes Artin's result to the case where $g_0 = b(x)$ and $g_i(x) = a(x)x^{i-1}$, $1 \leq i \leq n-r-s$, where s is fixed with $0 \leq s \leq n-r-1$ (that is, the first s coefficients $t_1, \ldots, t_s$ of $F(x)$ are fixed).

Theorem 1.2 ([1, 23]). *Let $s \geq 0$ and $r \geq 0$ be integers with $m = n-r-s \geq 1$. Let $a(x) \in \mathbb{F}_q[x]$ have degree $r \leq n-1$ and $b(x) \in \mathbb{F}_q[x]$ degree $\leq n-1$. Suppose in (3) $g_0 = b(x)$ and $g_i(x) = a(x)x^{i-1}$, $1 \leq i \leq m$. Then, for large q,*

$$I_n(V_q) = \frac{1}{\kappa(a)} \frac{q^m}{n} + O\left(\frac{q^{nv}}{n}\right) \tag{4}$$

for some $1/2 \leq v < 1$ where $\kappa(a) = \varphi(a)/q^r$ and $\varphi(a)$ is the number of units in $\mathbb{F}_q[x]/(a(x))$.

The estimate (4) is nontrivial only if $m > n/2$. Lower bounds for $\kappa(a)$ are known. By Theorem 2.1 and its proof in [18],

$$1 \geq \kappa(a) \geq \begin{cases} \left(1-\frac{1}{q}\right)^r & \text{if } r \leq q, \\ \left(1-\frac{1}{q}\right) \frac{1}{e^{0.83(1+\log_q r)}} & \text{if } r > q, \end{cases}$$

where r is the degree of $a(x)$. Hence

$$1 \leq \frac{1}{\kappa(a)} \leq \begin{cases} \left(1+\frac{1}{q-1}\right)^r & \text{if } r \leq q, \\ \left(1+\frac{1}{q-1}\right) e^{0.83}(1+\log_q r) & \text{if } r > q. \end{cases}$$

Note that for fixed r, $1/\kappa(a)$ goes to 1 when $q \mapsto \infty$. But for fixed q, $1/\kappa(a)$ can be arbitrarily big when $r \mapsto \infty$. In fact, Theorem 3.4 in [18] shows that there is an infinite sequence of r such that

$$e^{\epsilon}\sqrt{1+\log_q r} \leq \frac{1}{\kappa(x^r-1)} \leq e^{0.83}(1+\log_q r)$$

for some constant ϵ depending only on q.

Theorem 1.2 improves previous work of Uchiyama [42] for $b(x) = x^r$ and Carlitz [8] for $b(x) = x^r$ and $s = r = 1$. By using Theorem 1.2, Hsu [25] proves that there is always an irreducible polynomial of degree n in $\mathbb{F}_q[x]$ with the lower or higher half of the coefficients fixed at any values.

The special polynomial $x^n + x + a$ (i.e. $m = 1$, $g_0 = x$ and $g_1 = 1$ in (3)), has attracted much attention. Chowla [9] conjectures that the number of such irreducibles is asymptotically q/n. Later, Cohen [11] and Ree [32] prove independently that indeed the number is $q/n + O(q^{1/2})$. They both use a function field analog of the Čebotarev density theorem, or Weil's theorem on the Riemann hypothesis for function fields over a finite field [41], and the fact that the Galois group of the polynomial $x^n + x + t$ over the function field $\mathbb{F}_q(t)$ is the symmetric group S_n of order n. The latter fact was previously determined by Birch and Swinnerton-Dyer [3] and a simple proof of it is given by Hayes [24]. In fact, Cohen considers the more general polynomials (3) for $m = 1$ in [11] and for an arbitrary m in [12]. In

other words, Cohen determines $I_n(V_q)$ for a linear affine variety V under certain restrictions.

Theorem 1.3 ([12],Theorem 3). *Let V be a linear affine variety of dimension m over $\mathbb{F}_q$. Under certain conditions on V and for large q,*

$$I_n(V_q) = \frac{q^m}{n} + O(q^{m-\frac{1}{2}}), \tag{5}$$

where the implied constant depends only on n.

The estimate (5) works for all m when q is large, but the error term is worse than (4) when $m > n/2$. We omit the description of the exact conditions on V because they seem complicated and not easy to verify. Also, we believe that some of the conditions can be removed or simplified. Cohen gives simple conditions for two special cases of V:

(a) $g_i = x^{k_i}$, $1 \le i \le m$, with $n > k_1 > k_2 > \cdots > k_m \ge 0$;
(b) $g_0 = b(x)$ and $g_i = a(x)x^{i-1}$ for $1 \le i \le m$ where $m \ge 1$, $a(x) \in \mathbb{F}_q[x]$ has degree $n - m$ and $b(x) \in \mathbb{F}_q[x]$ has degree at most $n - 1$.

Let p be the characteristic of $\mathbb{F}_q$. For these two special cases, Cohen's conditions are: (a) $p > n$, $P(V_q)$ is not a subset of $\mathbb{F}_q[x^\ell]$ for any $\ell > 1$, and $g_0(0) \neq 0$ if $k_m > 0$; (b) $p > n$, and $x^n + b(x)$ and $a(x)$ are relatively prime. These two cases correspond to Theorems 1 and 2 in [12]. Cohen also considers the more general problem of determining the number of polynomials in $P(V_q)$ with a given factorization pattern; the general result is described in the next section.

In case (a) above, Stepanov [37] independently proves a formula for $I_n(V_q)$ by using the deep Deligne-Weil theorem [14]. For an arbitary variety, the problem has been studied by Chatzidakis, van den Dries and Macintyre [10], Wan [38], and Fried, Haran and Jarden [15] in a more general setting.

Theorem 1.4 ([10, 15, 38]). *Let V be an affine variety of dimension m over $\mathbb{F}_q$. Then, for large q, there is a constant $d \ge 0$ such that*

$$I_n(V_q) = d \cdot \frac{q^m}{n} + O(q^{m-\frac{1}{2}}). \tag{6}$$

In the above formula for $I_n(V_q)$, d depends on the variety. Also, if we replace q by q^k then the constant d may vary with k but is periodic. An interesting question is to determine d for special classes of varieties. As Theorem 1.3 indicates, d could be 1. At the end of our paper, we will give an example where $d = n$.

The above accounts essentially all we know about $I_n(V_q)$. These results are proved exclusively for large q. Little is known about $I_n(V_q)$ when q is small (or fixed). In Section 3, we present computer experiments on $I_n(V_q)$ for several special cases of linear varieties V over $\mathbb{F}_q$ for $q = 2$. We compare our data with the asymptotic formulas above that are valid for large q. It turns out these formulas hold very well for small q and the error terms are small as well.

For completeness, we comment in Section 2 on some related results and applications of polynomials of special forms, and describe two interesting related problems that arise in algorithm designs.

2. Related results, applications and problems

Sparse irreducible polynomials (i.e., when most coefficients are fixed at 0) over finite fields have several applications in computer algebra, coding theory and cryptography. In practice, $\mathbb{F}_{2^n}$ are among the most useful fields. Suppose that there is an irreducible polynomial $x^n + g(x) \in \mathbb{F}_2[x]$ with $g(x)$ having a small degree, say $\deg(g) \leq \log n + O(1)$. In [34], Shoup shows that exponentiation in $\mathbb{F}_{2^n}$ can be sped up using this type of polynomial, which is desirable in implementing pseudorandom number generators and several public-key cryptosystems. By exploring the low degree of $g(x)$, Coppersmith [13] designs one of the fastest algorithms for computing discrete logarithms in $\mathbb{F}_{2^n}$. Recently, Gao [16] constructs elements of provable high orders in finite fields by using irreducible factors of $x^n + g(x)$ with $\deg g(x)$ small. Irreducible polynomials with a few nonzero terms are also important in efficient hardware implementation of feedback shift registers and finite field arithmetic ([2, 21, 40]).

When the degree n is a power of 2, there is always an irreducible binomial or trinomial over $\mathbb{F}_q$. For example, when $q \equiv 1 \bmod 4$, if $a \in \mathbb{F}_q$ is a quadratic nonresidue then $x^{2^k} - a$ is irreducible over $\mathbb{F}_q$ for all $k \geq 0$. When $q \equiv 3 \bmod 4$, there is no irreducible binomial of degree 2^k for $k \geq 2$. In this case, we have from [6] the following construction of irreducible trinomials. Suppose that $q = p^m$ where m is odd and $p \equiv 3 \bmod 4$ is a prime. Let $2^v | (p+1)$, $2^{v+1} \nmid (p+1)$. Then $v \geq 2$. Compute $u \in \mathbb{F}_p$ iteratively as follows:

$$\begin{aligned} u_1 &= 0, \\ u_i &= \pm\left(\frac{u_{i-1}+1}{2}\right)^{\frac{p+1}{4}} \pmod p, \quad \text{for } 1 < i < v, \\ u_v &= \pm\left(\frac{u_{v-1}-1}{2}\right)^{\frac{p+1}{4}} \pmod p, \end{aligned}$$

where one can take at each step any of the signs arbitrarily. Let $u = u_v$. Then

$$x^{2^k} - 2ux^{2^{k-1}} - 1$$

is irreducible over $\mathbb{F}_p$, and over $\mathbb{F}_q$ as well, for all $k \geq 1$. Other constructions of more general sparse irreducible polynomials appear in [35, Theorem 1], and [19, Theorem 5.1]. Irreducible trinomials have been extensively studied and tabulated (see [27, Chapter 3], [4, 5, 22, 43, 44]).

The factorization "behaviour" of polynomials of special forms are important in algorithm designs. This is particularly true for index-calculus methods for computing discrete logarithms in $\mathbb{F}_{q^n}$ for small q. Coppersmith's algorithm for computing discrete logarithms in $\mathbb{F}_{2^n}$ has a good running time if polynomials of the form

$$u_1(x)h(x) + u_2(x) \tag{7}$$

behave like random polynomials of the same degree where $h(x) \in \mathbb{F}_2[x]$ is fixed and $u_1(x), u_2(x) \in \mathbb{F}_2[x]$ are chosen at random of certain degrees. Recently Semaev [33] designs another fast algorithm for computing discrete logarithms in $\mathbb{F}_{q^n}$ when q and n satisfy one of the two conditions:

(a) if $r = 2n + 1$ is a prime and $\mathbb{Z}_r^\times = < q, -1 >$;
(b) if $q^n - 1$ has a small primitive prime divisor r, i.e., $r | (q^n - 1)$ but $r \nmid (q^k - 1)$ for $1 \leq k < n$.

The condition (a) is equivalent to the existence of an optimal normal basis in $\mathbb{F}_{q^n}$; see [29, 20]. In case (a), the running time analysis of Semaev's algorithm relies on the assumption that polynomials of the following forms behave like random polynomials:

$$\sum_{k=d-m}^{d} c_k D_k(x), \quad \sum_{k=d-m}^{d} c_k \phi_{i_k}(x) \tag{8}$$

where $c_k \in \mathbb{F}_q$ vary, but $m < d < n$ and $i_k \leq d$ are fixed, D_k are the well–known Dickson polynomials defined by

$$D_0 = 2, \quad D_1 = x, \quad D_k = xD_{k-1} - D_{k-2}, \ k \geq 2,$$

and ϕ_k are defined by

$$\phi_0 = 1, \quad \phi_k = D_k - D_{k-1} + \cdots + (-1)^{k-1} D_1 + (-1)^k, k \geq 1.$$

In case (b), Semaev assumes that polynomials of the following forms behave like random polynomials:

$$\sum_{k=1}^{m} c_k x^{i_k}, \quad \sum_{k=1}^{m} c_k x^{j_k} \tag{9}$$

where $c_k \in \mathbb{F}_q$ vary, and i_k, j_k are related but fixed.

The polynomials in (7), (8) and (9) are special cases of $P(V_q)$ for a linear variety V as in (3). For index-calculus methods, it is important to know how polynomials in $P(V_q)$ are distributed. Particularly, how many polynomials in $P(V_q)$ are smooth? Here "smooth" means that the polynomials have only irreducible factors of degrees up to a given bound. The phrase "behave like random polynomials" above means that the proportion of smooth polynomials among the polynomials of the form (7), (8), or (9) is approximately the same as that among all polynomials in $\mathbb{F}_q[x]$ of the same degree. This raises the question of finding a good lower bound or asymptotic formula for the number of smooth polynomials in $P(V_q)$. Let $V_q \subseteq \mathbb{F}_q^n$ and $r \leq n$. Define $S_r(V_q)$ to be the number of polynomials in $P(V_q)$ that have no irreducible factors of degrees $> r$.

Problem 2.1. *Let V be an affine variety over $\mathbb{F}_q$ and $r \leq n$. Determine $S_r(V_q)$.*

When $V_q = \mathbb{F}_q^n$, $S_r(V_q)$ is well studied. Let $N_q(n,r) = S_r(\mathbb{F}_q^n)$, the number of r-smooth polynomials of degree n over $\mathbb{F}_q$. Odlyzko [30] gives estimates when $q = 2$ that easily generalize to any q (see [26]). Using the saddle point method when $n \to \infty$ and $n^{1/100} \leq r \leq n^{99/100}$, one has

$$N_q(n,r) = q^n \left(\frac{r}{n}\right)^{(1+o(1))\frac{n}{r}}.$$

Car [7] shows that for large values of r, say $r > cn \log\log n / \log n$, the smooth polynomials behave like the well–known number theoretic Dickman function. Later, Soundararajan [36] obtained estimates for the full range of q, r and n. Recently, Panario, Gourdon and Flajolet [31] used an analytic approach to show that the smooth polynomials also behave like the Dickman function for $r > (\log n)^{1/k}$ for k a positive integer constant. Nothing is known about $S_r(V_q)$ when $V_q \neq \mathbb{F}_q^n$.

More precise information on the distribution of polynomials in $P(V_q)$ can be obtained by studying the number of polynomials that have a given factorization pattern. A polynomial of degree n is said to have a factorization pattern $\lambda =$

$1^{a_1}2^{a_2}\dots n^{a_n}$ if it has exactly a_i irreducible factors of degree i for $1 \le i \le n$. The number of polynomials in $P(V_q)$ with factorization pattern λ is denoted by $I_\lambda(V_q)$. This agrees with our previous notation $I_n(V_q)$ when $\lambda = n$.

Problem 2.2. *Let V be an affine variety over $\mathbb{F}_q$ and λ any factorization pattern. Determine $I_\lambda(V_q)$.*

When V is a linear variety, $I_\lambda(V_q)$ has been studied by Cohen. To state his result, for any factorization pattern $\lambda = 1^{a_1}2^{a_2}\dots n^{a_n}$ we define

$$T(\lambda) = \frac{1}{a_1!a_2!\cdots a_n!1^{a_1}2^{a_2}\cdots n^{a_n}}$$

which represents the proportion of permutations with cycle pattern λ in the symmetric group S_n. When q is large, $T(\lambda)$ is also asymptotically the proportion of polynomials with factorization pattern λ among all monic polynomials of degree n in $\mathbb{F}_q[x]$.

Theorem 2.3 ([12],Theorem 3). *Let V be a linear affine variety of dimension m over $\mathbb{F}_q$. Under certain conditions on V and for large q,*

$$I_\lambda(V_q) = \frac{1}{T(\lambda)} \cdot \frac{q^m}{n} + O(q^{m-\frac{1}{2}}), \tag{10}$$

where the implied constant depends only on n.

The exact conditions are not stated here for the same reasons as in Theorem 1.3. Also, the two special cases (a) and (b) for Theorem 1.3 apply to Theorem 2.3 as well. More work need to be done to simplify Cohen's conditions. In the case (a), Stepanov [37] also proves a similar result.

For an arbitary variety V, Problem 2.2 is studied by Chatzidakis, van den Dries and Macintyre [10], and Fried, Haran and Jarden [15] in a more general setting.

Theorem 2.4 ([10, 15]). *Let V be an affine variety of dimension m over $\mathbb{F}_q$ and λ any facterization pattern of a polynomial of degree n. Then there is a constant $d \ge 0$ such that, for large q,*

$$I_\lambda(V_q) = d \cdot \frac{q^m}{n} + O(q^{m-\frac{1}{2}}). \tag{11}$$

It is interesting to determine the constant d for special varieties V. Cohen's result above indicates that for certain linear variety, $d = T(\lambda)$.

When q is small or fixed, little is known about Problem 2.2. It is not even clear what can be proved for fixed q when m and n are large. Probably new methods are needed to attack it. A resolution of Problem 2.2 will shed light on Problem 2.1.

3. Experimental results

In this section we present experimental results on $I_n(V_q)$ when q is small. The following is a list of types of polynomials we consider. All polynomials are over $\mathbb{F}_2$. However, similar experiments can be conducted over any finite field. We seek for the number of irreducible polynomials of the given forms. Let m be a positive integer (in most of our computation we let $m = 2\lceil \log n \rceil$).

(A) $f(x) = x^n + xg(x) + 1$, $\deg g(x) \le m - 1$.
(B) $f(x) = x^n + x^k g(x) + 1$ where $\deg g(x) \le m - 1$ and $1 \le k \le n - m - 1$.
(C) $f(x) = g_0(x) + x^k g(x) + 1$, $g_0(x)$ has degree n and is randomly chosen, where $\deg g(x) \le m - 1$ and $1 \le k \le n - m - 1$.

(D) $f(x) = g_0(x) + a_1 g_1(x) + \cdots + a_m g_m(x)$, where $g_0, g_1, \ldots, g_m \in \mathbb{F}_2[x]$ are randomly chosen and are linearly independent over $\mathbb{F}_2$ with $\deg g_0(x) = n$ and $\deg g_i(x) < n$ for $1 \le i \le m$.

(D.1) $g_0(x) = D_n(x)/x$, $g_i(x) = D_{k-i}(x)/x$, $1 \le i \le m$, where $D_n(x)$ is a Dickson polynomial of order n and $m \le k < n$.

(D.2) $g_0(x) = x^n + 1$, $g_i(x) = x^{k_i}$, $1 \le i \le m$, where $k_1, \ldots, k_m$ are randomly chosen satisfying $n > k_1 > \cdots > k_m > 0$.

(D.1) and (D.2) are polynomials from (8) and (9). In all the cases, V is an affine variety of dimension m over $\mathbb{F}_2$. For a linear variety of dimension m over $\mathbb{F}_q$, Theorem 1.2 indicates that $I_n(V_q) \sim dq^m/n$ for some constant $d \ge 1$ and d can be arbitrarily large. Theorem 1.3 suggests that this constant d is equal to 1 for many linear varieties, and the error term is $O(q^{m-1/2})$ when q is large. For linear varieties, we expect a smaller error term. So we hypothesize that

$$I_n(V_q) = d \cdot \frac{q^m}{n} + O\left(\frac{q^{m/2}}{n}\right)$$

where d is a constant depending on the variety V. It turns out that $d = 1$ or 2 for most of the above types of polynomials. We will also give examples with $d > 2$. To see the size of the constant in $O(\cdot)$, we compute $c > 0$ such that

$$\left| I_n(V_q) - d \cdot \frac{q^m}{n} \right| \le c \cdot \frac{q^{m/2}}{n},$$

i.e.,

$$\left| I_n(V_q) \cdot \frac{n}{q^{m/2}} - d \cdot q^{m/2} \right| \le c.$$

In our tables,

$$\begin{aligned} \textit{density} &= \frac{I_n(V_q) n}{q^m}, \\ c &= \left| I_n(V_q) \cdot \frac{n}{q^{m/2}} - d \cdot q^{m/2} \right| \end{aligned}$$

up to certain accuracy. We computed Case A for n up to 500 and $m = 2\lceil \log n \rceil$. Table 1 contains the values of d, *density* and c for some selected values of n.

In other tables, S stands for *smallest*, L for *largest*, and A for *average*. In Table 2, 3, 5 and 6, for each $1 \le k \le n-m-1$, we compute $I_n(V_q)$ and the corresponding *density* and c, then we find the smallest, largest, and average of them for each of *density* and c. In Table 4, we make 10 random choices for $\{g_0, g_1, \ldots, g_m\}$ for each pair of n and m, and for each choice we compute *density* and c, then find the smallest, largest, and average of them.

In Table 7, compute some classes of polynomials with larger d, using polynomials in Theorem 1.2 with $\kappa(a)$ small. For example when $a = x^2 - x$, $x^4 - x$, $x^8 - x$, or $x^{16} - x$, the corresponding d is expected to be $\frac{1}{\kappa(a)} = 4$, 5.33, 5.22, and 6.47, respectively. This is indeed verified by our computation. These polynomials provide examples for Problem 27 in [28].

We also did an experiment on the existence of irreducible polynomials of the form $x^n + g(x) \in \mathbb{F}_q[x]$ with $\deg g(x) = \log n + O(1)$. For $q = 2$ and $n \le 2000$, it turns out that such irreducibles always exist with $\deg g(x) \le \log n + 3$.

The computation of these tables is time consuming especially when m is large, since one needs to test irreducibility of 2^m polynomials to get a single value of

n	m	d	*density*	c
25	10	2	2.02637	0.84375
50	12	2	2.22168	14.1875
50	13	2	2.12402	11.2253
50	14	2	2.08435	10.7969
50	15	2	2.04620	8.36375
50	16	2	2.04239	10.8516
50	17	2	2.01797	6.50759
50	18	2	1.98898	5.64062
75	14	2	1.88141	15.1797
100	14	2	2.00195	0.2500
125	14	2	1.77002	29.4375
150	16	2	2.03934	10.0703
175	16	2	1.99203	2.03906
200	16	2	2.00195	0.50000
225	16	2	2.00157	0.40234
250	16	2	2.03323	8.50781
275	18	2	1.94387	28.7363
300	18	2	2.02789	14.2812
325	18	2	1.85595	73.7559
350	18	2	1.97067	15.0156
375	18	2	1.96552	17.6523
400	18	2	2.00042	0.21875
425	18	2	2.03466	17.7480
450	18	2	1.99470	2.71093
475	18	2	2.02579	13.2070
500	18	2	2.08473	43.3828

TABLE 1. Case A

			density			c		
n	m	d	S	L	A	S	L	A
25	10	2	1.83105	2.09961	1.9987	0.719	5.407	2.409
50	12	2	1.95312	2.24609	2.0874	0.125	15.750	6.515
75	14	2	1.81274	2.12402	1.9689	0.055	23.969	10.144
100	14	2	1.86157	2.39258	2.1517	0.251	50.250	20.267
125	14	2	1.75476	2.30408	1.9857	0.141	38.922	11.135

TABLE 2. Case B

$I_n(V_q)$. The data in our tables are based on several thousand values of $I_n(V_q)$ for m up to 18.

The data in our tables indicate that $c < n$, i.e. the error term is $O(q^{m/2})$. For a linear variety V of dimension m over $\mathbb{F}_q$, it seems that

$$I_n(V_q) = d \cdot \frac{q^m}{n} + O(q^{m/2})$$

where $d \geq 1$ is a constant depending only on the variety V and the implied constant in $O(\cdot)$ is independent of m, n and q.

			density			*c*		
n	m	d	S	L	A	S	L	A
25	10	2	1.31836	2.41699	1.9092	1.500	21.813	7.163
50	12	2	1.75781	2.63672	2.0459	0.125	40.750	12.838
75	14	2	1.73035	2.22015	1.99468	0.0546875	34.5156	8.26629

TABLE 3. Case C

			density			*c*		
n	m	d	S	L	A	S	L	A
25	10	1	0.732422	1.36719	1.074220	0.750	11.750	5.325
50	12	1	0.732422	1.22070	0.969238	1.625	17.125	7.969
75	14	1	0.924683	1.14441	1.031800	0.265	18.485	9.205
100	14	1	0.903320	1.09863	0.988770	0.125	12.625	6.851
125	14	1	0.823975	1.23596	0.997925	2.859	30.204	12.710
150	16	1	0.888062	1.16272	1.001590	5.218	41.657	17.451

TABLE 4. Case D

			density			*c*		
n	m	d	S	L	A	S	L	A
25	10	1	0.732422	1.17188	1.00911	0.032	8.5625	3.492
50	12	1	0.805664	1.19629	1.03053	0.063	12.5625	4.594
75	14	1	0.833131	1.16731	0.99538	0.266	21.4141	7.036
100	14	1	0.830078	1.17798	1.01333	0.126	22.7812	7.334
125	14	1	0.793457	1.14441	0.98901	0.071	26.4375	8.403

TABLE 5. Case D.1: Dickson polynomials

			density			*c*		
n	m	d	S	L	A	S	L	A
25	10	2	1.31836	2.41699	1.9092	1.501	21.813	7.163
50	12	2	1.75781	2.63672	2.0459	0.125	40.751	12.838

TABLE 6. Case D.2

Our experiments do not cover the arbitrary variety case. In general, $I_n(V_q)$ is much more difficult to determine. When q is small, it is even not clear what to expect on the size of $I_n(V_q)$. When q is large, we have some control on the major term of $I_n(V_q)$, but the constant d is yet to be determined. We hope that our experimental results will stimulate more interests in this problem.

Finally, we remark that when $F(x)$ is a multivariate polynomial, Theorem 1.4 also holds [10, 15, 38]. Here we would like to provide an example with $d/n = 1$. Let $\mathbb{F}$ be any field over which x and y are algebraically independent. Define a polynomial

$$F(x, y) = x^m + y^n + x^u y^v + \sum c_{ij} x^i y^j$$

				density			*c*		
n	m	$a(x)$	d	S	L	A	S	L	A
25	10	$x^2 - x$	4	3.61328	4.49219	4.01106	0.125	15.75	5.24129
25	10	$x^4 - x$	5.33	4.66309	5.85938	5.33936	0.2475	21.3413	5.72504
25	10	$x^8 - x$	5.22	4.6875	5.7373	5.23529	0.1475	17.04	6.20377
50	12	$x^2 - x$	4	3.50342	4.62646	4.00031	0.25	40.0938	9.91799
50	12	$x^4 - x$	5.33	4.74854	5.98145	5.36126	0.28625	41.6925	10.7219
50	12	$x^8 - x$	5.22	4.63867	5.99365	5.24532	0.295	49.5138	11.6792
50	12	$x^{16} - x$	6.47	5.94482	7.10449	6.44112	0.0175	40.6075	11.3236
75	14	$x^2 - x$	4	3.63922	4.30298	3.98748	0.109375	46.1797	12.1067
75	14	$x^4 - x$	5.33	4.953	5.86395	5.34038	0.20875	68.3459	14.4665
75	14	$x^8 - x$	5.22	4.83398	5.61676	5.21434	0.19125	50.7853	12.7299

TABLE 7. Theorem 1.2

where $c_{ij} \in \mathbb{F}$ and the sum is over all pairs (i, j) such that in the real Euclidean plane the point (i, j) is inside the triangle determined by the points $(m, 0)$, $(0, n)$ and (u, v) (so $un + vm \neq mn$). In [17], it is proved that if $\gcd(m, n, u, v) = 1$ then $F(x, y)$ is absolutely irreducible over $\mathbb{F}$. In particular, let $\mathbb{F} = \mathbb{F}_q$ and

$$F(x, y, z_1, \ldots, z_k) = x^m + y^n + x^u y^v + \sum x^i y^j c_{ij}(z_1, \ldots, z_k)$$

where $c_{ij}(z_1, \ldots, z_k)$ are polynomials in $\mathbb{F}_q[z_1, \ldots, z_k]$ and the sum is same as above. Then for any point $(a_1, \ldots, a_k) \in \mathbb{F}_q^k$, the bivariate polynomial $F(x, y, a_1, \ldots, a_k)$ is (absolutely) irreducible over $\mathbb{F}_q$. Let $V_q = \mathbb{F}_q^k$, a variety of dimension k. Then the number of points a in V_q such that $F(x, y, a)$ is irreducible is exactly q^k. So in Theorem 1.4 for multivariate polynomials $F(x)$, the constant d/n is 1 and the error term is zero.

Acknowledgement. We thank Daqing Wan for his useful comments on the first draft of the paper. We used Victor Shoup's NTL package in our computations.

REFERENCES

[1] E. ARTIN, Quadratische Körper im Gebiete der höheren Kongruenzen. II. *Math. Z.*, **19** (1924), 207–246.

[2] E.R. BERLEKAMP, Bit-serial Reed-Solomon encoders. *IEEE Trans. Info. Th.*, **28** (1982), 869-874.

[3] J. BIRCH AND H. SWINNERTON-DYER, Note on a problem of Chowla. *Acta Arith. 5* (1959), 417–423.

[4] I.F. BLAKE, S. GAO AND R. LAMBERT, Constructive problems for irreducible polynomials over finite fields. *Information Theory and Applications*, eds., A. GULLIVER AND N. SECORD, LNCS 793, Springer-Verlag, 1994, 1-23.

[5] I.F. BLAKE, S. GAO AND R. LAMBERT, Construction and distribution problems for irreducible trinomials over finite fields. *Applications of Finite Fields*, ed., D. GOLLMANN, Oxford, Clarendon Press, 1996, 19–32.

[6] I.F. BLAKE, S. GAO AND R.C MULLIN, Explicit factorization of $x^{2^k} + 1$ over F_p with prime $p \equiv 3 (\mathrm{mod}\ 4)$. *App. Alg. in Eng., Comm. and Comp.*, **4** (1993), 89–94.

[7] M. CAR, Théorèmes de densité dans $\mathbb{F}_q[X]$. *Acta Arith.* **48** (1987), 145–165.

[8] L. CARLITZ, Theorem of Dickson on irreducible polynomials. *Proc. Amer. Math. Soc.* **3** (1952), 693–700.

[9] S. CHOWLA, A note on the construction of finite galois fields $\mathrm{GF}(p^n)$. *J. Math. Anal. Appl. 15* (1966), 53–54.

[10] Z. CHATZIDAKIS, L. VAN DEN DRIES AND A. MACINTYRE, Definable sets over finite fields. *J. Reine Angew. Math.* **427** (1992), 107–135.
[11] S.D. COHEN, The distribution of polynomials over finite fields. *Acta Arith.* **17** (1970), 255–271.
[12] S.D. COHEN, Uniform distribution of polynomials over finite fields. *J. London Math. Soc.* **6** (1972), 93–102.
[13] D. COPPERSMITH, Fast evaluation of logarithms in fields of characteristic two. *IEEE Trans. Info. Theory* **30** (1984), 587–594.
[14] P. DELIGNE, La conjecture de Weil I. In *Publ. Math. IHES*, **43** (1974), 273–307.
[15] M. FRIED, D. HARAN AND M. JARDEN, Effective counting of the points of definable sets over finite fields. *Israel J. Math.*, **85** (1994), no. 1-3, 103-133.
[16] S. GAO, Elements of provable high orders in finite fields. Preprint (9 pages) 1997. To appear in *Proc. American Math. Soc.*.
[17] S. GAO, Absolute irreducibility of polynomials via Newton polytopes. In preparation.
[18] S. GAO AND D. PANARIO, Density of normal elements. *Finite Fields and Their Applications* **3** (1997), 141–150.
[19] S. GAO AND D. PANARIO, Tests and constructions of irreducible polynomials over finite fields. In *Foundations of Computational Mathematics*, ed. F. CUCKER AND M. SHUB, 346–361. Springer Verlag, 1997.
[20] S. GAO AND H.W. LENSTRA, JR., Optimal normal bases. *Designs, Codes and Cryptography* **2** (1992), 315-323.
[21] S.W. GOLOMB, *Shift register sequences.* Aegean Park Press, Laguna Hills, California, 1982.
[22] T. HANSEN AND G.L. MULLEN, Primitive polynomials over finite fields. *Math. Comp.*, **59** (1992), 639–643.
[23] D.R. HAYES, The distribution of irreducibles in $\mathbb{F}_q[x]$. *Trans. American Math. Soc.* **117** (1965), 101–127.
[24] D.R. HAYES, The Galois group of $x^n + x - t$. *Duke Math. J.* **40** (1973), 459–461.
[25] C.-H. HSU, The distribution of irreducibles in $\mathbb{F}_q[t]$. *J. Number Theory* **61** (1996), 85–96.
[26] R. LOVORN BENDER AND C. POMERANCE, Rigorous discrete logarithm computations in finite fields via smooth polynomials. *Computational perspectives on number theory* (Chicago, IL, 1995), 221–232, AMS/IP Stud. Adv. Math., 7, Amer. Math. Soc., Providence, RI, 1998.
[27] A.J. MENEZES, I.F. BLAKE, X. GAO, R.C. MULLIN, S.A. VANSTONE, AND T. YAGHOOBIAN, *Applications of Finite Fields.* Kluwer Academic Publishers, Boston, Dordrecht, Lancaster, 1993.
[28] G.L. MULLEN AND I.E. SHPARLINSKI, Open problems and conjectures in finite fields. In *Finite Fields and Applications* (S.D. Cohen and H. Niederreiter Eds.), Cambridge University Press, Lecture Note Series of London Math. Society, Vol. 233 (1996), 243-268.
[29] R.C. MULLIN, I.M. ONYSZCHUK, S.A. VANSTONE AND R.M. WILSON, Optimal normal bases in $GF(p^n)$. *Discrete Applied Math.* **22** (1988/1989), 149-161.
[30] A. ODLYZKO, Discrete logarithms and their cryptographic significance. In *Advances in Cryptology, Proceedings of Eurocrypt 1984, Lecture Notes in Computer Science*, Vol. 209, Springer-Verlag, 1985, 224–314.
[31] D. PANARIO, X. GOURDON AND P. FLAJOLET *An analytic approach to smooth polynomials over finite fields.* In Algorithmic Number Theory Symposium (Proceedings of ANTS III, Ed. J. P. Buhler), LECTURE NOTES IN COMPUTER SCIENCE, Vol. 1423, Springer-Verlag, 1998, 226-236.
[32] R. REE, Proof of a conjecture of S. Chowla. *J. Number Theory 3* (1971), 210–212.
[33] I. A. SEMAEV, An algorithm for evaluation of discrete logarithms in some nonprime finite fields. Preprint 1994. To appear in *Math. Comp.*.
[34] V. SHOUP, 1994. Private communication.
[35] I.E. SHPARLINSKI, Finding irreducible and primitive polynomials. *Appl. Alg. Eng. Comm. Comp.* **4** (1993), 263–268.
[36] K. SOUNDARARAJAN, Asymptotic formulae for the counting function of smooth polynomials. To appear in *J. London Math. Soc.*.
[37] S.A. STEPANOV, The number of irreducible polynomials of a given form over a finite field. *Math. Notes* **41** (1987), 165–169.
[38] D. WAN, Hilbert sets and zeta functions over finite fields. *J. Reine Angew. Math.* **427** (1992), 193-207.

[39] D. WAN, Computing Zeta functions over finite fields. These proceedings, to appear.
[40] M. WANG AND I.F. BLAKE, Bit-serial multiplication in finite fields. *IEEE Trans. Comput.*, **38** (1989), 1457-1460.
[41] S. WEIL, Sur les courbes algébriques et les variétés qui s'en déduisent. *Actualités Sei. et Ind.* **1041**, Paris 1948.
[42] S. UCHIYAMA, Sur les polynomes irréductibles dans un corps fini. II. *Proc. Japan Acad.* **31** (1955), 267–269.
[43] M. ŽIVKOVIĆ, A table of primitive binary polynomials. *Math. Comp.*, **62** (1994), 385–386.
[44] M. ŽIVKOVIĆ, Table of primitive binary polynomials. *Math. Comp.*, **63** (1994), 301–306.

DEPARTMENT OF MATHEMATICAL SCIENCES, CLEMSON UNIVERSITY, CLEMSON, SC 29634-1907, USA *E-mail address*: SGAO,HOWELL@MATH.CLEMSON.EDU

DEPARTMENT OF COMPUTER SCIENCE, UNIVERSITY OF TORONTO, TORONTO, ONTARIO M5S 3G4, CANADA *E-mail address*: DANIEL@CS.TORONTO.EDU

Contemporary Mathematics
Volume **225**, 1999

An application of Galois calculus to $\mathbf{F}_q[t]$

Yves HELLEGOUARCH

ABSTRACT. Using new differential tools, we show that if a great number of polynomials of the same degree in $\mathbf{F}_q[t]$ are pairwise prime and generate an $\mathbf{F}_q-$vector space of small dimension then, collectively, they must have a certain number of roots of small degree over $\mathbf{F}_q$.

1. Introduction

This paper develops a theme sketched in [1] which is the result of two different types of considerations.

The older ones (which go back to Liouville [4], Korkine, Stothers) are generally called "'Mason's theorem". The version of its proof used in this paper is the elementary one given by Oesterlé in [6]. It has been generalized here to higher dimensions. The more recent considerations have been developed in [2] and [3] and are linked to the Carlitz module. They use a "Galois calculus" based on special divided differences, which is similar to the ordinary calculus in many ways and can be developed quite naturally in $\mathbf{F}_q(t)$, in place of the ordinary calculus, to give indications on the location of roots of polynomials of $\mathbf{F}_q[t]$ in an algebraic closure of $\mathbf{F}_q$.

The properties of the Galois calculus which are essential to the proof are mentioned in the prerequisites. They are the analogues of the ingredients of the classical proof (see [3] and [6]) i.e. the $\mathbf{F}_q-$linearity of the Galois derivatives, the Wronskian criterion which ensures the non nullity of crucial determinantal expressions, the evaluation of upper bounds for the degree of the Galois derivatives of a polynomial and, finally, information concerning the behaviour of the multiplicity of a root under Galois derivation (theorem 4). We can express in a loose way the results obtained by saying that if we have many $\mathbf{F}_q-$linear combinations of a "small" number of polynomials which are pairwise prime, and if q is "small", then some of those linear combinations must have roots in a certain finite extension of $\mathbf{F}_q$ of bounded degree.

2. Some prerequisites

Let Ω be any field containing $\overline{\mathbf{F}}_q[t]$ as a subring and let $x \in \Omega$. We define the n^{th} Galois derivative $D_t^{(n)}(x)$ by the recursion formulae :

$$D_t^{(0)}(x) := x, \quad D_t^{(1)}(x) := \frac{x^q - x}{t^q - t}, \ldots$$
$$D_t^{(n)}(x) := \frac{D_t^{(n-1)}(x)^q - D_t^{(n-1)}(x)}{t^{q^n} - t} \tag{1}$$

1991 Mathematics Subject Classification. Primary 12E20, 12D10, Secondary 13M10.

© 1999 American Mathematical Society

Properties of Galois derivatives are developed in [1] and [2] in a more general setting and we restrict ourselves to a few results.
First of all we remark that :

$$D_t^{(1)} = \frac{1}{t^q - t}(\sigma - id_\Omega)$$

where σ denotes the Frobenius endomorphism of Ω :

$$\sigma : x \longmapsto x^q$$

Then one gets (by induction) an analog of Leibniz's formula ([1], [2]) :

$$D_t^{(n)}(xy) = \sum_{i=0}^{n} D_t^{(i)}(x)\sigma^i[D_t^{(n-i)}(y)] \tag{2}$$

From Leibniz's formula one deduces :

$$D_t^{(n)}(t^m) = \sum_{\gamma_0+\ldots+\gamma_n=m-n} t^{\gamma_0+\gamma_1 q+\ldots+\gamma_n q^n}$$

which shows that $D_t^{(n)}(P) \in \mathbb{F}_q[t]$ for each polynomial $P \in \mathbb{F}_q[t]$.
Now we denote by $\mathbb{F}_q(t)\{\sigma\}$ (resp. $\mathbb{F}_q(t)\{\{\sigma\}\}$) the ring of Ore polynomials (resp. formal series) in the twisted indeterminate σ. So we see that $D_t^{(1)}, D_t^{(2)}, \ldots$ are all in $\mathbb{F}_q(t)\{\sigma\}$. More precisely we have the following result.

THEOREM 1. *Let us write*

$$\Delta_t^{(n)} := \begin{vmatrix} 1 & t & \ldots & t^{n-1} & \sigma^0 \\ 1 & \sigma(t) & \ldots & \sigma(t^{n-1}) & \sigma \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ 1 & \sigma^n(t) & \ldots & \sigma^n(t^{n-1}) & \sigma^n \end{vmatrix} \in \mathbb{F}_q(t)\{\sigma\}$$

then we have :

$$D_t^{(n)} = \frac{1}{\Delta_t^{(n)}(t^n)}\Delta_t^{(n)} \in \mathbb{F}_q(t)\{\sigma\} \tag{3}$$

REMARK. A well known property of Moore's determinant shows that $\Delta_t^{(n)}(t^n)$ is non null. For a proof of (3) one is referred to [1] or [2].

COROLLARY 1. *The Galois derivative $D_t^{(n)}$ is :*

$$D_t^{(n)} = a_n\sigma^n + a_{n-1}\sigma^{n-1} + \cdots + a_0\sigma^0$$

with :

$$\begin{cases} a_n^{-1} &= \prod_{j=0}^{n-1}[\sigma^n(t) - \sigma^j(t)] = A_n \\ a_{n-1}^{-1} &= -[\sigma^n(t) - \sigma^{n-1}(t)]\prod_{j=0}^{n-2}[\sigma^{n-1}(t) - \sigma^j(t))] = A_{n-1} \\ a_{n-h}^{-1} &= (-1)^h \prod_{i=n-h}^{n}[\sigma^i(t) - \sigma^{n-h}(t)]\prod_{j=0}^{h-1}[\sigma^h(t) - \sigma^j(t)] = A_{n-h} \\ a_0^{-1} &= (-1)^n\prod_{j=0}^{n}[\sigma^i(t) - t] = A_0 \end{cases} \tag{4}$$

with $A_n, A_{n-1}, \ldots, A_0$ in $\mathbb{F}_q[t]$.

Proof – Formulas (4) are deduced from (3) by development along the $(n+1)^t h$ column of $\Delta_t^{(n)}$ and by the use of the well known formula :

$$(5)\quad \Delta_t^{(n)}(t^n) = \begin{vmatrix} 1 & t & \dots & t^{n-1} & t^n \\ 1 & \sigma(t) & \dots & \sigma(t^{n-1}) & \sigma(t^n) \\ \dots & \dots & \dots & \dots & \dots \\ 1 & \sigma^n(t) & \dots & \sigma^n(t^{n-1}) & \sigma^n(t^n) \end{vmatrix} = \prod_{0\le i<j\le n} (\sigma^j(t)-\sigma^i(t))$$

It is well known ([5]) that a necessary and sufficient condition for $x_1,\dots,x_n$ to be linearly independent over $\mathbf{F}_q$ is the non nullity of the Moore determinant :

$$(6)\quad M(x_1,\dots,x_n) = \begin{vmatrix} x_1 & x_2 & \dots & x_n \\ \sigma(x_1) & \sigma(x_2) & \dots & \sigma(x_n) \\ \dots & \dots & \dots & \dots \\ \sigma^{n-1}(x_1) & \sigma^{n-1}(x_2) & \dots & \sigma^{n-1}(x_n) \end{vmatrix} \neq 0$$

Then formula (6) furnishes the Wronskian criterion. ∎

THEOREM 2 (Wronskian criterion). *Let $x_1,\dots,x_n \in \Omega$. Then a necessary and sufficient condition for $x_1,\dots,x_n$ to be linearly independent over $\mathbb{F}_q$ is :*

$$(7)\quad \begin{vmatrix} x_1, & x_2, & \dots, & x_n \\ D_t^{(1)}(x_1), & D_t^{(1)}(x_2), & \dots, & D_t^{(1)}(x_n) \\ \vdots & \vdots & \vdots & \vdots \\ D_t^{(n-1)}(x_1), & D_t^{(n-1)}(x_2), & \dots, & D_t^{(n-1)}(x_n) \end{vmatrix} \neq 0$$

Once we have Galois derivative $D_t^{(0)}, D_t^{(1)}, etc.\dots$ we can consider the Ore generating series :

$$\varphi_t(x) := D_t^{(0)}(x) + D_t^{(1)}(x)\sigma + D_t^{(2)}(x)\sigma^2 + \dots \in \Omega\{\{\sigma\}\}$$

and Leibniz's formula implies the following result.

THEOREM 3. *The mapping :*

$$\begin{cases} \Omega & \xrightarrow{\varphi_t} \Omega\{\{\sigma\}\} \\ x & \longmapsto \varphi_t(x) \end{cases}$$

is a morphism of $\mathbb{F}_q$–algebras. Moreover $x \in \mathbb{F}_q[t]$ is tantamount to $\varphi_t(x) \in \mathbb{F}_q(t)\{\sigma\}$.

PROOF. We only need to prove the last assertion. We have already noticed that if x is a polynomial, $\varphi_t(x) \in \mathbb{F}_q[t]\{\sigma\}$.
Reciprocally suppose $\varphi_t(x) \in \mathbb{F}_q(t)\{\sigma\}$ and suppose :

$$\deg_\sigma \varphi_t(x) = n$$

Then $x, 1, t, t^2, \dots, t^n$ are all in the kernel of the $\mathbb{F}_q$–linear map $D_t^{(n+1)}$. By the Wronskian criterion they are $\mathbb{F}_q$–linearly dependant.

REMARKS.

1) φ_t is nothing else than the extension to Ω of the Carlitz module and the formulae (1) were known to Carlitz and Goss when $x \in \mathbb{F}_q[t]$.

2) If we denote by $e = \sigma^0 + \frac{\sigma}{F_1} + \frac{\sigma^2}{F_2} + \cdots$ with $F_1 = \sigma(t) - t$, $F_2 = (\sigma^2(t) - t)\sigma(F_1)$, etc., the Carlitz exponential, we have in $\mathbb{F}_q(t)\{\{\sigma\}\}$

$$\varphi_t(x) = e.x\sigma^0.e^{-1}$$

THEOREM 4. *Let $n \in \mathbb{N}$, $P(t) \in \mathbb{F}_q[t]$ and let $\alpha \in \Omega$ be a root of $P(t)$ of degree d and multiplicity $\nu \geq \frac{n}{d}$. Then we have :*

i) When $d > n$, α is a root of $D_t^{(n)}P$ of the same multiplicity ν.

ii) If $d \leq n$, α is a root of $D_t^{(n)}P$ of multiplicity $\nu - [\frac{n}{d}]$, where $[\frac{n}{d}]$ means the entire part of the rational $\frac{n}{d}$

Proof -

1) Suppose first that $d > n$. Then α is a root of multiplicity ν of :

$$D_t^{(1)}(P) = \frac{P^q - P}{t^q - t}$$

because α is not a root of $t^q - t$, and so on for the next derivatives.
Then one gets that the multiplicity of α in $D_t^{(n)}(P)$ is ν.

2) Now we consider the situation where $d \leq n$, $d > 1$. If α is a root of order μ_m of $D_t^{(md)}(P)$, then we have :

$$D_t^{(md+1)}(P) := \frac{D_t^{(md)}(P)^q - D_t^{(md)}(P)}{t^{q^{md+1}} - t}$$

as d does not divide $md + 1$ we see that α is not a root of $t^{q^{md+1}} - t$. So α is a root of order μ_m of $D_t^{(md+1)}(P)$ and so on, up to $D_t^{(md+d-1)}(P)$. When we come to $D_t^{((m+1)d)}(P)$ we have :

$$D_t^{((m+1)d)}(P) := \frac{(D_t^{(m+1)d-1}(P))^q - D_t^{(m+1)d-1}}{t^{q^{(m+1)d}} - t}$$

and α is a simple root of $t^{q^{(m+1)d}} - t$, so we have $\mu_{m+1} = \mu_m - 1$. So the multiplicity of α in $D_t^{(n)}(P)$ is $\nu - [\frac{n}{d}]$.

3) Finally we must consider the case $d = 1$ and $\nu \geq n$. The multiplicity of α in $D_t^{(m)}(P)$ decreases by one at each step, so the formula remains valid. ∎

3. First series of applications

This first series of applications is modelled on the elementary proof of Mason's theorem given in [6], the usual derivative being replaced by the first Galois derivative $D_t^{(1)}$.
Recall that Mason's theorem is about ABC relations and that an ABC relation is just an equation :

$$A + B + C = 0 \tag{8}$$

between pairwise prime polynomials A, B, C in $\mathbb{F}_q[t]$. Relation (8) is considered to be non trivial if $ABC \notin \mathbb{F}_q$ (at least in this paper).

Let us mention the characteristic p version of Mason's theorem as given in [3] for any field of characteristic p.

PROPOSITION. *If, in the ABC relation (8), the derivative of* $\frac{A}{B}$ *is non null, then the number of roots of the polynomial ABC (in a specified algebraic closure to the constant field) whose multiplicity is not divisible by p is strictly greater than sup* $(\deg A, \deg B, \deg C)$.

For an application of this proposition to polynomial Diophantine equations over any field of characteristic p see [3].

Let us proceed now towards a more specialized version of this result for **finite fields.**

DEFINITION. *Let* $P \in \mathbb{F}_q[t]$, *we define the* rational radical R_r *of* P *over* $\mathbb{F}_{q^r}$ *as the product :*

$$R_r(P) = \prod_{\alpha \in S_r} (t - \alpha) \in \mathbb{F}_{q^r}[t]$$

where S_r *denotes the set of roots of* P *in* $\mathbb{F}_{q^r}$

APPLICATION 1. *Given a non trivial ABC relation in* $\mathbb{F}_q[t]$ *let* R_1 *be the rational radical of the product ABC over* $\mathbb{F}_q$. *Then we have :*

$$\deg R_1 \geq q - (q-2)s$$

where $s := \sup(\deg A, \deg B, \deg C)$.

REMARK. This result is not really interesting as it can be easily checked but the method of proof is the prototype of later proofs. Let us verify it for $q = 3$ and $q = 2$.

If $q = 3$ and $s = 2$, we have $\deg R_1 \geq 1$. This implies that if A et B are irreducible in $\mathbb{F}_3[t]$, pairwise prime and degree 2, then $A + B$ has a root in $\mathbb{F}_3$.

This can be easily checked since there are just three irreducible monic polynomials of degree two in $\mathbb{F}_3[t]$.

If $q = 2$, we always have $\deg R_1 \geq 2$. This can also be very easily checked in a different way. Since we have :

$$\begin{cases} C(0) = A(0) + B(0) \in \mathbb{F}_2 \\ C(1) = A(1) + B(1) \in \mathbb{F}_2 \end{cases}$$

so $ABC(0) = ABC(1) = 0 \in \mathbb{F}_2$!

Proof – Consider the determinant :

$$\Delta = \begin{vmatrix} A & B \\ D^{(1)}(A) & D^{(1)}B \end{vmatrix} = \begin{vmatrix} B & C \\ D^{(1)}(B) & D^{(1)}(C) \end{vmatrix} = \begin{vmatrix} C & A \\ D^{(1)}(C) & D^{(1)}(A) \end{vmatrix}$$

We remark that $\Delta \neq 0$. Otherwise the Wronskian criterion (th. 2) would imply that $\lambda A + \mu B = 0$. As A and B are prime to each other we would have $A, B \in \mathbb{F}_q$ so $C \in \mathbb{F}_q$ which contradicts the non triviality of the relation AB. Suppose that α is a root of A in $\mathbb{F}_q$ of multiplicity ν, then theorem 4 shows that α is a root of $D^{(1)}(A)$ of multiplicity $\nu - 1$ and, as α is not a root of B or C, then α is a root of Δ of multiplicity $\nu - 1$.

On the other hand if α is a root of A in $\overline{\mathbb{F}}_q \setminus \mathbb{F}_q$ the same theorem shows that α_1 is a root of $D^{(1)}(A)$ of multiplicity ν, so α is a root of Δ of multiplicity $\geq \nu$.

We conclude that $\frac{ABC}{R_1}$ divides Δ. Taking degrees we have :

$$\deg(ABC) - \deg(R_1) \leq \deg \Delta$$

Now if we set :

$$\epsilon := \inf(\deg A, \deg B, \deg C)$$

we have :

$$\deg \Delta \leq q(s-1) + \epsilon$$

and, if $\deg A = \deg B = s$ (for instance) :

$$2s + \epsilon - q(s-1) - \epsilon \leq \deg(R_1)$$

which gives our result.

To get a more general result we now realize a small change of notations and consider the homogeneous polynomial in two indeterminates X_1, X_2 :

$$P(X_1, X_2) := X_1 X_2 \varphi_1(X_1, X_2) \cdots \varphi_n(X_1, X_2) \in \mathbb{F}_q[X_1, X_2]$$

where $\varphi_i(X_1, X_2) = X_1 - c_i X_2$ for distinct $c_1, \ldots, c_n$ in $\mathbb{F}_q^*$. ∎

APPLICATION 2. *Let A_1 and A_2 be polynomials in $\mathbb{F}_q[t]$ prime to each other and let $s := \sup(\deg A_1, \deg A_2)$. Then the polynomial $P(A_1, A_2)$ has at least $(n+1-q)s + q$ distinct roots in $\mathbb{F}_q$ when $s \geq 1$.*

Proof – We set :

$$B_{-1} = A_1, \quad B_0 = A_2, \quad B_i = \varphi(A_1, A_2) \text{ for } 1 \leq i \leq n.$$

Obviously the polynomials B_i are pairwise prime.
If we consider the Wronskians :

$$W_{i,j} = \begin{vmatrix} B_i & B_j \\ D^{(1)}B_i & D^{(1)}B_j \end{vmatrix} \qquad i \neq j$$

we see that they only differ by a constant multiplicative factor. They are non null because A_1 and A_2 must not be dependent in $\mathbb{F}_q$. Let $\epsilon = \inf\{\deg B_i$, for $i = -1, 0, \ldots n\}$. It is clear that ϵ is reached only for one index i when $\epsilon < s$. Let R_1 be the rational radical of $B_{-1}B_0 \ldots B_n$. As in application 1 we see, taking a good pair (i, j), that :

$$\deg W := \deg W_{i,j} = q(s-1) + \epsilon$$

We see also that $\frac{P(A_1, A_2)}{R_1}$ divides W so, taking degrees, we have :

$$(n+1)s + \epsilon - \deg R_1 \leq q(s-1) + \epsilon$$

which gives our result. ∎

REMARK. Since $\mathbb{F}_{q^r}/\mathbb{F}_q$ is a Galois extension, we see that $R_r(P) \in \mathbb{F}_q[t]$ in fact.

4. Second applications

We consider n "linear forms" $\varphi_i(X_1, X_2, X_3) \in \mathbb{F}_q[X_1, X_2, X_3]$, meaning polynomials of degree one in each indeterminate, and we denote by $P(X_1, X_2, X_3)$ the polynomial :

$$P(X_1, X_2, X_3) := X_1 X_2 X_3 \varphi_1(X_1, X_2, X_3) \cdots \varphi_n(X_1, X_2, X_3)$$

We suppose that there exist three $\mathbb{F}_q-$linearly independent polynomials A_1, A_2, A_3 in $\mathbb{F}_q[t]$ such that $A_1, A_2, A_3, \varphi_1(A_1, A_2, A_3), \ldots, \varphi_n(A_1, A_2, A_3)$ are pairwise prime in $\mathbb{F}_q[t]$.
Let R_1 (resp. R_2) be the rational radical of $P(A_1, A_2, A_3)$ over $\mathbb{F}_q$ (resp. $\mathbb{F}_{q^2}$) then we have

APPLICATION 3. *Suppose the above conditions verified and :*

$$\deg A_1 = \deg A_2 = \deg A_3 = \deg \varphi_i(A_1, A_2, A_3) = s$$

except for at most two values of i, then we have :

$$\deg(R_1 R_2) \geq s(n + 2 - q - q^2) + 2q^2 + q$$

with $s = \sup(\deg A_1, \deg A_2, \deg A_3)$.

EXAMPLE. If $n = q + q^2 - 3$, then $P(A_1, A_2, A_3)$ has at least $[\frac{1}{2}(2q^2 + q - s)]$ roots in $\mathbb{F}_{q^2}$.

Proof – We write :

$$B_{-2} = A_1,\ B_{-1} = A_2,\ B_0 = A_3,\ B_i = \varphi_i(A_1, A_2, A_3)$$

for $1 \leq i < j < k \leq n$, and we consider the Wronskians :

$$W_{i,j,k} := \begin{vmatrix} B_i & B_j & B_k \\ D^{(1)}B_i & D^{(1)}B_j & D^{(1)}B_k \\ D^{(2)}B_i & D^{(2)}B_j & D^{(2)}B_k \end{vmatrix}$$

We see that those Wronskians only differ by a constant multiplicative factor and are non null in $\mathbb{F}_q[t]$ (Wronskian criterion) if B_i, B_j, B_k are $\mathbb{F}_q-$linearly independent.
We also see that for any $k \in \{1, \ldots, n\}$ there are $i, j \in \{-2, -1, 0\}$ such that $W_{i,j,k} \neq 0$.
Let us denote by $\nu_\alpha(S)$ the order of a polynomial S at a root α of $R_1 R_2$. Theorem 4 implies that for all non null $W_{i,j,k}$ we have :

$$\nu_\alpha[P(A_1, A_2, A_3)] - \nu_\alpha(R_1 R_2) \leq \nu_\alpha(W_{i,j,k})$$

This is obvious if $\nu \geq \dfrac{2}{\deg(\alpha)}$, so there is nothing to prove if $(\nu, \deg(\alpha)) \neq (1, 1)$.
But in the latter case we see that the left hand side is negative.
We deduce that if all the B_i are of degree s :

$$\deg(R_1 R_2) \geq (n + 3)s - \deg W_{i,j,k}$$

But $\deg W_{i,j,k} \leq s + q(s - 1) + q^2(s - 2)$, so :

$$\deg(R_1 R_2) \geq (n + 2 - q - q^2)s + 2q^2 + q$$

Now we suppose that $\deg B_{i_0} < \deg B_i$ for $i = i_0$, and we write $\deg B_{i_0} = s_0$. Then if we consider W_{i,j,i_0} we have :

$$\begin{cases} \deg P(A_1, A_2, A_3) = (n+2)s + s_0 \\ \deg W_{i,j,i_0} \leq s_0 + q(s-1) + q^2(s-2) \end{cases}$$

and we get the same result.
Finally we suppose that :

$$s_0 = \text{ degree } B_{i_0} \leq s_1 = \text{ degree } B_{i_1} < \deg B_i \text{ for } i \notin \{i_0, i_1\}.$$

Then we can write :

$$\begin{cases} B_{i_0} = \lambda_1 A_1 + \lambda_2 A_2 + \lambda_3 A_3 \\ B_{i_1} = \mu_1 A_1 + \mu_2 A_2 + \mu_3 A_3 \end{cases}$$

with λ_i, μ_j in $\mathbf{F}_q$. If the vectors $(\lambda_1, \lambda_2, \lambda_3)$ and (μ_1, μ_2, μ_3) were colinear, then B_{i_0} and B_{i_1} would not be prime to each other. So $(\lambda_1, \lambda_2, \lambda_3)$ and (μ_1, μ_2, μ_3) are $\mathbf{F}_q$−independent, and there is an index j such that B_{i_0}, B_{i_1} and A_j are independent. Let $A_j = B_{i_2}$ so we see that $W_{i_0,i_1,i_2} \neq 0$ and :

$$\begin{cases} \deg P(A_1, A_2, A_3) & = (n+1)s + s_0 + s_1 \\ \deg W_{i_0,i_1,i_2} & \leq s_0 + q(s_1 - 1) + q^2(s-2) \end{cases}$$

so :

$$\deg(R_1 R_2) \geq (n+1)s + s_1 - q(s_1 - 1) - q^2(s-2)$$

As $s_1 < s$ we get :

$$(q-1)s_1 < (q-1)s$$

and :

$$\deg(R_1 R_2) > (n + 2 - q - q^2)s + 2q^2 + q.$$

The last case in the above discussion of the proof of Application 3 shows that the minoration of $\deg(R_1 R_2)$ can be improved if the degrees of the factors of $P(A_1, A_2, A_3)$ are unequal. As a matter of fact we have the following result. ∎

APPLICATION 4. *Suppose A_1, A_2, A_3 are such that $\deg A_1 = s_2 > \deg A_2 = s_1 > \deg A_3 = s_0$ and set :*

$$P(A_1, A_2, A_3) = A_3 \prod_{i,j} (A_1 + \lambda_i A_2 + \mu_j A_3) \prod_k (A_2 + \nu_k A_3)$$

where λ_i, μ_j, ν_k are chosen in $\mathbf{F}_q$ such that the factors of $P(A_1, A_2, A_3)$ are pairwise prime. Then we have :

$$\deg(R_1 R_2) \geq (\ell m - q^2)s_2 + (n-q)s_1 + 2q^2 + q$$

where ℓ (resp.(m, n)) is the number of λ_i (resp. μ_j, ν_k).

Proof – This time we take $B_{-2} = B_3$, and choose B_{-1} among the $A_1 + \lambda_i A_2 + \lambda_j A_3$ and B_0 among the $A_2 + \nu_k A_3$.
The Wronskian criterion implies that $W_{-2,-1,0}$ is non null and (varying the choices) we get :

$$\deg(R_1 R_2) \geq \deg P(A_1, A_2, A_3) - \deg W_{-2,-1,0}.$$

Now we have :

$$\deg W_{-2,-1,0} \leq q^2(s_2 - 2) + q(s_1 - 1) + s_0$$

so :

$$\begin{aligned} \deg(R_1 R_2) &\geq s_0 + \ell m s + n s_1 - [q^2(s_2 - 2) + q(s-1) + s_0] \\ &= (\ell m - q^2)s_2 + (n-q)s_1 + 2q^2 + q \end{aligned}$$

∎

EXAMPLE. As an illustration we take $s_2 < 2q$ and $A_3 = 1$, $A_2 = t$, and we suppose that $n = 0$. Then if A_1 is irreductible we have :

$$2\deg(R_2) \geq \deg(R_1R_2) \geq (\ell m - q^2)s_2 + 2q^2.$$

Let us take $\ell m = q(q-1)$ and write $s_2 = 2q - d$, we have :

$$2\deg(R_2) \geq -q(2q-d) + 2q^2 = qd$$

so $\deg(R_2) \geq 1$ and one of the polynomials $A_1 + \lambda_2 t + \mu_3$ has at least one root in $\mathbb{F}_{q^2}$ and, therefore, is reducible if $\deg A_1 > 2$ (note that we can choose it with a non null constant term).

5. Generalization

We will only study generalizations of the two applications of last paragraph.

We consider n linear forms $\varphi_i(X_1, \ldots, X_{r+1}) \in \mathbb{F}_q[X_1, \cdots, X_{r+1}]$ and we denote by $P(X_1, \ldots, X_{r+1})$ the polynomial :

$$P(X_1, \ldots, X_{r+1}) := X_1X_2 \ldots X_{r+1}\varphi_1(X_1, \ldots, X_{r+1}) \cdots \varphi_n(X_1, \ldots, X_{r+1})$$

We suppose there exist r polynomials $A_1, \ldots, A_{r+1}$ in $\mathbb{F}_q[t]$, linearly independent over $\mathbb{F}_q$, such that

$$A_1, \ldots, A_{r+1},\ \varphi_1(A_1, \ldots, A_{r+1}), \ldots, \varphi_n(A_1, \ldots, A_{r+1})$$

are pairwise prime in $\mathbb{F}_q[t]$.

Let $R_1, R_2, \ldots, R_r$ the rational radicals of $P(A_1, \ldots, A_r)$ over $\mathbb{F}_q, \mathbb{F}_{q^2}, \ldots, \mathbb{F}_{q^r}$ respectively, then we have.

APPLICATION 5. *Suppose the above conditions verified and :*

$$\deg A_1 = \ldots = \deg A_{r+1} = \deg \varphi_i(A_1, \ldots, A_{r+1}) = s$$

except for at most 2 values of i. Then we have :

$$\deg(R_1 \ldots R_r) \geq s(n + r - q - q^2 - \cdots - q^r) + rq^r + \cdots + q$$

with $s = \sup(\deg A_1, \ldots, \deg A_{r+1})$.

Proof - We write :

$$B_{-r} = A_1,\quad B_{-r+1} = A_2, \ldots, B_0 = A_{r+1},\quad B_i = \varphi_i(A_1, \ldots, A_{r+1})$$

for $1 \leq i \leq n$.

We consider the Wronskians :

$$W_{i_0,\ldots,i_r} = \begin{vmatrix} B_{i_0}, & B_{i_1} & \ldots & B_{i_r} \\ D^{(1)}B_{i_0}, & D^{(1)}B_{i_1} & \ldots & D^{(1)}B_{i_r} \\ \ldots & \ldots & \ldots & \ldots \\ D^{(r)}B_{i_0}, & D^{(r)}B_{i_1} & \ldots & D^{(r)}B_{i_r} \end{vmatrix}$$

Our hypotheses show that for any $k \in \{1, \ldots, n\}$ there are $i_0, \ldots, i_{r-1}$ in $\{-r, \ldots, 0\}$ such that :

$$W_{i_0,\ldots,i_{r-1},k} \neq 0$$

Moreover we know (Wronskian criterion) that all non null $W_{i_0,\dots,i_r}$ are associated in $\mathbb{F}_q[t]$.

Let us denote by $v_\alpha(S)$ the order of a polynomial S at a root α of $R_1 \dots R_r$. Again theorem 4 implies that if $\nu \geq \dfrac{r}{\deg(\alpha)}$ we have :

$$\nu_\alpha[P(A_1,\dots,A_r)] - \nu_\alpha(R_1 \cdots R_r) \leq \nu_\alpha(W_{i_0,\dots,i_r})$$

for all non null $W_{i_0,\dots,i_r}$. Finally if $\nu < \dfrac{r}{\deg(\alpha)}$ the left hand side is negative and the inequality is still valid. So we get :

$$\deg P(A_1,\dots,A_r) - \deg(R_1 \cdots R_r) \leq \deg(W_{i_0,\dots,i_{r-1},k})$$

The last step is the calculation of the degree of the right hand side.

If all the factors of $P(A_1,\dots,A_r)$ are of the same degree s, we get :

$$\deg(RHS) \leq s + q(s-1) + q^2(s-2) + \cdots + q^r(s-r)$$

so :

$$\deg(R_1 \cdots R_r) \geq (s+r+1)n - [s + q(s-1) + \cdots + q^r(s-r)]$$

The two remaining cases can be treated in exactly the same fashion as in application 3. ∎

APPLICATION 6. *Suppose $A_1,\dots,A_{r-1}$ are such that :*

$$s_r = \deg A_1 > s_{r-1} = \deg A_2 > \dots > s_0 = \deg A_{r+1}$$

and set :

$$P(A_1,\dots,A_{r+1}) = A_{r+1} \prod_{\lambda_i^{(1)}} (A_1 + \lambda_2^{(1)} A_2 + \cdots + \lambda_{r+1}^{(1)} A_{r+1}) \prod_{\lambda_i^{(2)}} (A_2 + \lambda_3^{(r)} A_3 + \cdots + \lambda_{r+1}^{(r)} A_{r+1})$$

$$\cdots \prod_{\lambda_i^{(r)}} (A_r + \lambda_{r+1}^{(r)} A_{r+1})$$

with pairwise factors.

Then we have :

$$\deg(R_1 \cdots R_r) \geq (\ell_2^{(1)} \cdots \ell_{r+1}^{(1)} - q^r) s_r + \cdots + (\ell_{r+1}^{(r)} - q) s_1 + r q^r + \cdots + q$$

where $\ell_i^{(j)}$ denotes the number of $\lambda_i^{(j)}$ in the above expression of $P(A_1,\dots,A_{r+1})$.

Proof – Since $A_1,\dots,A_{r+1}$ have decreasing degrees, they are $\mathbb{F}_q$–linearly independent, and the Wronskian criterion implies

$$W = \begin{vmatrix} A_1,\dots,A_{r+1} \\ D^{(1)}A_1,\dots,D^{(1)}A_{r+1} \\ \dots\dots\dots\dots \\ D^{(r)}A_1,\dots,D^{(r)}A_{r+1} \end{vmatrix} \neq 0$$

Now, as in the proof of application 5, we see that $\dfrac{P(A_1,\dots,A_{r+1})}{R_1 \dots R_r}$ divides W.

So, as in application 4, we are led to calculate the degree of W which is :

$$q^r(s_r - r) + q^{r-1}(s_{r-1} - (r-1)) + \dots + s_0.$$

Now we have :

$$\deg P(A_1,\dots,A_{r+1}) = \ell_2^{(1)} \cdots \ell_{r+1}^{(1)} s_r + \ell_3^{(2)} \cdots \ell_{r+1}^{(3)} s_{r-1} + \cdots + \ell_{r+1}^{(r)} s_1 + s_0$$

so we get the required minoration. ∎

EXAMPLE. We take $s_r < rq$ and $A_{r+1} = 1, \ldots, A_2 = t^{r-1}$, and we suppose that $\ell_i^{(j)} = 0$ for $j \geq 2$. Then if A_1 is irreductible we have :

$$r \deg(R_r) \geq \deg(R_1 \cdots R_r) \geq (\ell_2^{(1)} \cdots \ell_{r+1}^{(1)} - q^r)s_r + rq^r$$

Let us take $\ell_2^{(1)} \cdots \ell_{r+1}^{(1)} = q^{r-1}(q-1)$ and write $s_r = rq - d$, we have :

$$r \deg(R_r) \geq -q^{r-1}(rq - d) + rq^r = q^{r-1}d$$

so $\deg(R_r) \geq 1$ and one of the polynomials $A_1 + \lambda_2^{(1)} t^{r-1} + \cdots + \lambda_{r+1}^{(1)}$ has at least are root in $\mathbb{F}_{q^r}$ and, therefore, si reducible if $r < \deg A_1 < rq$ (note that we can choose it with a non null constant term).

6. References

1. Y. Hellegouarch, *Un analogue d'un théorème d'Euler*, C.R. Acad. Sci. Paris, Ser. I, Math **313**, (1991), p. 155-158.
2. Y. Hellegouarch, *Galois calculus and Carlitz exponentials*, in The Arithmetic of Functions Fields, Walter de Gruyter, (1992), 33-50.
3. Y. Hellegouarch, *Analogues en caractéristique p d'un théorème de Mason*, C.R. Acad. Sci. *Paris Ser. I Math.* **325** (1991) no. 2, 141–144.
4. R. Liouville, *Sur l'impossibilité de la relation algébrique* $X^n + Y^n + Z^n = 0$, C.R. Acad. Sci. Paris, 87, (1879), 1108-1110.
5. D. Goss, *Basic structures of function field arithmetic*, Springer, (1996).
6. J. Oesterlé, *Nouvelles approches du "théorème de Fermat"* in séminaire Bourbaki, (1987/1988), 165-186.

DEPARTEMENT DE MATHEMATIQUES ET MECANIQUE
Esplanade de la Paix
14032 CAEN CEDEX
FRANCE

This page intentionally left blank

Contemporary Mathematics
Volume **225**, 1999

Composition behaviour of sub-linearised polynomials over a finite field

Marie Henderson* and Rex Matthews

ABSTRACT. Sub-linearised polynomials are natural "twists" of linearised polynomials. It is shown that a decomposable sub-linearised polynomial can be written as the composition of sub-linearised polynomials. Other results connect the decomposition of sub-linearised and linearised polynomials.

1. Introduction

Let $q = p^e$ where p is a prime and denote by $\mathbb{F}_q$ the finite field of order q. Further, $\overline{\mathbb{F}}_q$ shall denote the algebraic closure of $\mathbb{F}_q$ and $\mathbb{F}_q^*$ the set of non-zero elements of $\mathbb{F}_q$. A polynomial $L \in \mathbb{F}_q[X]$ of the form

$$L(X) = \sum_{i=0}^{n} a_i X^{p^i}$$

is called a *linearised polynomial.* Linearised polynomials satisfy $L(X+Y) = L(X)+L(Y)$ and have been studied widely, see [**6**, Chapter 3].

A polynomial $f \in \mathbb{F}_q[X]$ which represents a permutation of the elements of $\mathbb{F}_q$ is called a *permutation polynomial* of $\mathbb{F}_q$. For example, a linearised polynomial L is a permutation polynomial on $\mathbb{F}_q$ if and only if it has the single root $x = 0$ in $\mathbb{F}_q$. This is easily seen from the additive property of linearised polynomials. For a positive integer s a *p^s-polynomial* is a linearised polynomial where $a_i = 0$ for each i not divisible by s. It follows that every linearised polynomial is a p-polynomial.

If $g, f \in \mathbb{F}_q[X]$ then the composition of g and f will be given by $g(f) = g \circ f$. Clearly, the composition of two p^s-polynomials is again a p^s-polynomial. We will call the polynomials g, f *composition factors* of $g \circ f$. Further, g will be referred to as a *left composition factor* and f as a *right composition factor.* A polynomial g for which there are no polynomials $f_1, f_2 \in \mathbb{F}_q[X]$ satisfying $g = f_1(f_2)$ and degree$(f_i) > 1$ is called *indecomposable.*

In Section 3 we present new results on the composition behaviour of the sub-linearised polynomials (the definition of a sub-linearised polynomial is in Section 3). In particular, we show that if a sub-linearised polynomial decomposes, then it may be written as the composition of sub-linearised polynomial and all other

1991 *Mathematics Subject Classification.* 11T06.

* This author was partially supported by the Australian Research Council.

decompositions are related to the sub-linearised one. This is revealed in Theorem 3.3. It will be shown that the sub-linearised polynomial behaviour mimics the linearised polynomial behaviour. In fact, in the final section we will show that the composition behaviour of certain subgroups of sub-linearised polynomials and the associated linearised polynomials are connected (Theorem 4.1). Linearised polynomials are considered first as this work forms a framework for the sub-linearised results which follow.

2. Composition behaviour of linearised polynomials

In [5] counterexamples were provided to the statement: If $f \in \mathbb{F}_q[X]$ is indecomposable, then it is indecomposable over $\overline{\mathbb{F}}_q$. The validity of this statement was questioned by Cohen in [4]. We note that a method of finding counterexamples to this statement had already been supplied in 1933 by Ore [7]. It was shown in [7] that every linearised polynomial will decompose into compositions of polynomials of the form $X^p - \alpha X$ in some extension field of $\mathbb{F}_q$. Hence any indecomposable linearised polynomial of degree larger then p must decompose over $\overline{\mathbb{F}}_q$. We generalise Ore's result in the next theorem. The proof is omitted as it is similar to the proof described in [7]. The result demonstrates how a composition factor of the form $X^{p^s} - \alpha X$ can be found.

THEOREM 2.1. *The p^s-polynomial $L \in \mathbb{F}_q[X]$, with degree > 1, given by*

$$L(X) = \sum_{i=0}^{k} a_i X^{p^{si}}$$

has a right composition factor of $X^{p^s} - \alpha X$ if and only if α is a solution of the equation

$$a_k y^{(p^{ks}-1)/(p^s-1)} + \cdots + a_2 y^{(p^{2s}-1)/(p^s-1)} + a_1 y + a_0 = 0. \tag{1}$$

From this theorem we deduce the following two natural conclusions.

COROLLARY 2.2. *Let $L \in \mathbb{F}_q[X]$ be a p^s-polynomial with degree > 1. Then L may be written as a composition of p^s-polynomials of the form $X^{p^s} - \alpha X$ over an extension field of $\mathbb{F}_q$.*

Note that any such decomposition is not necessarily unique as it depends on the solution α selected.

COROLLARY 2.3. *Let $L \in \mathbb{F}_q[X]$ be a linearised polynomial with degree > 1. If L is indecomposable over $\overline{\mathbb{F}}_q$ then L is of the form $X^p + \alpha X$.*

We can find a similar condition for a p^s-polynomial L to have a left composition factor of the form $X^{p^s} - \alpha X$. However, the equation that α must satisfy for this case is not as simple or as useful having no direct connection to other properties of L. In [7] a necessary and sufficient condition for a p-polynomial to have a left composition factor of $X^p - \alpha X$ was given. In his proof Ore raises the resulting equations to the power p^{-1}. However positive powers of p are used instead to obtain our result.

LEMMA 2.4. *The p^s-polynomial, with degree > 1, given by*

$$L(X) = \sum_{i=0}^{k} a_i X^{p^{si}} \in \mathbb{F}_q[X],$$

has a left composition factor of $X^{p^s} - \alpha X$ *if and only if* α *is a solution of the equation*

$$a_0^{p^{ks}} + y^{p^{ks}} a_1^{p^{(k-1)s}} + \cdots + y^{p^{ks}+\cdots+p^s} a_k = 0.$$

Recall that a polynomial $f \in \mathbb{F}_q[X]$ has simple roots if and only if f and the derivative of f are relatively prime. Therefore a linearised polynomial has simple roots provided the coefficient of X is non-zero. The next lemma is a slight generalisation of Lemma 3.50 of [**6**]. We do not include a proof.

LEMMA 2.5. *Let* L *be a* p^s*-polynomial over* $\mathbb{F}_q$ *with degree* > 1. *Let* $\mathbb{F}_{q^k}$ *contain the roots of* L. *Then* $L(X) = X^{p^{sm}} \circ L_1(X)$ *and* $L(X) = L_2(X) \circ X^{p^{sm}}$ *where the first non-zero coefficient of* L *is the coefficient of* $X^{p^{sm}}$. *In addition,* L_1 *and* L_2 *are both* p^s*-polynomials and have simple roots. The roots of* L *form a linear subspace of* $\mathbb{F}_{q^k}$ *where* $\mathbb{F}_{q^k}$ *is regarded as a vector space over* $\mathbb{F}_p$.

Evidently, to investigate indecomposable linearised polynomials other than X^p, we need only consider those linearised polynomials which have simple roots.

LEMMA 2.6. *Let* $L \in \mathbb{F}_q[X]$ *be a linearised polynomial with degree* > 1. *If* L *is indecomposable over* $\mathbb{F}_q$ *then either* $L(X) = X^p - \alpha X$ *for some* $\alpha \in \mathbb{F}_q$ *or* L *is a permutation polynomial of* $\mathbb{F}_q$ *with simple roots.*

PROOF. We only have to find a decomposition of those L, with degree $< p$, that do not permute $\mathbb{F}_q$. In (1) the solution α that we seek is a $(p^s - 1)$th power of a non-zero root of L. So L will have $X^{p^s} - \beta^{(p^s-1)}X$ as a right composition factor if and only if there exists a $\beta \in \mathbb{F}_q^*$ satisfying $L(\beta) = 0$. Hence any polynomial L of degree p^k, $k > 1$, which is not a permutation polynomial of $\mathbb{F}_q$, will decompose in this way. □

Suppose that the linearised polynomial L does decompose over $\mathbb{F}_q$. Then the next lemma, proven by Cohen in [**1**], restricts the possible composition factors that L can have.

LEMMA 2.7. *Suppose the linearised polynomial* L *decomposes over* $\mathbb{F}_q$ *with* $L = f_1(f_2)$. *Then* $L = f_1'(f_2')$ *where* $f_1'(X) = f_1(X) + f_1(f_2(0))$, $f_2'(X) = f_2(X) - f_2(0)$ *and* f_1' *and* f_2' *are linearised polynomials.*

So if L does decompose over $\mathbb{F}_q$, then it may be written as the composition of linearised polynomials.

3. Composition behaviour of Sub-linearised Polynomials

Let L be a p^s-polynomial and $d > 1$ a divisor of $p^s - 1$. Then $L(X) = XM(X^d)$ for some $M \in \mathbb{F}_q[X]$. The polynomial $S(X) = XM^d(X)$ is called a *sub-linearised polynomial* or (p^s, d)*-polynomial* and satisfies $S(X^d) = L^d(X)$. Such a polynomial S will be referred to as the (p^s, d)-polynomial *associated* with L. Let ζ be a dth root of unity in $\mathbb{F}_q$. Then there are $gcd(d, q-1)$ p^s-polynomials $\zeta^j L$ which satisfy $S(X^d) = (\zeta^j L(X))^d$ for each (p^s, d)-polynomial S. We may avoid confusion by selecting L to be the p^s-polynomial associated with S as constant factors will not affect composition behaviour.

Sub-linearised polynomials were introduced by Cohen in [**3**] with conditions for these polynomials to be permutation polynomials given. These conditions were improved upon in [**2**]: the sub-linearised polynomial S is a permutation polynomial

of $\mathbb{F}_q$ if and only if S has the single root $x = 0$ in $\mathbb{F}_q$. We start this section with the following simple connection between the composition of linearised and sub-linearised polynomials of a particular form. Notice that the monomial $X^{p^{sm}}$ is both a p^s-polynomial and a (p^s, d)-polynomial.

LEMMA 3.1. *Let $L \in \mathbb{F}_q[X]$ be a p^s-polynomial and S be the associated (p^s, d)-polynomial. Suppose $L(X) = X^{p^{sm}} \circ L_1(X)$ and $L(X) = L_2(X) \circ X^{p^{sm}}$ for $L_1, L_2 \in \mathbb{F}_q[X]$. Then $S(X) = X^{p^{sm}} \circ S_1(X)$ and $S(X) = S_2(X) \circ X^{p^{sm}}$ where $S_i^d(X) = L_i(X^d)$.*

PROOF. Let $L(X) = XM(X^d)$ for some $M \in \mathbb{F}_q[X]$ so that $S(X) = XM^d(X)$. Suppose $L(X) = X^{p^{sm}} \circ L_1(X)$. From Lemma 2.7 L_1 is a p^s-polynomial and so has the form $L_1(X) = \sum_{i=0}^{n} a_i X^{p^{si}}$, where $a_i \in \mathbb{F}_q$. Further, L_1 has associated (p^s, d)-polynomial S_1 given by

$$S_1(X) = X\left(\sum_{i=0}^{n} a_i X^{(p^{si}-1)/d}\right)^d.$$

Using L_1 we now have

$$L(X) = X^{p^{sm}} \circ L_1(X) = \sum_{i=0}^{n} a_i^{p^{sm}} X^{p^{s(m+i)}}.$$

We may determine from L that

$$S(X) = X\left(\sum_{i=0}^{n} a_i^{p^{sm}} X^{(p^{s(m+i)}-1)/d}\right)^d.$$

Consider the composition of (p^s, d)-polynomials given by

$$X^{p^{sm}} \circ S_1(X) = X^{p^{sm}}\left(\sum_{i=0}^{n} a_i^{p^{sm}} X^{p^{sm}(p^{si}-1)/d}\right)^d = X\left(\sum_{i=0}^{n} a_i^{p^{sm}} X^{(p^{s(m+i)}-1)/d}\right)^d.$$

This is precisely the (p^s, d)-polynomial S and so $S(X) = X^{p^{sm}} \circ S_1(X)$ as required. The proof of the second case is similar. □

Consequently, if the sub-linearised polynomial $S(X) \neq X^p$ is indecomposable, then the coefficient of X must be non-zero.

LEMMA 3.2. *Let S_1 and S_2 be (p^s, d)-polynomials in $\mathbb{F}_q[X]$. Then $S_1(S_2)$ is a (p^s, d)-polynomial in $\mathbb{F}_q[X]$.*

PROOF. Let M_1 and M_2 be the polynomials in $\mathbb{F}_q[X]$ satisfying $S_i(X) = XM_i^d(X)$, $i = 1, 2$. Let L_1 and L_2 be the p^s-polynomials given by $L_i(X) = XM_i(X^d)$, $i = 1, 2$. Now

$$S_1\big(S_2(X)\big) = XM_2^d(X)M_1^d\big(XM_2^d(X)\big) = XM^d(X)$$

where $M(X) = M_2(X)M_1\big(XM_2^d(X)\big)$. If we can show that $XM(X^d)$ is a p^s-polynomial, then $XM^d(X)$ is indeed a (p^s, d)-polynomial. By substituting we have

$$XM(X^d) = XM_2(X^d)M_1\big(X^dM_2^d(X^d)\big) = L_1\big(L_2(X)\big).$$

As the composition of two p^s-polynomials is again a p^s-polynomial, $S_1(S_2)$ is a (p^s, d)-polynomial. □

In Lemma 3.2 we have shown that $L_1(L_2)$ is the p^s-polynomial associated with $S_1(S_2)$. We will come back to this point in Section 4. Next we consider the possible decomposition factors that a sub-linearised polynomial can have. The following theorem is motivated by Lemma 2.7.

THEOREM 3.3. *Let S be a (p^s, d)-polynomial which decomposes over $\mathbb{F}_q$ with $S = f_1(f_2)$ for some $f_1, f_2 \in \mathbb{F}_q[X]$. Then $S = f_1'(f_2')$ where $f_1'(X) = f_1\big(X + f_2(0)\big)$, $f_2'(X) = f_2(X) - f_2(0)$ and f_1' and f_2' are (p^r, d)-polynomials where r divides s.*

PROOF. We only have to show that f_1 and f_2 are (p^r, d)-polynomials where $f_2(0) = 0$. Otherwise we could look at $f_1'(f_2')$, as $S = f_1(f_2) = f_1'(f_2')$ and $f_2'(0) = 0$. We can also assume that S has a non-zero coefficient of X which means the associated p^s-polynomial L has simple roots. Otherwise, from Lemma 3.1, we could look at the polynomial S_1, where $S(X) = X^{p^{sm}} \circ S_1(X)$ and the coefficient of $X^{p^{sm}}$ is the first non-zero coefficient of S.

Firstly, we shall deal with the polynomial f_2. As S is a (p^s, d)-polynomial, there must be a p^s-polynomial L such that $L^d(X) = S(X^d)$. Then

$$L^d(X) - L^d(Y) = S(X^d) - S(Y^d) = f_1\big(f_2(X^d)\big) - f_1\big(f_2(Y^d)\big)$$

so that $f_2(X^d) - f_2(Y^d)$ must divide $L^d(X) - L^d(Y)$. Let ζ be a primitive dth root of unity. As d divides $p^s - 1$

$$\begin{aligned} L^d(X) - L^d(Y) &= \prod_{i=0}^{d-1} L(X) - \zeta^i L(Y) \\ &= \prod_{i=0}^{d-1} L(X - \zeta^i Y). \end{aligned}$$

As $f_2(X^d) - f_2(Y^d)$ divides $L^d(X) - L^d(Y)$ this polynomial may be written as the product

$$f_2(X^d) - f_2(Y^d) = \prod_{i=0}^{d-1} t_i(X - \zeta^i Y),$$

where $t_i(X - \zeta^i Y)$ divides $L(X - \zeta^i Y)$. Suppose t_k is the polynomial of maximum degree among the t_i. As $f_2(X^d) - f_2(Y^d)$ is invariant under the mapping $\tau : Y \mapsto \zeta Y$, the image of $t_k(X - \zeta^k Y)$ is also a factor of $f_2(X^d) - f_2(Y^d)$. So $t_i = t_k = t$ for $i = 0, \ldots, d-1$ and

$$f_2(X^d) - f_2(Y^d) = \prod_{i=0}^{d-1} t(X - \zeta^i Y).$$

By making the substitution $Y = 0$, then $f_2(X^d) = t^d(X)$ and it remains to show that $t(X)$ is linearised. We know that

$$t^d(X) - t^d(Y) = \prod_{i=0}^{d-1} t(X) - \zeta^i t(Y) = \prod_{i=0}^{d-1} t(X - \zeta^i Y).$$

Let Ω_t be the set of roots of t. Then

$$t(X - Y) = \prod_{\alpha \in \Omega_t} (X - Y - \alpha).$$

We will show that each factor $(X - Y - \alpha)$ divides $t(X) - t(Y)$. Suppose that $(X - Y - \alpha')$ divides $t(X) - \zeta^i t(Y)$ for some i where $1 \leq i \leq d-1$. Replacing Y by $X - \alpha'$ then $t(X) - \zeta^i t(X - \alpha')$ must be the zero polynomial, yet this has leading coefficient $(1 - \zeta^i)$ which is not zero, a contradiction. Hence $i = 0$ and all of the factors $(X - Y - \alpha)$ where $\alpha \in \Omega_t$ must divide $t(X) - t(Y)$. By comparing the degrees then $t(X) - t(Y) = t(X - Y)$ so t is linearised.

The polynomial f_1 will now satisfy $L^d(X) = f_1\big(t^d(X)\big)$. Let Ω_f be the set of non-zero roots of f_1. Hence

$$f_1(X) = X^r \prod_{\beta \in \Omega_f} (X - \beta)$$

where $\beta \neq 0$. Then

$$f_1\big(t^d(X)\big) = t^{rd}(X) \prod_{\beta \in \Omega_f} \big(t^d(X) - \beta\big).$$

Recall that $t(X)$ divides $L(X)$. As L has simple roots t can not have any repeated factors. Thus each factor of $h(X) = t^d(X) - \beta$ has no repeated linear factors as $h(X)$ and the derivative of $h(X)$ are relatively prime. If Ω_L is the set of roots of L then

$$L(X) = \prod_{\alpha \in \Omega_L} (X - \alpha).$$

Each factor $(X - \alpha)$ of L must divide d distinct factors of $h(X)$. This means that the roots in Ω_f may be grouped together into sets of d equal factors in Ω and

$$L^d(X) = \left(t^r(X) \prod_{\beta \in \Omega} \big(t(X) - \beta\big)\right)^d = g^d\big(t(X)\big)$$

for some $g \in \mathbb{F}_q[X]$. Thus $L(X) = \zeta^j g\big(t(X)\big)$ where $j \in \mathbb{Z}$ and as both L and t are linearised polynomials g must also be linearised.

As t is linearised, it has the shape $t(X) = \sum_{i=0}^{n} a_i X^{p^{mi}}$ for some largest choice of $m \in \mathbb{Z}$. This choice of m guarantees that there exist integers n_1 and n_2 where $1 \leq n_1, n_2 \leq n$, a_{n_1} and a_{n_2} are non-zero and $gcd(n_1, n_2) = 1$ so that $gcd(p^{mn_1} - 1, p^{mn_2} - 1) = p^m - 1$. Also the polynomial $t(X)$ must have simple roots as $t(X)$ divides $L(X)$ so a_0 is non-zero. Because $f_2(X^d) = t^d(X)$ then $t^d(X)$ is a polynomial in X^d. Now

$$t^d(X) = X^d \left(\sum_{i=0}^{n} a_i X^{(p^{mi}-1)}\right)^d$$

and in particular the terms $\sum_{i=1}^{n} a_i X^{(p^{mi}-1)}$ have non-zero coefficient da_0^{d-1}. Each of these terms must be of the form $(X^d)^r$ for some $r \in \mathbb{Z}$. Thus d divides $p^{mi} - 1$ for $1 \leq i \leq n$ and for our choice of m we have d divides $p^m - 1$. Hence $t(X)$ is a p^m-polynomial where d divides $p^m - 1$.

By a similar argument the polynomial $g(X)$ is a p^k-polynomial where d divides $p^k - 1$. In fact both t and g are p^r-polynomials where $r = (m, k)$ and d divides $p^r - 1$. As $\zeta^j g(t(X)) = L(X)$ then r divides s and L is also p^r-polynomial. We may now conclude that f_1, f_2 and S are (p^r, d)-polynomials as each must satisfy $f_1(X^d) = g^d(X)$, $f_2(X^d) = t^d(X)$ and $S(X^d) = L^d(X)$ respectively. □

Hence, if a (p^s, d)-polynomial S decomposes, then it can be written as the composition of (p^r, d)-polynomials where r divides s. Note that the polynomial S is itself a (p^r, d)-polynomial. This behaviour imitates the behaviour of the linearised polynomials, see Lemma 2.7. We can use Theorem 3.3 and results from Section 2 to obtain results for sub-linearised polynomials. This is precisely what we shall now proceed to do for the remainder of this section.

THEOREM 3.4. *Let $S \in \mathbb{F}_q[X]$ be a (p^s, d)-polynomial and $L(X) = \sum_{i=0}^{k} a_i X^{p^{si}}$ an associated p^s-polynomial. Then S has a right composition factor of the form*

$$X(X^{(p^s-1)/d} - \alpha)^d$$

over $\mathbb{F}_q$ if and only if α is a solution of the equation

$$a_k y^{(p^{ks}-1)/(p^s-1)} + \cdots + a_2 y^{(p^{2s}-1)/(p^s-1)} + a_1 y + a_0 = 0$$

or equivalently, L has a right composition factor of $X^{p^s} - \alpha X$.

PROOF. If α is a solution of the above equation, then from Theorem 2.1 L has a right composition factor of $X^{p^s} - \alpha X$. Hence $L(X) = L_1(X) \circ (X^{p^s} - \alpha X)$ where $L_1(X) = XM_1(X^d)$ is also a p^s-polynomial. Consider the composition

$$L_1(X) \circ (X^{p^s} - \alpha X) = X(X^{(p^s-1)} - \alpha) M_1\big(X^d (X^{(p^s-1)} - \alpha)^d\big).$$

This must also equal $XM(X^d)$. Therefore

$$M(X) = (X^{(p^s-1)/d} - \alpha) M_1\big(X(X^{(p^s-1)/d} - \alpha)^d\big).$$

Using this identity

$$\begin{aligned} S(X) &= XM^d(X) \\ &= X(X^{(p^s-1)/d} - \alpha)^d M_1^d\big(X(X^{(p^s-1)/d} - \alpha)^d\big) \\ &= XM_1^d(X) \circ (X(X^{(p^s-1)/d} - \alpha)^d) \end{aligned}$$

and we have the desired decomposition.

Suppose that $S(X) = S_1(X) \circ X(X^{(p^s-1)/d} - \alpha)^d$ for some $S_1 \in \mathbb{F}_q[X]$. From Theorem 3.3 S_1 is a (p^s, d)-polynomial so $S_1(X) = XM_1^d(X)$ for some $M_1 \in \mathbb{F}_q[X]$ and $L_1(X) = XM_1(X^d)$ is a p^s-polynomial. By reversing the steps in the first part of the proof then $L(X) = L_1(X) \circ (X^{p^s} - \alpha X)$. From Theorem 2.1 this can happen if and only if α is a solution of the given equation. □

From the above theorem we see that if the p^s-polynomial L is not a permutation polynomial of $\mathbb{F}_q$, then the associated (p^s, d)-polynomial S will decompose in the way described in the theorem. This provides us with a method of constructing more counterexamples relevant to the introductory discussion of Section 2.

COROLLARY 3.5. *Let $S \in \mathbb{F}_q[X]$ be a (p^s, d)-polynomial with degree > 1. Then S may be written as a composition of (p^s, d)-polynomials of the form*

$$X(X^{(p^s-1)/d} - \alpha)^d$$

over an extension field of $\mathbb{F}_q$.

COROLLARY 3.6. *Let $S \in \mathbb{F}_q[X]$ be a (p^s, d)-polynomial with degree > 1. If S is indecomposable over $\overline{\mathbb{F}}_q$ then S has the form $X(X^{(p^s-1)/d} - aX)^d$ where d divides $p^s - 1$ but d does not divide $p^t - 1$ for any integer $t < s$.*

PROOF. Let d be a fixed divisor of $p^s - 1$. Then any (p^s, d)-polynomial of $\mathbb{F}_q$ of the form $X(X^{(p^s-1)/d} - \alpha)^d$ can not be obtained through the composition of (p^s, d)-polynomials over $\mathbb{F}_q$. If it did decompose as (p^s, d)-polynomials then they would all have degree $< p^s$ and the only such polynomial is X.

Suppose d divides $p^t - 1$ for some $0 < t < s$ then $X(X^{(p^s-1)/d} - \alpha)^d$ will decompose further over $\overline{\mathbb{F}}_q$. To see this put $r = gcd(t, s)$ and let L be a p^s-polynomial associated with $S(X) = X(X^{(p^s-1)/d} - \alpha)^d$. If d divides $(p^t - 1)$ then d divides $gcd(p^s - 1, p^t - 1) = p^r - 1$. As $r|s$ then L is a p^r-polynomial and S is the (p^r, d)-polynomial associated with L. From Corollary 3.5 S must decompose over $\overline{\mathbb{F}}_q$ into (p^r, d)-polynomials of the form $X(X^{(p^r-1)/d} - \beta)^d$ where $\beta \in \overline{\mathbb{F}}_q$. We have already seen that $X(X^{(p^s-1)/d} - \alpha)^d$ is indecomposable as (p^s, d)-polynomials and so from Theorem 3.3 it is indecomposable over $\overline{\mathbb{F}}_q$ if no such integer t exists. □

We summarise our findings concerning indecomposable sub-linearised polynomials with the next theorem.

THEOREM 3.7. *Let $S \in \mathbb{F}_q[X]$ be a sub-linearised polynomial with degree > 1. If S is indecomposable over $\mathbb{F}_q$ then either $S(X) = X(X^{(p^s-1)/d} - \alpha)^d$ where d does not divide $p^t - 1$ for any integer t less than s or the associated p^s-polynomial L has simple roots and is a permutation polynomial of $\mathbb{F}_q$.*

Of course, we can also find left composition factors of (p^s, d)-polynomials of the form $X(X^{(p^s-1)/d} - \alpha)^d$. We omit the proof as it is similar to the proof of Theorem 3.4 using Lemma 2.4 instead of Theorem 2.1.

THEOREM 3.8. *Let $S \in \mathbb{F}_q[X]$ be a (p^s, d)-polynomial and $L(X) = \sum_{i=0}^{k} a_i X^{p^{si}}$ an associated p^s-polynomial. Then $X(X^{(p^s-1)/d} - \alpha)^d$ is a left composition factor of S if and only if α is a solution of the equation*

$$a_0^{p^{ks}} + y^{p^{ks}} a_1^{p^{(k-1)s}} + \cdots + y^{p^{ks}+\cdots+p^s} a_k$$

or equivalently, L has a left composition factor of $X^{p^s} - \alpha X$.

Finally we combine the conclusions of Lemma 3.2 and Theorem 3.3 to gain a precise description of when the composition of two sub-linearised polynomials is again a sub-linearised polynomial.

THEOREM 3.9. *Let S_1 be a (p^s, d_1)-polynomial and S_2 be (p^t, d_2)-polynomial, both in $\mathbb{F}_q[X]$. Then $S_1(S_2)$ is a (p^k, d)-polynomial for some $k \in \mathbb{Z}$ if and only if $d_1 = d_2 = d$.*

PROOF. Assume $d_1 = d_2 = d$ and put $k = gcd(s, t)$. Then d divides $(p^k - 1)$ and both S_1 and S_2 are (p^k, d)-polynomials. From Lemma 3.2 we have $S_1(S_2)$ is also a (p^k, d)-polynomial. Conversely, suppose $S_1(S_2)$ is a (p^k, d)-polynomial. Then from Theorem 3.3 as it decomposes over $\mathbb{F}_q$ it can be written as the composition of (p^r, d)-polynomials, where r divides k. In fact, as S_2 is sub-linearised, then $S_2(0) = 0$ and from Theorem 3.3 the polynomials S_1, S_2 and $S_1(S_2)$ must be (p^r, d)-polynomials. Hence $d = d_1 = d_2$. □

4. A connection

We now turn our attention to the promised connection between the composition behaviour of p^s-polynomials and (p^s, d)-polynomials.

THEOREM 4.1. *Let $L_1, L_2 \in \mathbb{F}_q[X]$ be p^s-polynomials with associated (p^s, d)-polynomials $S_1, S_2 \in \mathbb{F}_q[X]$ respectively. Then $L_1^d(L_2(X)) = S_1(S_2(X^d))$. Let $L \in \mathbb{F}_q[X]$ be a p^s-polynomial with associated (p^s, d)-polynomial S. Then $L = L_1(L_2)$ for p^r-polynomials L_1 and L_2, where r divides s and d divides $p^r - 1$, if and only if $S = S_1(S_2)$ for (p^r, d)-polynomials S_1 and S_2 where $L_i^d(X) = S_i(X^d)$, $i = 1, 2$.*

PROOF. The first part follows easily by applying the fact that $L^d(X) = S(X^d)$ for associated p^s and (p^s, d)-polynomials. Suppose $L = L_1(L_2)$ for some p^r-polynomials $L_1, L_2 \in \mathbb{F}_q[X]$ where r divides s and d divides $p^r - 1$. Then L_1 and L_2 have associated (p^r, d)-polynomials S_1 and S_2 respectively which satisfy $L_i^d(X) = S_i(X^d)$, $i = 1, 2$. In the proof of Lemma 3.2 we showed that $S_1(S_2)$ is the (p^r, d)-polynomial associated with $L = L_1(L_2)$. The converse follows using a similar argument. □

This is a useful connection as it shows that the composition behaviour of the (p^s, d)-polynomials for a fixed d is entirely dependent on the composition behaviour of their associated p^s-polynomials. Consequently, we may determine the composition of two (p^s, d)-polynomials by calculating the composition of the associated p^s-polynomials and then determining the (p^s, d)-polynomial associated with this composition. Also, two (p^s, d)-polynomials commute with respect to composition precisely when their associated p^s-polynomials commute. The condition being that all of the coefficients lie in $\mathbb{F}_{p^s}$. It is probable that there are other implications and applications of this connection.

References

1. S.D. Cohen, *The irreducibility of compositions of linear polynomials over a finite field*, Compositio Math. **47** (1982), 149–152.
2. ———, *Exceptional polynomials and the reducibility of substitution polynomials*, L'Enseignement Math. **36** (1990), 53–65.
3. ———, *The factorable core of polynomials over finite fields*, J. Austral. Math. Soc. Ser. A **49** (1990), 309–318.
4. ———, *Permutation polynomials and primitive permutation groups*, Arch. Math. **57** (1991), 417–423.
5. M.D. Fried, R. Guralnick, and J. Saxl, *Schur covers and Carlitz's conjecture*, Isr. J. Math. **82** (1993), 157–225.
6. R. Lidl and H. Niederreiter, *Finite Fields*, Encyclopedia Math. Appl., vol. 20, Addison-Wesley, Reading, 1983, (now distributed by Cambridge University Press).
7. O. Ore, *On a special class of polynomials*, Trans. Amer. Math. Soc. **35** (1933), 559–584, Errata, *ibid.* **36**, 275 (1934).

SCHOOL OF INFORMATION TECHNOLOGY, THE UNIVERSITY OF QUEENSLAND, QUEENSLAND 4072, AUSTRALIA

E-mail address: marie@csee.uq.edu.au

SCHOOL OF INFORMATION TECHNOLOGY, THE UNIVERSITY OF QUEENSLAND, QUEENSLAND 4072, AUSTRALIA

Current address: 179 Melville street, West Hobart 7000, Australia

E-mail address: galois@hilbert.maths.utas.edu.au

This page intentionally left blank

Contemporary Mathematics
Volume **225**, 1999

KERNELS AND DEFAULTS

PHILIPPE LANGEVIN AND PATRICK SOLÉ

ABSTRACT. We consider the metric space of the set of boolean functions from a space over the field with two elements provided of the Hamming distance. The non-linearity of a boolean function is equal to its distance from the space of affine boolean functions. The functions having maximal non-linearity are called the bent functions. In this paper, we generalize the well known notions of kernels and defaults of the theory of quadratic forms, and we apply these notions to the study of the non-linearity of the cubic functions.

1. BOOLEAN FUNCTIONS

Let E be a space of finite dimension m over the finite field $\mathbb{F}_2$. The set of functions from E into $\mathbb{F}_2$ is denoted by ${\mathbb{F}_2}^E$, an element of ${\mathbb{F}_2}^E$ is a *boolean function.* Let f be a boolean function, the set $\{x \in E \mid f(x) = 1\}$ is the *support* of f, it is denoted by $\mathrm{supp}(f)$. Conversely, for any subset X of E, the *indicating* function 1_X is the unic boolean function whose support is X. With the operations inherited of the field $\mathbb{F}_2$, the set of boolean function is a $\mathbb{F}_2$-algebra isomorphic to the algebra of subsets of E with the operations Δ and $\cap$. If $x_1, x_2, \ldots, x_m$ is any basis of the dual of E then the map sending a polynomial p of $\mathbb{F}_2[X_1, X_2, \ldots, X_m]$ to the boolean function $p(x_1, x_2, \ldots, x_m)$ defines an epimorphism of algebras which the kernel is the ideal generated by the polynomials $X_i^2 - X_i$. Hence, the algebra ${\mathbb{F}_2}^E$ is isomorphic to the quotient $\mathbb{F}_2[X_1, X_2, \ldots, X_m]/(X_1^2 - X_1, X_2^2 - X_2, \ldots, X_m^2 - X_m)$. The *degree* of a boolean function f, denoted by $\deg(f)$, is the smallest integer k such that f has an antecedent of degree k by the morphism above. This definition does not depend on the choice of the basis, moreover

Proposition 1. *The space* $\mathrm{RM}(k, m)$ *of boolean functions of degree at most* k *is generated by the indicating functions of the supports of the affine varieties of codimension* k. *In other words, if* f *has degree less than* k *then there exits* N *affine varieties of codimension* k V_1, V_2, ..., V_N *such that* $f = \sum_{i=1}^{N} 1_{V_i}$.

Proof. This is a result by Delsarte [3]. One can see it as a consequence of the fact that the Reed-Muller codes are the only codes invariant under the action of the general affine group, see also [11]. □

The *weight* of f, denoted by $\mathrm{wt}(f)$, is equal to the cardinality of the support of f. The *Hamming distance* between two function f and g is the weight of $f + g$. The minimal distance between f and any affine function from E into

Key words and phrases. boolean functions, Reed-Muller codes, covering radius **94B75**.

$\mathbb{F}_2$ is the *non-linearity* of f, that is :

$$\delta(f) = \inf_{\phi} \mathrm{wt}(f + \phi).$$

The maximal value of $\delta(f)$, when f ranges the set of boolean function, is the *covering radius* of the first order Reed-Muller code. It is denoted by $\rho(m)$, a function with non-linearity $\rho(m)$ is a *bent* function. These functions have a great importance for cryptographic applications, see [14, 6].

2. Characters

Let $(a, b) \mapsto a.b$ be a symmetric non-degenerate bilinear symmetric form. Let χ be the non trivial additive character of the field $\mathbb{F}_2$: $\chi(0) = 1$ and $\chi(1) = -1$. The set of boolean functions is embedded in the set of complex function by the mapping $f \mapsto f_\chi$, where $f_\chi(x) = \chi(f(x)) = (-1)^{f(x)}$. The *Fourier transform* of the complex function h is the complex function defined by

$$\hat{h}(a) = \sum_{x \in E} h(x)\chi(a.x).$$

Par abus de langage, we say that $\widehat{f_\chi}$ is the Fourier transform of f. The relation :

$$\mathrm{wt}(f(x) + a.x + b) = 2^{m-1} - \frac{\chi(b)}{2}\widehat{f_\chi}(a), \tag{1}$$

shows that $\delta(f) = 2^{m-1} - \frac{1}{2}\|\widehat{f_\chi}\|_\infty$. This last equality justifies the definition of *spectral radius* of the set of affine functions, that is :

$$R(m) = \min_{f \in \mathbb{F}_2{}^E} \|\widehat{f_\chi}\|_\infty, \tag{2}$$

so that $\rho(m) = 2^{m-1} - \frac{1}{2}R(m)$.

For any complex function h, we have :

$$\sum_{a \in E} \hat{h}(a)\overline{\hat{h}(a)} = 2^m \sum_{a \in E} h(a)\overline{h(a)} \tag{3}$$

this is the famous Plancherel-Parseval identity. Its leads to the estimate

$$R(m) \leq 2^{\frac{m}{2}} \tag{4}$$

3. Quadrics

Let q be a quadratic form, that is a boolean function satisfying

$$q(x + y) = q(x) + q(y) + \phi(x, y), \tag{5}$$

where ϕ is a symetric bilinear form, the bilinear form associated to q. One defines the kernel and the default of q. [5] The kernel of q is the subspace $\ker(q) = \{x \in E \mid \phi(x, y) = 0, \quad \forall y \in E\}$; Clearly, the restriction of q to its kernel is a linear form, and the default of q is the intersection $\ker(q) \cap \mathrm{supp}(q)$. Let us denote by k the dimension of the kernel of q. A straigthforward calculation show that, for any vector a in E, we have :

$$\left(\widehat{q_\chi}(a)\right)^2 = 2^m \sum_{z \in \ker(q)} \chi(a.z) = \begin{cases} 2^{m+k}, & \text{si } a \perp \ker(q); \\ 0, & \text{sinon.} \end{cases} \tag{6}$$

On an other hand, we know that a non degenerate quadratic form has a kernel of dimension 0 if m is even, and dimension 1 if m is odd. Hence, we get the estimation

$$2^{\frac{m}{2}} \leq R(m) \leq 2^{\lceil \frac{m}{2} \rceil} \tag{7}$$

which is an equality if m is even. When m is odd, the exact value of $R(m)$ is known for $m = 3, 5, 7$, see [12] and [9]. Since the paper of Paterson and Wiedeman [13], we know that there exists a boolean function of RM(8, 155) which the Fourier transform has norm 216, consequently, for any odd m greater than 15 , we have :

$$R(m) \leq 216 \times 2^{\frac{m-15}{2}} = \frac{27}{32} 2^{\lceil \frac{m}{2} \rceil} \tag{8}$$

Conjecture 1. *The spectral radius $R(m)$ is equivalent to $2^{\frac{m}{2}}$.*

Let k be an integer, $0 \leq k \leq m$. We define the spectral radius of the function of degree less or equal than k by $R_k(m) = \inf_{\deg(f) \leq k} \|\hat{f}\|_\infty$. The goal of that paper is to present new notions in order to study $R_3(m)$. We believe that the number of cubic functions is great enough to conjecture :

Conjecture 2. *The spectral radii $R(m)$ and $R_3(m)$ are asymptotically equivalent.*

Note that, $R_3(m) = R_2(m)$ holds for m less or equal to 13, see [9] and [10].

4. Kernel and defaults

In this section, we generalize the notions of kernel and default of the above section. Let v be a vector of ${\mathbb{F}_2}^m$ and let f be a boolean function. The derivation of f in the direction of v is the boolean function $x \mapsto D_v f(x) = f(x+v) + f(x)$. If V is a system of r vectors, say $\{v_1, v_2, \ldots, v_r\}$, then the derivation in the direction of the system V is the composition $D_{v_1} \circ D_{v_2} \circ \cdots \circ D_{v_r}$. The map $V \mapsto D_V f(0)$ is a particular case of the combinatorial polarization of H. Ward [15]. If the vectors of V are linearly dependent then $D_V f$ is equal to zero, else it is equal to the convolutional product of f by the indicating function of the support of the subspace S of ${\mathbb{F}_2}^m$ generated by V : $D_V f(x) = 1_S * f(x)$; that is the derivation of f in the direction of S, introduced by Dillon in [6]. For any vector v , we have :

$$D_v(\sum_S a_S 1_S) = \sum_S a_S \, d(v, S) \, 1_{(v+S) \cup S} \tag{9}$$

where the S's are affine spaces, and $d(v, S)$ is equal to 1 if and only if v does not lie in the direction of S. .

Proposition 2. *Let f be a boolean function; Then*

$$\forall v \in E, \quad \deg(D_v f) \leq \deg(f) - 1, \quad et \quad \exists v \in E \quad \deg(D_v f) = \deg(f) - 1$$

Proof. Note that is v is not in the direction of S then the codimension of $(v + S) \cup S$ is equal to the codimension of S minus 1, the first point is a consequence of 1. For the second point, we may assume that, the variable x_1 appears in a monomial of degree $\deg(f)$. Hence, f reads $g(x_2, x_3, \ldots, x_m) +$

$x_1 h(x_2, x_3, \ldots, x_m)$ where h is a function of degree $\deg(f) - 1$, which proves the result since $D_{e_1} f = h$. □

Let r be an integer. We define the map $\lambda^{(r)}$ which transforms the boolean function f defined on ${\mathbb{F}_2}^m$ in the boolean function defined over ${\mathbb{F}_2}^{mr}$ by :

$$\lambda^{(r)}(f)[x_1, x_2, \ldots, x_r] = \sum_{\lambda_1, \lambda^{(2)}, \ldots, \lambda^{(r)}} f\Big(\sum_{i=1}^{r} \lambda_i x_i\Big) = D_{\{v_1, v_2, \ldots, v_r\}} f(0)$$

Proposition 3. *The restriction of $\lambda^{(r)}$ to $\mathrm{RM}(r, m)$ is onto $\Lambda^r(E)$, its kernel is $\mathrm{RM}(r-1, m)$.*

Proof. Indeed, the proposition above shows that $x \mapsto D_{\{v_1, v_2, \ldots, v_r\}} f(x)$ is constant. □

When the degree of f is equal to r, the map $\lambda^{(r)}(f)$ is a r-linear map; That is [2] the multilinear form associate to f. We define the kernel and the default of f as in the degree 2 case :

$$\ker(f) = \{(x_1, x_2, \ldots, x_{r-1}) \mid \lambda^{(r)}(f)[x_1, x_2, \ldots, x_r] = 0, \quad \forall x_r \in E\}$$

$$\mathrm{def}(f) = \{(x_1, x_2, \ldots, x_{r-1}) \mid \lambda^{(r-1)}(f)[x_1, x_2, \ldots, x_{r-1}] = 1\}$$

The cardinality of $\ker(f)$ and $\mathrm{def}(f)$ are respectively denoted by $k(f)$ and $d(f)$. These numbers are affine numerical invariants : for any affine transformation T, we have

$$k(f) = k(f \circ T), \qquad \text{et} \qquad d(f) = d(f \circ T),$$

which comes from the equality, $D_v(f \circ T) = (D_{\theta(v)} f) \circ T$, where θ is the linear map associate to the affine map T. For example, let $1 \leq i, j, k \leq m$ be three distinct integers, and consider the monomial function $x_i x_j x_k$. Its multilinear form is not zero, so that is a lift of the determinant function of the space generated by e_i, e_j and e_k.

$$\lambda^{(3)}(x_i x_j x_k)[x, y, z] = \det_{i,j,k}(x, y, z) = \begin{pmatrix} x_i & y_i & z_i \\ x_j & y_j & z_j \\ x_k & y_k & z_k \end{pmatrix} \tag{10}$$

It follows that for any quadratic function $q \in \mathrm{RM}(2, 3)$, the function $x_1 x_2 x_3 + q(x)$ of $\mathrm{RM}(3, 3)$ has no default.

5. Cubics

In [1] C. Carlet proposes to study the non-linearity of a boolean function by means of the hight order moments of its fourier transform. For example, he gives the inequality :

$$\sum_{a \in E} \big(\widehat{f_\chi}(a)\big)^4 \geq 2^{3m},$$

which is satisfied by any boolean function. The equality occurs if and only if f is bent and m is even. In this section, we study the links between the kernel and the moments of order 4 of the Fourier transform of a cubic. We begin by two simple fact about the trilinear form of a cubic.

It is easy to check that the trilinear form of the cubic f satisfies

$$\lambda^{(3)}(f)[x,y,z] = \lambda^{(2)}(f)[x,y] + D_{x,y}f(z). \tag{11}$$

Which leads to the main formula of this paper,

Proposition 4. *If f is a boolean function of degree 3 then*

$$\sum_{a\in E} \big(\widehat{f_\chi}(a)\big)^4 = 2^{2m}\big(k(f) - 2d(f)\big),$$

Proof. Indeed,

$$\begin{aligned}
\sum_{a\in E} \big(\widehat{f_\chi}(a)\big)^4 &= 2^m f_\chi * f_\chi * f_\chi * f_\chi(0) \\
&= 2^m \sum_{x+y+z+t=0} \chi\big(f(x)+f(y)+f(z)+f(t)\big) \\
&= 2^m \sum_{x,y,z} \chi\big(f(x)+f(y)+f(z)+f(x+y+z)\big) \\
&= 2^m \sum_{x,y,z} \chi\big(f(x+z)+f(y+z)+f(z)+f(x+y+z)\big) \qquad (12) \\
&= 2^m \sum_{x,y,z} \big(\lambda^{(3)}(f)[x,y,z] + \lambda^{(2)}(f)[x,y]\big) \\
&= 2^{2m} \sum_{(x,y)\in \ker(f)} \big(\lambda^{(2)}(f)[x,y]\big) \\
&= 2^{2m}\big(k(f) - 2d(f)\big)
\end{aligned}$$

□

We say that a boolean function exceeds the quadratic bound if its nonlinearity is greater than the non-linearity of any quadratic function. Of course, this notion takes sense only is the case of odd m. From [8] and [10], we know that if m is less or equal than 13 then the cubics do not exceed the quadratic bound.

Proposition 5. *Let f be a boolean function of degree 3 such that $k(f) - 2d(f) \geq 2^{m+1}$ then f does not exceed the quadratic bound.*

Proof. That is a consequence of the following trick about meanings. Let $(a_i)_{1\leq i\leq n}$ be a sequence of n positive real numbers. Let μ be the meaning of the a_i's, and let ν be the meaning of the $(a_i)^2$'s. If $\nu > 2\mu^2$ then there exist i such that $a_i \geq 2\mu$. Indeed, $\frac{1}{n}\sum_{i=1}^n (a_i - \mu)^2 = \nu - \mu^2$, and there exists i such that $|a_i - \mu| > \mu$, since $a_i \geq 0$, we get $a_i > 2\mu$. □

Note that if f has no default then $k(f) - 2d(f) = k(f) \geq 32^m - 2$, so :

Corollary 1. *If f is cubic without default then f does not exceed the quadratic bound.*

This result was obtained in [11] but only for $m \leq 19$. The proposition 4 shows that in order to construct cubics far from the first order Reed-Muller code, we have to construct cubics f doing $k(f) - 2d(f)$ small.

6. Bounds

Let f be a boolean function of degree 3. The ordered pair $(x, y) \in {\mathbb{F}_2}^m \times {\mathbb{F}_2}^m$ is in the kernel of f if and only if y is in the kernel of the quadratic function $D_x f$. Let us denote by $r(x)$ the dimension of the kernel of the quadratic form $D_x f$. We have,

$$|\ker(f)| = \sum_{x \in E} 2^{r(x)}. \tag{13}$$

Proposition 6. *Assume that m is even. If f is a boolean function of degree 3 then the kernel of f contains at least $5 \times 2^m - 4$ elements.*

Proof. One remarks that the kernel of $D_x f$ contains x. Hence, $r(x) \geq 2$ since $r(x)$ and m have the same parity. □

Proposition 7. *Assume m odd. If f is a boolean function of degree 3 then the kernel of f contains at least $3 \times 2^m - 2$ elements.*

Proof. idem. □

In the next section, we will see that these bound are reached when $m = 3$ and $m = 6$. The above estimate must be compared with some results of Goethals about the space of quadratic forms, [4, 7]. For any odd integer m, there exists a space of dimension m of quadratic forms of rank 0 or $m - 1$. For example, the space of quadratic forms $x \mapsto \mathrm{Tr}_{{\mathbb{F}_2}^m/\mathbb{F}_2}\left(ax^{2^t} + (ax)^{2^{t+1}}\right)$, where $a \in {\mathbb{F}_2}^m$.

Problem 1. *Let τ be a trilinear alternate form. We have a natural map from E into $\Lambda^2(E)$ which sends $a \in E$ on a bilinear form. Let $r(a)$ be the rank of the image of a. What can we say about $\sum_{a \in E} 2^{r(a)}$ when τ varies ?*

Problem 2. *Let f be a boolean function. From proposition 1, we know that f decomposes as $\sum_{S \in X} 1_S$ where X is a set of affine subspaces. Let x and y be two vectors of E. The derivation of f in the direction of $\{x, y\}$ is $D_{x,y}(f) = \sum_{S \in X} d(x, y, S) 1_{S(x,y)}$ where $S(x, y)$ is the affine space $S \cup (x + S) \cup (y + S) \cup (x + y + S)$, and where $d(x, y, S) \in \mathbb{F}_2$ is equal to 0 if and only if the direction of S contains al least one vector of x, y or $x + y$. Use this description to construct a set X of variety of codimension 3 in order to obtain a cubic with small kernel.*

7. Numerical Results

The next tables give all the values of kernel, and default for all the cubic functions, $4 \leq m \leq 7$. Kernels and defaults are affine invariant, so we use the action of the general linear group $GL(m, \mathbb{F}_2)$ on the space of boolean cubics modulo the space of quadratic functions to reduce the problem of enumeration. In the paper [9], one can find systems of representatives for small m. For each representative h, there is a three columns table. Let us denote by k be the cardinality of the kernel of h. When q ranges the space of the homogeneous quadratic functions $\ker(h + q)$ is invariant, the value of k appears in the header of the table. A row (d, δ, c) means that there are c homogeneous quadratic functions q with d defaults, and δ is to $k - 2d$: the quantity that appears in the RHS of (12). Note that if f is a boolean

function of degree more than 2 then its kernel and default do not depend of the affine terms.

$m = 4$, $k = 88$, h_1			$m = 4$, $k = 88$, h_2		
24	40	56	24	40	56
0	88	8	24	40	56

$m = 5$, $k = 352$, h_1			$m = 5$, $k = 184$, h_3		
132	88	512	60	64	192
144	64	336	48	88	480
96	160	168	36	112	320
0	352	8	0	184	32

$m = 6$, $k = 1408$, h_1			$m = 6$, $k = 736$, h_3		
528	352	3584	336	64	192
624	160	25088	288	160	23520
672	64	1344	96	544	32
576	256	2352	240	256	8192
384	640	392	192	352	480
0	1408	8	144	448	320
			0	736	32

$m = 6$, $k = 316$, h_6			$m = 6$, $k = 484$, h_4			$m = 6$, $k = 400$, h_5		
84	148	7680	168	148	10752	168	64	64
60	196	21504	144	196	18816	120	160	15680
36	244	3584	96	292	3136	96	208	14336
			0	484	64	72	256	2240
						24	352	448

$m = 7$, $k = 5632$, h_1			$m = 7$, $k = 760$, h_{12}		
2640	352	917504	240	280	32256
2112	1408	17920	216	328	516096
2496	640	376320	192	376	959616
2688	256	772800	168	424	368640
2304	1024	11760	0	760	128
1536	2560	840	96	568	16128
0	5632	8	144	472	204288

$m = 7$, $k = 2944$, h_3			$m = 7$, $k = 928$, h_{10}		
1104	736	32768	168	592	6144
1248	448	512000	216	496	92160
1296	352	983040	312	304	284672
1344	256	450624	264	400	632832
1152	640	93600	336	256	3072
384	2176	96	288	352	801792
960	1024	24192	240	448	236288
768	1408	480	192	544	27648
576	1792	320	144	640	11776
0	2944	32	48	832	768

$m=7, k=1936, h_4$			$m=7, k=1600, h_5$			$m=7, k=1264, h_8$		
768	400	903168	672	256	161344	456	352	589824
672	592	111104	624	352	1376256	480	304	483840
816	304	903168	576	448	397824	384	496	225408
720	496	150528	480	640	26432	336	592	46080
576	784	18816	528	544	114688	288	688	18944
528	880	7168	384	832	17920	144	976	1024
384	1168	3136	288	1024	2240	192	880	768
0	1936	64	96	1408	448	0	1264	128
						432	400	731136

$m=7, k=2272, h_7$			$m=7, k=1264, h_6$			$m=7, k=928, h_9$		
1008	256	368640	480	304	645120	336	256	24576
960	352	999936	336	592	7680	288	352	1476608
912	448	645120	432	400	1290240	240	448	544768
768	736	40320	384	496	129024	144	640	28672
720	832	43008	240	784	21504	192	544	21504
0	2272	128	144	976	3584	0	928	1024

$m=7, k=592, h_{11}$		
120	352	983040
96	400	1024000
48	496	81920
0	592	8192

List of homogeneous cubics :

$h_1 = X_1X_2X_3$, $h_2 = X_1X_2X_3 + X_2X_3X_4$, $h_3 = X_1X_2X_3 + X_2X_4X_5$,
$h_4 = X_1X_2X_3 + X_4X_5X_6$, $h_5 = X_1X_2X_3 + X_2X_4X_5 + X_3X_4X_6$,
$h_6 = X_1X_2X_3 + X_1X_4X_5 + X_2X_4X_6 + X_3X_5X_6 + X_4X_5X_6$,
$h_7 = X_1X_2X_7 + X_3X_4X_7 + X_5X_6X_7$,
$h_8 = X_1X_2X_3 + X_4X_5X_6 + X_1X_4X_7$,
$h_9 = X_1X_2X_3 + X_2X_4X_5 + X_3X_4X_6 + X_1X_4X_7$,
$h_{10} = X_1X_2X_3 + X_4X_5X_6 + X_1X_4X_7 + X_2X_5X_7$,
$h_{11} = X_1X_2X_3 + X_1X_4X_5 + X_2X_4X_6 + X_3X_5X_6 + X_4X_5X_6 + X_1X_6X_7$,
$h_{12} = X_1X_2X_3 + X_1X_4X_5 + X_2X_4X_6 + X_3X_5X_6 + X_4X_5X_6 + X_2X_4X_7 + X_1X_6X_7$

References

[1] C. Carlet. Codes de reed-muller, codes de kerdock et de preparata. *Ph. D. thesis*, 1990.

[2] C. Carlet. A new generalization of bent functions to the odd case. *private communication*, 1997.

[3] P. Delsarte. A geometrical approach to a class of cyclic codes. *Journal of Combinatorial Theory*, 6:340–358, 1969.

[4] P. Delsarte and J.M. Goethals. Alternating bilinear forms over $gf(q)$. *Journal of combinatorial theory*, (A) 19:26–50, 1975.

[5] J. Dieudonné. *La géométrie des groupes classiques*. 1971.

[6] J. F. Dillon. Elementary hadamard difference sets. *Ph. D thesis*, 1974.

[7] J.M. Goethals. Nonlinear codes and quadratic forms. *Information and Control*, 31(1):43–75, 1976.

[8] X.D. Hou. On the covering radius of $r(1,m)$ into $r(3,m)$. *preprint.*
[9] X.D. Hou. $gl(m,2)$ acting on $r(r,m)/r(r-1,m)$. *Discrete Mathematics*, 149:99–122, 1996.
[10] Ph. Langevin. The covering radius of $r(1,9)$ in $r(3,9)$. *Lectures notes in computer sciences*, 514:51–61, 1990.
[11] Ph. Langevin. rayon de recouvrement des codes de reed-muller affines. *Ph. D Thesis*, 1992.
[12] J. J. Mykkelveit. The covering radius of the (128,8) reed-muller codes is 56. *IEEE transactions on information theory*, 26:359–362, 1980.
[13] N.J. Patterson and D.H. Wiedemann D.H. The covering radius of the $(2^{15},16)$ reed-muller code is at least 16276. *IEEE transactions on Inf. Theory*, 29:354–356, 1983.
[14] O.S. Rothaus. on bent functions. *Journal of Combinatorial Theory*, 20:300–305, 1976.
[15] Harold N. Ward. Combinatorial polarization. *Discrete Math.*, 26:185–197, 1979.

CNRS, I3S, BÂTIMENT 4, 250 RUE A. EINSTEIN, 06560 VALBONNE, FRANCE
E-mail address: langevin@alto.unice.fr, sole@alto.unice.fr

This page intentionally left blank

Contemporary Mathematics
Volume **225**, 1999

GLOBAL FUNCTION FIELDS WITH MANY RATIONAL PLACES AND THEIR APPLICATIONS [1]

HARALD NIEDERREITER AND CHAOPING XING

ABSTRACT. Global function fields with many rational places have been studied intensively in the last few years. Such function fields are of great theoretical interest and they also allow important applications to algebraic coding theory and the construction of low-discrepancy sequences. We present new results on narrow ray class extensions and alternative – and in a sense simpler – proofs of the recent asymptotic results of the authors which led to improvements on the Gilbert-Varshamov bound in coding theory. Tables of bounds for $N_q(g)$, the maximum number of rational places that a global function field with full constant field $\mathbf{F}_q$ and genus g can have, and for quality parameters of low-discrepancy sequences complement the paper.

1. Introduction

Let q be an arbitrary prime power and let K be a global function field with full constant field $\mathbf{F}_q$, i.e., an algebraic function field over $\mathbf{F}_q$ with $\mathbf{F}_q$ algebraically closed in K. We use the notation $K/\mathbf{F}_q$ if we want to emphasize the fact that $\mathbf{F}_q$ is the full constant field of K. By a *rational place* of K we mean a place of K of degree 1. We write $g(K)$ for the genus of K and $N(K)$ for the number of rational places of K. For fixed $g \geq 0$ and q we put

$$N_q(g) = \max N(K),$$

[1] 1991 *Mathematics Subject Classification.* Primary 11G20, 11R58, 14G15, 14H05, 94B27; Secondary 11G09, 11K38, 11T71, 94B65.

© 1999 American Mathematical Society

where the maximum is extended over all global function fields $K/\mathbf{F}_q$ with $g(K) = g$. Equivalently, $N_q(g)$ is the maximum number of $\mathbf{F}_q$-rational points that a smooth, projective, absolutely irreducible algebraic curve over $\mathbf{F}_q$ of given genus g can have. The calculation of $N_q(g)$ is a very difficult problem, so usually one has to make do with bounds for this quantity. A well-known general upper bound for $N_q(g)$ is the Weil-Serre bound

$$N_q(g) \leq q + 1 + g\lfloor 2q^{1/2} \rfloor, \tag{1}$$

where $\lfloor u \rfloor$ denotes as usual the greatest integer not exceeding the real number u.

Global function fields $K/\mathbf{F}_q$ of genus g with many rational places, that is, with $N(K)$ reasonably close to $N_q(g)$ or to a known upper bound for $N_q(g)$, have received a lot of attention in the literature. Quite a number of papers on the subject have also been written in the language of algebraic curves over finite fields. The first systematic account of the subject was given by Serre [26], and for recent surveys we refer to Garcia and Stichtenoth [2] and Niederreiter and Xing [19]. The construction of global function fields with many rational places, or equivalently of algebraic curves over $\mathbf{F}_q$ with many $\mathbf{F}_q$-rational points, is of great theoretical interest. Moreover, it is also important for applications in the theory of algebraic-geometry codes and in recent constructions of low-discrepancy sequences. We will say more about these two applications later in the paper.

Recent work of the authors [12], [14], [15], [17], [18], [21], [35], [36] has led to considerable progress in the construction of global function fields with many rational places, by means of techniques based on Drinfeld modules and narrow ray class extensions. The most involved part in these techniques is usually the calculation of the genus of the constructed function field. In Section 2 of this paper we establish a new general genus formula for a family of subfields of narrow ray class extensions that is widely used in the constructions above. The proof of this genus formula is based on ramification theory for local fields and the theory of conductors.

Section 3 of the paper discusses updated tables of lower and upper bounds for $N_q(g)$ reflecting all the recent work on this topic. In Section 4 we present recent results on the asymptotic behavior of $N_q(g)$ as $g \to \infty$ (with, in a sense, simpler proofs) and we show how these are employed to beat the Gilbert-Varshamov coding bound by means of algebraic-geometry codes (see also [20]). Applications of global function

fields with many rational places to the construction of low-discrepancy sequences and updated tables of relevant parameters are discussed in Section 5.

2. Genera and conductors of narrow ray class extensions

Let F be a global function field and K/F a finite abelian extension. For a place P of F we denote by $G_i(P; K/F), i \geq 0$, the ith ramification group of P in K/F. Let $a_P(K/F)$ be the least integer $k \geq 0$ such that $|G_i(P; K/F)| = 1$ for all $i \geq k$. We write $e_P(K/F)$ for the ramification index and $d_P(K/F)$ for the different exponent of P in K/F. We define the *conductor exponent* $c_P(K/F)$ of P in K/F by

$$c_P(K/F) = \frac{d_P(K/F) + a_P(K/F)}{e_P(K/F)}.$$

From the Hilbert different formula [27, p. 64] and the Hasse-Arf theorem [27, p. 76] we see that $c_P(K/F)$ is always a nonnegative integer. Note that $c_P(K/F) = 0$ if and only if P is unramified in K/F and that $c_P(K/F) \geq 2$ if and only if P is wildly ramified in K/F.

We use the ramification theory for local fields (see [27, Chapter IV]) to derive a formula for the different exponent $d_P(K/F)$ in the case where $c_P(K/F) \leq 2$. An interesting aspect of this formula is that it just depends on the value of $e_P(K/F)$. The following proof determines not only $d_P(K/F)$, but also the orders of all ramification groups of P in K/F.

THEOREM 1. *Let K/F be a finite abelian extension of global function fields and let P be a place of F with conductor exponent $c_P(K/F) \leq 2$. Write $e_P(K/F) = bp^l$, where p is the characteristic of F, b is an integer with $\gcd(b, p) = 1$, and l is a nonnegative integer. Then*

$$d_P(K/F) = 2e_P(K/F) - b - 1.$$

Proof. The case $l = 0$ of tame ramification is trivial, and so we can assume $l \geq 1$. We use the abbreviations $a = a_P(K/F), c = c_P(K/F), d = d_P(K/F), e = e_P(K/F)$, and $g_i = |G_i(P; K/F)|$ for $i \geq 0$. Since $d \geq e$ and $a \geq 1$, we have $c = 2$. Ramification theory yields $g_0 = e = bp^l$ and $g_1 = p^l$ (see [27, Section IV.2]). For $1 \leq r \leq l$ let n_r be the number of

$i \geq 1$ with $g_i = p^{l-r+1}$. The Hasse-Arf theorem shows that g_0 divides $\sum_{i=1}^{n_1} g_i = n_1 p^l$, and so b divides n_1. Furthermore, we have

$$\begin{aligned} a &= 1 + \sum_{r=1}^{l} n_r, \\ d &= e - 1 + \sum_{r=1}^{l} n_r \left(p^{l-r+1} - 1\right), \end{aligned}$$

the latter by the Hilbert different formula. From $c = 2$ we get

$$2e = d + a = e + \sum_{r=1}^{l} n_r p^{l-r+1},$$

hence

$$\sum_{r=1}^{l} n_r p^{l-r+1} = bp^l.$$

Since b divides n_1, we must have $n_1 = b, n_2 = \ldots = n_l = 0$, thus

$$d = e - 1 + b(p^l - 1) = 2e - b - 1. \quad \square$$

The second aim in this section is to study the conductor exponents in subextensions of narrow ray class extensions. The following general lemma on conductor exponents will be useful.

LEMMA 1. *Let $F \subseteq K \subseteq L$ be three global function fields with L/F being a finite abelian extension. Let P be a place of F and R a place of K lying over P. Then*

$$c_P(K/F) \leq c_P(L/F) \leq \max(c_P(K/F), c_R(L/K)).$$

Proof. For the proof of the first inequality we can assume that $e_P(K/F) > 1$. Put $c = c_P(L/F) \geq 1$ and $a = a_P(L/F) \geq 1$. Let φ and ψ be the functions defined in [27, p. 73] that are indexed by the extensions to which they belong. Note that by definition we have

$$\varphi_{L/F}(a-1) + 1 = \frac{1}{e_P(L/F)} \sum_{i=0}^{a-1} |G_i(P; L/F)| = c,$$

hence $\psi_{L/F}(c-1) = a-1$ since $\psi_{L/F}$ is the inverse function of $\varphi_{L/F}$. By Herbrand's theorem [27, p. 75] with $H = \mathrm{Gal}(L/K)$ and $v = \psi_{K/F}(c)$ we get

$$G_v(P; K/F) \simeq G_u(P; L/F)H/H, \tag{2}$$

where

$$u = \psi_{L/K}(v) = \psi_{L/K}(\psi_{K/F}(c)) = \psi_{L/F}(c)$$

by the transitivity of ψ (see [27, p. 74]). Moreover,

$$u > \psi_{L/F}(c-1) = a-1,$$

and so $u \geq a$. It follows that $|G_u(P; L/F)| = 1$, thus (2) implies $|G_v(P; K/F)| = 1$. Consequently,

$$a_P(K/F) \leq v = \psi_{K/F}(c),$$

and so

$$c_P(K/F) = \varphi_{K/F}(a_P(K/F) - 1) + 1 < \varphi_{K/F}(\psi_{K/F}(c)) + 1 = c + 1,$$

which shows the first inequality.

For the proof of the second inequality we can assume that $e_P(L/F) > 1$. If $H = \mathrm{Gal}(L/K)$ as above, then we have

$$G_i(R; L/K) = G_i(P; L/F) \cap H \quad \text{for all } i \geq 0. \tag{3}$$

Let $c \geq 1$ and $a \geq 1$ be as above and put

$$m = \max(c_P(K/F), c_R(L/K)).$$

Suppose first that

$$|G_{a-1}(R; L/K)| > 1.$$

Then $a - 1 \leq a_R(L/K) - 1$, and so

$$\begin{aligned} c &= \varphi_{L/F}(a-1) + 1 \leq \varphi_{L/F}(a_R(L/K) - 1) + 1 \\ &= \varphi_{K/F}(\varphi_{L/K}(a_R(L/K) - 1)) + 1, \end{aligned}$$

where we used the transitivity of φ (see [27, p. 74]) in the last step. Therefore

$$c \leq \varphi_{K/F}(c_R(L/K) - 1) + 1 \leq \varphi_{K/F}(m-1) + 1 \leq m.$$

In the remaining case we have

$$|G_{a-1}(R; L/K)| = 1.$$

Then by Herbrand's theorem with $j = \varphi_{L/K}(a-1)$ we get

$$G_j(P; K/F) \simeq G_{a-1}(P; L/F)H/H$$

$$\simeq G_{a-1}(P; L/F)/(G_{a-1}(P; L/F) \cap H) = G_{a-1}(P; L/F),$$

where we used (3) in the last step. From $|G_{a-1}(P; L/F)| > 1$ it follows that

$$\varphi_{L/K}(a-1) = j \leq a_P(K/F) - 1.$$

By applying the transitivity of φ, we conclude that

$$\begin{aligned} c &= \varphi_{L/F}(a-1) + 1 = \varphi_{K/F}(\varphi_{L/K}(a-1)) + 1 \\ &\leq \varphi_{K/F}(a_P(K/F) - 1) + 1 = c_P(K/F) \leq m, \end{aligned}$$

and so the second inequality is shown. □

Now we recall the definition of narrow ray class extensions (see [6, Section 7.5], [7, Section 16]). Let $F/\mathbf{F}_q$ be a global function field with $N(F) \geq 1$ and distinguish a rational place ∞ of F. Let H_∞ be the *Hilbert class field* of F with respect to ∞, that is, H_∞ is the maximal unramified abelian extension of F (in a fixed separable closure of F) in which ∞ splits completely. By [23] we have $\mathrm{Gal}(H_\infty/F) \simeq \mathrm{Div}^0(F)$, the group of divisor classes of F of degree 0, so that in particular $[H_\infty : F] = h(F)$, the divisor class number of F. Now let A be the ∞-integral ring of F and let ϕ be a sign-normalized Drinfeld A-module of rank 1. By [7, Section 15] we can assume that ϕ is defined over H_∞, i.e., that for each $y \in A$ the $\mathbf{F}_q$-endomorphism ϕ_y is a polynomial in the Frobenius with coefficients from H_∞. If $\overline{H_\infty}$ is a fixed algebraic closure of H_∞ and M is a nonzero integral ideal of A, then we write Λ_M for the A-submodule of $\overline{H_\infty}$ consisting of the M-division points. Let $E_M := H_\infty(\Lambda_M)$ be the subfield of $\overline{H_\infty}$ generated over H_∞ by all elements of Λ_M. Then E_M/F is called the *narrow ray class extension* of F with modulus M. The field E_M is independent of the specific choice of the sign-normalized Drinfeld A-module ϕ of rank 1. Furthermore, E_M/F is a finite abelian extension with

$$\mathrm{Gal}(E_M/F) \simeq \mathrm{Pic}_M(A) := \mathcal{I}_M(A)/\mathcal{P}_M(A),$$

where $\mathcal{I}_M(A)$ is the group of fractional ideals of A that are prime to M and $\mathcal{P}_M(A)$ is the subgroup of principal fractional ideals that are generated by elements $z \in F$ with $z \equiv 1 \bmod M$ and $\mathrm{sgn}(z) = 1$ (here sgn is the given sign function). We have $\mathrm{Gal}(E_M/H_\infty) \simeq (A/M)^*$, the group of units of the ring A/M.

In the following we use the standard identification between places of F and prime ideals of A. For an arbitrary place Q of an arbitrary

global function field K we write ν_Q for the normalized discrete valuation corresponding to Q.

In the next two lemmas we study the conductor exponents for (subextensions of) narrow ray class extensions. These results may be part of the folklore, but we have been unable to find proofs in the literature. Since the proofs are not entirely trivial, we provide the details here.

LEMMA 2. *Let $P \neq \infty$ be a place of F and E_M/F the narrow ray class extension of F with modulus $M = P^n, n \geq 1$. Then $c_P(E_M/F) = n$.*

Proof. Let Q be a place of H_∞ lying over P. We use some standard facts about narrow ray class extensions with a modulus of the form $M = P^n$ (see [15], [36] for convenient summaries). First of all, Q is totally ramified in E_M/H_∞, and so we have the ramification index

$$e_Q(E_M/H_\infty) = |(A/M)^*| = (q^d - 1)q^{d(n-1)},$$

where d is the degree of P. Furthermore, by the proof of [36, Proposition 2] we get the different exponent

$$d_Q(E_M/H_\infty) = n(q^d - 1)q^{d(n-1)} - q^{d(n-1)}.$$

The A-module Λ_M is cyclic and it thus has a generator $\lambda \in \Lambda_M$. If R is the place of E_M lying over Q, then $\nu_R(\lambda) = 1$. Now take a Galois automorphism $\sigma \in \mathrm{Gal}(E_M/H_\infty) \simeq (A/M)^*$ that is not the identity. Then $\sigma = \sigma_{bA}$ with $b \in A$, $\mathrm{sgn}(b) = 1, \nu_P(b) = 0$, and $b \not\equiv 1 \bmod M$, and we have

$$\nu_R(\sigma(\lambda) - \lambda) = \nu_R(\sigma_{bA}(\lambda) - \lambda) = \nu_R(\phi_b(\lambda) - \lambda) = \nu_R(\phi_{b-1}(\lambda)).$$

If $t \in A$ is a uniformizer at P, then it is shown as in [36, Lemma 5] that

$$\nu_R(\phi_{t^k}(\lambda)) = q^{dk} \quad \text{for } k \geq 0.$$

Thus, if $y \in A$ with $\nu_P(y) = k \geq 0$, then

$$\nu_R(\phi_y(\lambda)) = q^{dk}.$$

Since $\nu_P(b-1) \leq n-1$, this yields

$$\nu_R(\sigma(\lambda) - \lambda) = \nu_R(\phi_{b-1}(\lambda)) \leq q^{d(n-1)}.$$

It follows then from [28, Proposition III.8.6] that with $i = q^{d(n-1)}$ we have $|G_i(Q; E_M/H_\infty)| = 1$. On the other hand, by choosing b such that $\nu_P(b-1) = n-1$, we see that $|G_{i-1}(Q; E_M/H_\infty)| > 1$, and so

$$a_Q(E_M/H_\infty) = q^{d(n-1)}.$$

By combining the above results, we see that $c_Q(E_M/H_\infty) = n$, and since the extension H_∞/F is unramified, we obtain $c_P(E_M/F) = n$ by Lemma 1 and the obvious inequality $c_P(E_M/F) \geq c_Q(E_M/H_\infty)$. □

LEMMA 3. *Let $M = \prod_{j=1}^{r} P_j^{n_j}$ be a nontrivial integral ideal of A, where $P_1, \ldots, P_r$ are distinct places of F different from ∞ and $n_1, \ldots, n_r$ are positive integers. Then for any subfield K of the narrow ray class extension E_M/F of F with modulus M we have*

$$c_{P_j}(K/F) \leq n_j \quad \text{for } 1 \leq j \leq r.$$

Proof. Note that E_M is the composite of the fields E_{M_j} with $M_j = P_j^{n_j}$ for $1 \leq j \leq r$. Therefore from Lemmas 1 and 2 and the fact that the places of E_{M_j} lying over P_j are unramified in the extension E_M/E_{M_j} we get

$$c_{P_j}(E_M/F) = n_j \quad \text{for } 1 \leq j \leq r.$$

Another application of Lemma 1 yields the desired result. □

The result of Lemma 3 can be conveniently expressed by using the notion of conductor. In general, if K/F is an arbitrary finite abelian extension of global function fields, then the *conductor* $\mathrm{Cond}(K/F)$ of K/F is defined to be the divisor

$$\mathrm{Cond}(K/F) = \sum_P c_P(K/F)P$$

of F, where the sum is over all places P of F. If K/F is now as in Lemma 3 and we introduce the divisor $D(M) = \sum_{j=1}^{r} n_j P_j$ of F, then by Lemma 3 we have

$$\mathrm{Cond}(K/F) \leq D(M) + \infty.$$

Here we used the additional fact that the place ∞ is tamely ramified in E_M/F, and thus in K/F, by the theory of narrow ray class extensions.

Let K/F again be an arbitrary finite abelian extension of global function fields, let P_0 be a place of F that is unramified in K/F, and let B be the P_0-integral ring of F. Then the *conductor ideal* $C_B(K/F)$ of K/F in B is defined by

$$C_B(K/F) = \prod_{P \neq P_0} P^{c_P(K/F)},$$

where the product is over all places $P \neq P_0$ of F (or over all nonzero prime ideals of B). This is clearly a nonzero integral ideal of B. In the

following succinctly stated consequence of Lemma 3 we can include the trivial ideal $M = A$.

COROLLARY 1. *If K is a subfield of an arbitrary narrow ray class extension E_M/F such that ∞ is unramified in K/F, then the conductor ideal $C_A(K/F)$ divides the modulus M.*

Theorem 1 and the concept of the conductor ideal can be combined to provide a genus formula for certain extension fields, in particular for a family of subfields of narrow ray class extensions.

THEOREM 2. *Let K/F be an arbitrary finite abelian extension of global function fields, let P_0 be a place of F that is unramified in K/F, and let B be the P_0-integral ring of F. Furthermore, let $P_1, \ldots, P_r$ be distinct places of F different from P_0. If the conductor ideal $C_B(K/F)$ divides $\prod_{j=1}^{r} P_j^2$, then*

$$g(K) = 1 + [K : F](g(F) - 1) + [K : F] \sum_{j=1}^{r} \left(1 - \frac{b_j + 1}{2e_j}\right) \deg(P_j),$$

where $e_j = e_{P_j}(K/F)$ and b_j is the p-free part of e_j for $1 \leq j \leq r$, with p being the characteristic of F.

Proof. By the assumptions, the only possible ramified places in K/F are $P_1, \ldots, P_r$ and the corresponding different exponents are given by Theorem 1. The rest follows from the Hurwitz genus formula. □

COROLLARY 2. *Let K be any subfield of the narrow ray class extension E_M/F of F with modulus M dividing $\prod_{j=1}^{r} P_j^2$, where $P_1, \ldots, P_r$ are distinct places of F different from ∞. Then*

$$g(K) = 1 + [K : F](g(F) - 1) + [K : F] \sum_{j=1}^{r} \left(1 - \frac{b_j + 1}{2e_j}\right) \deg(P_j)$$

$$+ [K : F] \left(\frac{1}{2} - \frac{1}{2e_\infty}\right),$$

where $e_j = e_{P_j}(K/F)$ and b_j is the p-free part of e_j for $1 \leq j \leq r$, with p being the characteristic of F, and where $e_\infty = e_\infty(K/F)$.

Proof. Proceed as in the proof of Theorem 2 and use Lemma 3 as well as the fact that ∞ is tamely ramified in E_M/F, and so in K/F. □

3. Tables for $N_q(g)$

At the end of the paper we provide two tables of bounds for $N_q(g)$. Table 1 is for $q = 2, 3, 4, 5, 8, 16$ and $1 \leq g \leq 50$ (for $g = 0$ we trivially have $N_q(0) = q+1$), and Table 2 extends Table 1 for the important case $q = 2$ to the range $51 \leq g \leq 95$. In each entry of the tables, the first number is a lower bound for $N_q(g)$ and the second is an upper bound for $N_q(g)$. If only one number is given, then this is the exact value of $N_q(g)$. A program for calculating upper bounds for $N_q(g)$, which is based on Weil's explicit formula for the number of rational places and on the trigonometric polynomials of Oesterlé, was kindly supplied to us by Jean-Pierre Serre. For $q = 16, g = 4, 5$, one can obtain an improved upper bound from a general result of Serre [26]. The lower bounds are obtained by combining data from the earlier table of Niederreiter and Xing [19], an updated version (August 1997) of the table of van der Geer and van der Vlugt [31], and the recent work of the authors in [17] for $q = 3$, in [18] for $q = 5$, and in [21] for $q = 8$ and 16. The following two new examples based on Hilbert class fields are also included in the present tables.

EXAMPLE 1. $q = 2, g(K) = 70, N(K) = 46$. Let $F = \mathbf{F}_2(x, y)$ with

$$y^2 + y = \frac{x^8 + x^4 + x^3 + 1}{x^3}.$$

Then F is an Artin-Schreier extension of the rational function field $\mathbf{F}_2(x)$ with $g(F) = 4$. If $N(F_r)$ denotes the number of rational places of the constant field extension $F_r = \mathbf{F}_{2^r} \cdot F$, then

$$N(F_1) = 4, \ N(F_2) = 8, \ N(F_3) = 10, \ N(F_4) = 24.$$

Therefore, the L-polynomial $L_F(t)$ of F (see [28, Section V.1]) is given by

$$L_F(t) = 16t^8 + 8t^7 + 8t^6 + 4t^5 + 4t^4 + 2t^3 + 2t^2 + t + 1,$$

and so we get the divisor class number $h(F) = L_F(1) = 46$. As a distinguished rational place of F we choose the pole ∞ of x, and then we let H_∞ be the Hilbert class field of F with respect to ∞. Let P be the place of F which is the unique zero of x. Since $2(P-\infty)$ is the principal divisor (x) and $P - \infty$ is not a principal divisor by the Weierstrass gap theorem, the cyclic subgroup G of $\mathrm{Div}^0(F) \simeq \mathrm{Gal}(H_\infty/F)$ generated by the divisor class $[P - \infty]$ has order 2. Thus, if K is the subfield of H_∞/F fixed by G, then $[K : F] = h(F)/2 = 23$. By construction,

the places P and ∞ split completely in K/F, hence $N(K) = 46$. Since the extension K/F is unramified, the Hurwitz genus formula yields $2g(K) - 2 = 23 \cdot (2g(F) - 2)$, that is, $g(K) = 70$.

EXAMPLE 2. $q = 2, g(K) = 76, N(K) = 50$. Let $F = \mathbf{F}_2(x, y)$ with

$$y^2 + y = \frac{x^8 + x^4 + x + 1}{x}.$$

Then F is an Artin-Schreier extension of the rational function field $\mathbf{F}_2(x)$ with $g(F) = 4$. With the same notation as in Example 1 we get

$$N(F_1) = 4, N(F_2) = 8, N(F_3) = 16, N(F_4) = 8,$$

hence

$$L_F(t) = 16t^8 + 8t^7 + 8t^6 + 8t^5 + 2t^4 + 4t^3 + 2t^2 + t + 1,$$

and so $h(F) = L_F(1) = 50$. By proceeding now in exactly the same way as in Example 1, we arrive at the desired values of $g(K)$ and $N(K)$.

4. Asymptotic results and the Gilbert-Varshamov bound

The asymptotic theory of global function fields with many rational places is concerned with the behavior of $N_q(g)$ for q fixed and $g \to \infty$. The basic quantity here is

$$A(q) = \limsup_{g \to \infty} \frac{N_q(g)}{g},$$

where g runs through positive values. It follows from (1) that $A(q) \leq \lfloor 2q^{1/2} \rfloor$. Vlăduț and Drinfeld [32] improved this to

$$A(q) \leq q^{1/2} - 1 \quad \text{for all } q. \tag{4}$$

If q is a square, then the work of Ihara [8] and Tsfasman, Vlăduț, and Zink [30] shows that $A(q) = q^{1/2} - 1$, and Garcia and Stichtenoth [1], [4] proved this result by constructing an explicit tower of global function fields over $\mathbf{F}_q$.

In the case where q is not a square, no exact values of $A(q)$ are known, but lower bounds are available which complement the general upper bound (4). According to a result of Serre [25], [26] based on class

field theory, we have $A(q) \geq c \log q$ with an absolute constant $c > 0$. For later use we note that Zink [37] proved

$$A(p^3) \geq \frac{2(p^2-1)}{p+2} \quad \text{for all primes } p. \tag{5}$$

Further lower bounds for $A(q)$ can be found in Garcia and Stichtenoth [3], Garcia, Stichtenoth, and Thomas [5], Perret [22], and Tsfasman and Vlădut [29, Theorem 2.3.25]. For small values of q, the following result of Niederreiter and Xing [20] improves on earlier bounds for $A(q)$ by Schoof [24], Serre [26], and Xing [33].

THEOREM 3. $A(2) \geq \frac{81}{317} = 0.2555\ldots$, $A(3) \geq \frac{62}{163} = 0.3803\ldots$, $A(5) \geq \frac{2}{3}$.

For composite nonsquares q, a new general lower bound for $A(q)$ was established by the authors in [20]. The proof uses infinite class field towers with a suitable base field. In [20] the existence of such a base field was demonstrated in a nonconstructive way. We now present an alternative proof with an explicitly constructed base field $K/\mathbf{F}_q$ of the class field tower. We treat the cases q odd and q even separately, and in the first case we actually get a slight improvement on the result in [20] (see Theorem 4 below).

The following proposition is derived from the work of Serre [26] and Schoof [24] (see also [20, Proposition 1]). It provides a sufficient condition for an infinite class field tower and the consequence for $A(q)$. For our present purposes we find it more convenient to state the result in terms of Galois groups rather than in terms of divisor class groups. For a prime l we write $d_l B$ for the l-rank of an abelian group B. Furthermore, for a real number u we let $\lceil u \rceil$ denote the least integer $\geq u$.

PROPOSITION 1. *Let $K/\mathbf{F}_q$ be a global function field of genus $g(K) > 1$ and let S be a nonempty set of rational places of K. Suppose that there exist an unramified abelian extension L/K in which all places in S split completely and a prime l such that*

$$d_l \mathrm{Gal}(L/K) \geq 2 + 2(|S| + \varepsilon_l(q))^{1/2},$$

where $\varepsilon_l(q) = 1$ if $l|(q-1)$ and $\varepsilon_l(q) = 0$ otherwise. Then

$$A(q) \geq \frac{|S|}{g(K)-1}.$$

THEOREM 4. *If q is an odd prime power and $m \geq 3$ is an integer, then*

$$A(q^m) \geq \frac{2q+2}{\lceil 2(2q+3)^{1/2} \rceil + 1}.$$

Proof. Put $n = \lceil 2(2q+3)^{1/2} \rceil + 3$, then n does not exceed the number of monic irreducible polynomials of degree m in $\mathbf{F}_q[x]$, except for $q = m = 3$, but in this case the result of the theorem is implied by (5).

Let $f_1, \ldots, f_n$ be n distinct monic irreducible polynomials of degree m in $\mathbf{F}_q[x]$ and for $1 \leq i \leq n$ let $\beta_i \in \mathbf{F}_{q^m}$ be a root of f_i. Put $F = \mathbf{F}_{q^m}(x)$ and let $K = F(y)$ with

$$y^2 = \prod_{i=1}^{n} (x - \beta_i)(x - \beta_i^q).$$

Then K/F is a Kummer extension with $g(K) = n - 1$ by [28, Example III.7.6]. For $1 \leq i \leq n$ let $K_i = F(y_i)$ with

$$y_i^2 = (x - \beta_i)(x - \beta_i^q)$$

and let L be the composite field of $K_1, \ldots, K_n$. Since the extensions $K_i/F, 1 \leq i \leq n$, are linearly disjoint, we have

$$\mathrm{Gal}(L/F) \simeq \prod_{i=1}^{n} \mathrm{Gal}(K_i/F) = (\mathbf{Z}/2\mathbf{Z})^n.$$

Note also that $K \subseteq L$ since we can take $y = y_1 \cdots y_n$. Thus,

$$\mathrm{Gal}(L/K) \simeq (\mathbf{Z}/2\mathbf{Z})^{n-1},$$

and so $d_2\mathrm{Gal}(L/K) = n - 1$. For $1 \leq i \leq n$ the places $x - \beta_i$ and $x - \beta_i^q$ of F have ramification index 2 in L/F and also ramification index 2 in K/F, and since there are no other ramified places in L/F, the extension L/K is unramified.

Now let T be the set of rational places of F given by

$$T = \{P_b = x - b : b \in \mathbf{F}_q\} \cup \{\infty\},$$

where ∞ is the pole of x. For all $1 \leq i \leq n$ and $b \in \mathbf{F}_q$ we have

$$\begin{aligned} (x - \beta_i)(x - \beta_i^q) &\equiv (b - \beta_i)(b - \beta_i^q) \equiv (b - \beta_i)(b^q - \beta_i^q) \\ &\equiv (b - \beta_i)^{q+1} \bmod P_b. \end{aligned}$$

Since q is odd, the last element is a nonzero square in the residue class field of P_b, and so P_b splits completely in K_i/F by Kummer's theorem. Moreover, ∞ splits completely in K_i/F. Thus, if S is the set of places of K lying over those in T, then $|S| = 2q + 2$ and all places in S split completely in L/K. By the definition of n,

$$d_2\mathrm{Gal}(L/K) = n - 1 \geq 2 + 2(2q+3)^{1/2} = 2 + 2(|S|+1)^{1/2}.$$

Therefore, all conditions in Proposition 1 are satisfied with $l = 2$, and so we obtain the result of the theorem. □

COROLLARY 3. *If $q = p^e$ with an odd prime p and an odd integer $e \geq 3$, then*

$$A(q) \geq \frac{2q^{1/m} + 2}{\lceil 2(2q^{1/m}+3)^{1/2} \rceil + 1},$$

where m is the least prime factor of e.

THEOREM 5. *If $q \geq 4$ is a power of 2 and $m \geq 3$ is an odd integer, then*

$$A(q^m) \geq \frac{q+1}{\lceil 2(2q+2)^{1/2} \rceil + 2}.$$

Proof. If $q = 4$, then q^m is a square and $A(q^m) = q^{m/2} - 1$ by a result mentioned at the beginning of this section, and so we are done. Thus, we can assume $q \geq 8$. Put $n = \lceil 2(2q+2)^{1/2} \rceil + 3$, then n does not exceed the number of monic irreducible polynomials of degree 2 in $\mathbf{F}_q[x]$.

Let $f_1, \ldots, f_n$ be n distinct monic irreducible polynomials of degree 2 in $\mathbf{F}_q[x]$. Since m is odd, each f_i is irreducible over $\mathbf{F}_{q^m}$ and can thus be identified with a place Q_i of $F = \mathbf{F}_{q^m}(x)$ of degree 2. Choose $\beta \in \mathbf{F}_{q^m}^*$ with trace

$$\mathrm{Tr}_{\mathbf{F}_{q^m}/\mathbf{F}_q}(\beta) = 0$$

and let $K = F(y)$ with

$$y^2 + y = \sum_{i=1}^{n} \frac{\beta}{f_i(x)}.$$

Then K/F is an Artin-Schreier extension with $g(K) = 2n - 1$ by [28, Proposition III.7.8]. For $1 \leq i \leq n$ let $K_i = F(y_i)$ with

$$y_i^2 + y_i = \frac{\beta}{f_i(x)}$$

and let L be the composite field of $K_1, \ldots, K_n$. We have $K \subseteq L$ since we can take $y = y_1 + \cdots + y_n$. The only ramified places in L/F are the $Q_i, 1 \leq i \leq n$, and so we see as in the proof of Theorem 4 that L/K is an unramified abelian extension with $d_2\mathrm{Gal}(L/K) = n - 1$.

Now let T be the set of rational places of F given by

$$T = \{P_b = x - b : b \in \mathbf{F}_q\} \cup \{\infty\},$$

where ∞ is the pole of x. For all $1 \leq i \leq n$ and $b \in \mathbf{F}_q$ we have

$$\mathrm{Tr}_{\mathbf{F}_{q^m}/\mathbf{F}_q}\left(\frac{\beta}{f_i(b)}\right) = \frac{1}{f_i(b)}\mathrm{Tr}_{\mathbf{F}_{q^m}/\mathbf{F}_q}(\beta) = 0,$$

and so the absolute trace

$$\mathrm{Tr}_{\mathbf{F}_{q^m}}\left(\frac{\beta}{f_i(b)}\right) = 0$$

by the transitivity of the trace [9, Theorem 2.26]. It follows then from Kummer's theorem and [9, Theorem 2.25] that P_b splits completely in K_i/F. Moreover, ∞ splits completely in K_i/F. Thus, if S is the set of all places of K lying over those in T, then $|S| = 2q + 2$ and all places in S split completely in L/K. By the definition of n,

$$d_2\mathrm{Gal}(L/K) = n - 1 \geq 2 + 2(2q + 2)^{1/2} = 2 + 2|S|^{1/2}.$$

Therefore, all conditions in Proposition 1 are satisfied with $l = 2$, and so we obtain the result of the theorem. □

COROLLARY 4. *If $q = 2^e$ with an odd integer $e \geq 3$, then*

$$A(q) \geq \frac{81}{317}$$

if e is a prime and

$$A(q) \geq \frac{q^{1/m} + 1}{\lceil 2(2q^{1/m} + 2)^{1/2} \rceil + 2}$$

if e is not a prime, where m is the least prime factor of e.

Proof. Since $A(q) \geq A(2)$ by considering constant field extensions, the first part follows from Theorem 3. The second part is implied by Theorem 5. □

The results on $A(q)$ in this section have applications to algebraic coding theory, in that they lead to improvements on the classical Gilbert-Varshamov bound for the existence of good linear codes over $\mathbf{F}_q$. For a linear code C over $\mathbf{F}_q$ we denote by $n(C), k(C)$, and $d(C)$ the length, the dimension, and the minimum distance of C, respectively. Let U_q^{lin} be the set of ordered pairs $(\delta, R) \in [0,1]^2$ for which there exists an infinite sequence $C_1, C_2, \ldots$ of linear codes over $\mathbf{F}_q$ with $n(C_i) \to \infty$ and

$$\delta = \lim_{i\to\infty} \frac{d(C_i)}{n(C_i)}, \quad R = \lim_{i\to\infty} \frac{k(C_i)}{n(C_i)}.$$

The following description of U_q^{lin} can be found in [29, Section 1.3.1].

PROPOSITION 2. *There exists a continuous function* α_q^{lin} *on* $[0,1]$ *such that*

$$U_q^{\mathrm{lin}} = \left\{(\delta, R) : 0 \le R \le \alpha_q^{\mathrm{lin}}(\delta), 0 \le \delta \le 1\right\}.$$

Moreover, $\alpha_q^{\mathrm{lin}}(0) = 1, \alpha_q^{\mathrm{lin}}(\delta) = 0$ *for* $\delta \in [(q-1)/q, 1]$, *and* α_q^{lin} *decreases on the interval* $[0, (q-1)/q]$.

The function α_q^{lin} is not known and may in fact be quite complicated. It is an important issue in algebraic coding theory to obtain good lower bounds for α_q^{lin} on the interval $(0, (q-1)/q)$. The classical and most widely quoted bound is the Gilbert-Varshamov bound

$$\alpha_q^{\mathrm{lin}}(\delta) \ge R_{GV}(q,\delta) := 1 - H_q(\delta) \quad \text{for all } \delta \in (0, \frac{q-1}{q}),$$

where H_q is the q-ary entropy function

$$H_q(\delta) = \delta \log_q(q-1) - \delta \log_q \delta - (1-\delta)\log_q(1-\delta),$$

with $\log_q$ denoting the logarithm to the base q.

Goppa's construction of algebraic-geometry codes uses algebraic curves over $\mathbf{F}_q$ with many $\mathbf{F}_q$-rational points, or equivalently global function fields with many rational places. For detailed expositions of the theory of algebraic-geometry codes we refer to the monographs [28] and [29]. According to [28, Proposition VII.2.5] or [29, Corollary 3.4.2], algebraic-geometry codes lead to the bound

$$\alpha_q^{\mathrm{lin}}(\delta) \ge R_{AG}(q,\delta) := 1 - \frac{1}{A(q)} - \delta \quad \text{for all } \delta \in [0,1].$$

A crucial question is whether we can ever have $R_{AG}(q,\delta) > R_{GV}(q,\delta)$. If we want to answer this question affirmatively, we need good lower bounds for $A(q)$. A well-known result of Tsfasman, Vlăduţ, and Zink [30] shows that $R_{AG}(q,\delta) > R_{GV}(q,\delta)$ if q is a sufficiently large square and δ belongs to a suitable subinterval of $[0,1]$. The proof of this theorem is based on the fact that $A(q) = q^{1/2} - 1$ if q is a square. It was open until recently whether an analogous result holds for nonsquares q. The following theorem of the authors [20] settles this problem for sufficiently large composite nonsquares q. The proof is based on Theorems 4 and 5.

THEOREM 6. *Let $m \geq 3$ be an odd integer and let r be a prime power with $r \geq 100m^3$ for odd r and $r \geq 576m^3$ for even r. Then there exists an open interval $(\delta_1, \delta_2) \subseteq (0,1)$ containing $(r^m - 1)/(2r^m - 1)$ such that*

$$R_{AG}(r^m,\delta) > R_{GV}(r^m,\delta) \quad \text{for all } \delta \in (\delta_1,\delta_2).$$

5. Applications to low-discrepancy sequences

Low-discrepancy sequences are sequences of points in an s-dimensional unit cube $[0,1]^s$ that are distributed very uniformly. Such sequences are used, for instance, in quasi-Monte Carlo methods for numerical integration over $[0,1]^s$ (see the book [10] for a general background). The most powerful constructions of low-discrepancy sequences yield so-called digital (t,s)-sequences constructed over $\mathbf{F}_q$; for the precise definition we refer to the recent survey article [16]. Here s is, as above, the dimension in which the sequence lives and the integer $t \geq 0$ is the quality parameter of the sequence, which should be as small as possible.

Recent work of the authors [11], [13], [16], [34] has shown that global function fields over $\mathbf{F}_q$ with many rational places can be used to obtain the currently best digital (t,s)-sequences constructed over $\mathbf{F}_q$. The most general construction is that in [34] and it has the following ingredients. For a given q and a given dimension $s \geq 1$, let $K/\mathbf{F}_q$ be a global function field containing at least one rational place P_∞ and let D be a positive divisor of K with $\deg(D) = 2g(K)$ and P_∞ not in the support of D. If $P_1, \ldots, P_s$ are s distinct places of K with $P_i \neq P_\infty$ for $1 \leq i \leq s$, then we obtain a digital (t,s)-sequence constructed over $\mathbf{F}_q$ with

$$t = g(K) + \sum_{i=1}^{s} (\deg(P_i) - 1). \tag{6}$$

If at least one of the places P_i, say P_1, is rational, then we can simply take $D = 2g(K)P_1$. In the special case where $N(K) \geq s+1$, we can choose all $P_i, 1 \leq i \leq s$, to be rational places, and then by optimizing K we get

$$t = V_q(s) := \min\{g \geq 0 : N_q(g) \geq s+1\}. \tag{7}$$

For any q and any dimension $s \geq 1$ let $d_q(s)$ be the least value of t such that there exists a digital (t,s)-sequence constructed over $\mathbf{F}_q$. In Table 3 below we tabulate upper bounds for $d_q(s)$ for $q = 2, 3, 5$ and $1 \leq s \leq 50$. This table improves and extends the bounds in [16, Table 2]. Most of the bounds in Table 3 are obtained from the trivial inequality $d_q(s) \leq V_q(s)$ implied by (7) and from upper bounds for $V_q(s)$ that can be read off immediately from Tables 1 and 2. Those few bounds for $d_q(s)$ that arise in a different manner stem either from [16, Table 2] or from Examples 3 to 6 below.

EXAMPLE 3. The bound $d_3(36) \leq 26$ in Table 3 arises in the following way. Let $K/\mathbf{F}_3$ be the global function field in [17, Example 8B] which satisfies $g(K) = 25, N(K) = 36$, and has at least six places of degree 2. Let P_∞ be one of the rational places of K, let $P_1, \ldots, P_{35}$ be the remaining rational places of K, and let P_{36} be one of the places of K of degree 2. Then (6) yields $t = 26$.

EXAMPLE 4. The bound $d_3(42) \leq 33$ in Table 3 arises in the following way. Let $K/\mathbf{F}_3$ be the global function field in [17, Example 12] which satisfies $g(K) = 29, N(K) = 42$, and has at least 14 places of degree 5. Let P_∞ be one of the rational places of K, let $P_1, \ldots, P_{41}$ be the remaining rational places of K, and let P_{42} be one of the places of K of degree 5. Then (6) yields $t = 33$.

EXAMPLE 5. The bound $d_5(22) \leq 8$ in Table 3 arises in the following way. Let $K/\mathbf{F}_5$ be the global function field in [18, Example 1] which is given by $K = \mathbf{F}_5(x,y)$ with

$$y^4 = (x^2+2)(x^4 - 2x^2 - 2).$$

Then $g(K) = 7, N(K) = 22$, and K has at least one place of degree 2 since the place x^2+2 of $\mathbf{F}_5(x)$ is totally ramified in $K/\mathbf{F}_5(x)$. Let P_∞ be one of the rational places of K, let $P_1, \ldots, P_{21}$ be the remaining rational places of K, and let P_{22} be a place of K of degree 2. Then (6) yields $t = 8$.

EXAMPLE 6. The bound $d_5(42) \leq 18$ in Table 3 arises in the following way. Let $K/\mathbf{F}_5$ be the global function field in [18, Example 9] which is given by $K = \mathbf{F}_5(x, y_1, y_2)$ with

$$y_1^2 = x(x^2 - 2), \quad y_2^5 - y_2 = \frac{x^4 - 1}{y_1}.$$

Then $g(K) = 17, N(K) = 42$, and K has at least one place of degree 2 since the place $x^2 - 2$ of $\mathbf{F}_5(x)$ is totally ramified in $K/\mathbf{F}_5(x)$. Let P_∞ be one of the rational places of K, let $P_1, \ldots, P_{41}$ be the remaining rational places of K, and let P_{42} be a place of K of degree 2. Then (6) yields $t = 18$.

Table 1: Bounds for $N_q(g)$

$g \backslash q$	2	3	4	5	8	16
1	5	7	9	10	14	25
2	6	8	10	12	18	33
3	7	10	14	16	24	38
4	8	12	15	18	25-29	45-47
5	9	12-14	17-18	20-22	29-32	49-55
6	10	14-15	20	21-25	33-36	65
7	10	16-17	21-22	22-27	33-39	63-70
8	11	15-18	21-24	22-29	34-43	61-76
9	12	19	26	26-32	36-47	72-81
10	13	19-21	27-28	27-34	38-50	81-87
11	14	20-22	26-30	32-36	48-54	80-92
12	14-15	22-24	28-31	30-38	49-57	68-97
13	15	24-25	33	36-40	50-61	97-103
14	15-16	24-26	32-35	39-43	65	97-108
15	17	28	33-37	32-45	54-68	98-113
16	16-18	27-29	36-38	40-47	56-71	93-118
17	17-18	24-30	40	42-49	61-74	96-124
18	18-19	26-31	34-42	32-51	65-77	93-129
19	20	27-32	36-43	41-54	58-80	121-134
20	19-21	30-34	36-45	30-56	68-83	121-140
21	21	32-35	41-47	48-58	72-86	129-145
22	21-22	28-36	40-48	51-60	66-89	129-150
23	22-23	26-37	40-50		68-92	126-155
24	20-23	28-38	42-52		66-95	129-161
25	24	36-40	51-53		66-97	144-166
26	24-25	36-41	55		72-100	150-171
27	22-25	39-42	49-56		96-103	128-176
28	24-26	37-43	44-58		97-106	136-181
29	25-27	42-44	49-60		97-109	130-187
30	24-27	34-46	52-61		80-112	144-192
31	27-28	40-47	60-63		72-115	150-197
32	26-29	38-48	52-65		72-118	132-202
33	28-29	37-49	65-66		92-121	153-207
34	27-30	44-50	57-68		80-124	156-213
35	28-31	38-51	54-69		106-127	144-218
36	30-31	36-52	64-71		105-130	165-223
37	28-32	48-54	66-72		121-132	144-228
38	28-33	36-55	56-74		129-135	152-233
39	33	42-56	56-75		117-138	160-239
40	32-34	54-57	75-77		100-141	162-244

$g\backslash q$	2	3	4	5	8	16
41	32-35	50-58	65-78		112-144	216-249
42	30-35	39-59	66-80		129-147	162-254
43	33-36	55-60	72-81		100-150	176-259
44	32-37	42-61	68-83		129-153	162-264
45	32-37	48-62	80-84		144-156	242-268
46	34-38	55-63	66-86		129-158	243-273
47	36-38	47-65	68-87		120-161	176-277
48	34-39	55-66	77-89		126-164	184-282
49	36-40	54-67	81-90		130-167	192-286
50	40	56-68	91-92		130-170	200-291

Table 2: Bounds for $N_2(g)$

g	51	52	53	54	55	56	57	58	59
$N_2(g)$	36-41	34-42	40-42	42-43	36-43	38-44	40-45	40-45	40-46

g	60	61	62	63	64	65	66	67	68
$N_2(g)$	40-47	40-47	44-48	42-48	42-49	48-50	42-50	44-51	45-51

g	69	70	71	72	73	74	75	76	77
$N_2(g)$	49-52	46-53	44-53	48-54	48-54	48-55	48-56	50-56	52-57

g	78	79	80	81	82	83	84	85	86
$N_2(g)$	48-57	52-58	56-59	48-59	53-60	52-60	57-61	52-62	56-62

g	87	88	89	90	91	92	93	94	95
$N_2(g)$	56-63	56-63	56-64	56-65	54-65	60-66	56-66	56-67	65-68

Table 3: Upper bounds for $d_q(s)$

$q\backslash s$	1	2	3	4	5	6	7	8	9	10	11	12	13
2	0	0	1	1	2	3	4	5	6	8	9	10	11
3	0	0	0	1	1	1	2	3	3	4	4	5	6
5	0	0	0	0	0	1	1	1	1	2	2	3	3

$q\backslash s$	14	15	16	17	18	19	20	21	22	23	24	25	26
2	13	15	15	18	19	19	21	23	25	25	29	31	31
3	7	7	9	9	9	11	12	12	13	13	15	15	15
5	3	3	4	4	5	5	6	7	8	9	9	9	10

$q\backslash s$	27	28	29	30	31	32	33	34	35	36	37	38
2	33	36	36	39	39	39	45	47	47	50	50	50
3	15	20	20	21	21	25	25	25	25	26	27	27
5	11	11	11	11	11	13	13	13	13	14	14	14

$q\backslash s$	39	40	41	42	43	44	45	46	47	48	49	50
2	50	54	54	59	62	65	65	65	65	69	75	77
3	29	29	29	33	34	37	37	37	37	40	40	40
5	16	17	17	18	21	21	21	21	21	22	22	22

References

1. A. Garcia and H. Stichtenoth, *A tower of Artin-Schreier extensions of function fields attaining the Drinfeld-Vladut bound*, Invent. Math. **121** (1995), 211–222.

2. A. Garcia and H. Stichtenoth, *Algebraic function fields over finite fields with many rational places*, IEEE Trans. Information Theory **41** (1995), 1548–1563.

3. A. Garcia and H. Stichtenoth, *Asymptotically good towers of function fields over finite fields*, C.R. Acad. Sci. Paris Sér. I Math. **322** (1996), 1067–1070.

4. A. Garcia and H. Stichtenoth, *On the asymptotic behaviour of some towers of function fields over finite fields*, J. Number Theory **61** (1996), 248–273.

5. A. Garcia, H. Stichtenoth, and M. Thomas, *On towers and composita of towers of function fields over finite fields*, Finite Fields Appl. **3** (1997), 257–274.

6. D. Goss, *Basic structures of function field arithmetic*, Springer, Berlin, 1996.

7. D.R. Hayes, *A brief introduction to Drinfeld modules*, The arithmetic of function fields (D. Goss, D.R. Hayes, and M.I. Rosen, eds.), W. de Gruyter, Berlin, 1992, 1–32.

8. Y. Ihara, *Some remarks on the number of rational points of algebraic curves over finite fields*, J. Fac. Sci. Univ. Tokyo Sect. IA Math. **28** (1981), 721–724.

9. R. Lidl and H. Niederreiter, *Introduction to finite fields and their applications*, revised ed., Cambridge University Press, Cambridge, 1994.

10. H. Niederreiter, *Random number generation and quasi-Monte Carlo methods*, SIAM, Philadelphia, 1992.

11. H. Niederreiter and C.P. Xing, *Low-discrepancy sequences and global function fields with many rational places*, Finite Fields Appl. **2** (1996), 241–273.

12. H. Niederreiter and C.P. Xing, *Explicit global function fields over the binary field with many rational places*, Acta Arith. **75** (1996), 383–396.

13. H. Niederreiter and C.P. Xing, *Quasirandom points and global function fields*, Finite fields and applications (S. Cohen and H. Niederreiter, eds.), London Math. Soc. Lecture Note Series, Vol. **233**, Cambridge University Press, Cambridge, 1996, 269–296.

14. H. Niederreiter and C.P. Xing, *Cyclotomic function fields, Hilbert class fields, and global function fields with many rational places*, Acta Arith. **79** (1997), 59–76.

15. H. Niederreiter and C.P. Xing, *Drinfeld modules of rank 1 and algebraic curves with many rational points. II*, Acta Arith. **81** (1997), 81–100.

16. H. Niederreiter and C.P. Xing, *The algebraic-geometry approach to low-discrepancy sequences*, Monte Carlo and quasi-Monte Carlo methods 1996 (H. Niederreiter et al., eds.), Lecture Notes in Statistics, Vol. **127**, Springer, New York, 1998, 139–160.

17. H. Niederreiter and C.P. Xing, *Global function fields with many rational places over the ternary field*, Acta Arith. **83** (1998), 65–86.

18. H. Niederreiter and C.P. Xing, *Global function fields with many rational places over the quinary field*, Demonstratio Math. **30** (1997), 919–930.

19. H. Niederreiter and C.P. Xing, *Algebraic curves over finite fields with many rational points*, Number theory (K. Győry et al., eds.), W. de Gruyter, Berlin, 1998, 423–443.

20. H. Niederreiter and C.P. Xing, *Towers of global function fields with asymptotically many rational places and an improvement on the Gilbert-Varshamov bound*, Math. Nachr., to appear.

21. H. Niederreiter and C.P. Xing, *Algebraic curves with many rational points over finite fields of characteristic 2*, Proc. Number Theory Conf. (Zakopane, 1997), W. de Gruyter, Berlin, to appear.

22. M. Perret, *Tours ramifiées infinies de corps de classes*, J. Number Theory **38** (1991), 300–322.

23. M. Rosen, *The Hilbert class field in function fields*, Exposition. Math. **5** (1987), 365–378.

24. R. Schoof, *Algebraic curves over* $\mathbf{F}_2$ *with many rational points*, J. Number Theory **41** (1992), 6–14.

25. J.-P. Serre, *Sur le nombre des points rationnels d'une courbe algébrique sur un corps fini*, C.R. Acad. Sci. Paris Sér. I Math. **296** (1983), 397–402.

26. J.-P. Serre, *Rational points on curves over finite fields*, lecture notes, Harvard University, 1985.

27. J.-P. Serre, *Local fields*, Springer, New York, 1995.

28. H. Stichtenoth, *Algebraic function fields and codes*, Springer, Berlin, 1993.

29. M.A. Tsfasman and S.G. Vlădut, *Algebraic-geometric codes*, Kluwer, Dordrecht, 1991.

30. M.A. Tsfasman, S.G. Vlădut, and T. Zink, *Modular curves, Shimura curves, and Goppa codes, better than Varshamov-Gilbert bound*, Math. Nachr. **109** (1982), 21–28.

31. G. van der Geer and M. van der Vlugt, *How to construct curves over finite fields with many points*, Arithmetic geometry (F. Catanese, ed.), Cambridge University Press, Cambridge, 1997, 169–189.

32. S.G. Vlădut and V.G. Drinfeld, *Number of points of an algebraic curve*, Funct. Anal. Appl. **17** (1983), 53–54.

33. C.P. Xing, *Multiple Kummer extension and the number of prime divisors of degree one in function fields*, J. Pure Appl. Algebra **84** (1993), 85–93.

34. C.P. Xing and H. Niederreiter, *A construction of low-discrepancy sequences using global function fields*, Acta Arith. **73** (1995), 87–102.

35. C.P. Xing and H. Niederreiter, *Modules de Drinfeld et courbes algébriques ayant beaucoup de points rationnels*, C.R. Acad. Sci. Paris Sér. I Math. **322** (1996), 651–654.

36. C.P. Xing and H. Niederreiter, *Drinfeld modules of rank 1 and algebraic curves with many rational points*, Monatsh. Math., to appear.

37. T. Zink, *Degeneration of Shimura surfaces and a problem in coding theory*, Fundamentals of computation theory (L. Budach, ed.), Lecture Notes in Computer Science, Vol. **199**, Springer, Berlin, 1985, 503–511.

INSTITUTE OF INFORMATION PROCESSING, AUSTRIAN ACADEMY OF SCIENCES, SONNENFELSGASSE 19, A–1010 VIENNA, AUSTRIA
E-mail: {niederreiter, xing}@oeaw.ac.at

This page intentionally left blank

Contemporary Mathematics
Volume 225, 1999

TRACES OF ROOTS OF UNITY OVER PRIME FIELDS

GREG STEIN

ABSTRACT. We re-examine the impact of knowing the traces of r^{th} roots of unity over $\mathbb{F}_p$, r and p distinct primes, to being able to factor the corresponding cyclotomic polynomial. We further examine the question of when two different primitive r^{th} roots of unity can have the same trace over $\mathbb{F}_p$ and include a table of all such occurences for $r < p < 1000$. We also include a table of all cases where zero appears as the trace of an r^{th} root of unity over $\mathbb{F}_p$ for $r < p < 1000$.

1. INTRODUCTION

Among the topics of interest at the Third International Conference on Finite Fields and Applications was that of being able to factor the r^{th} cyclotomic polynomial, Φ_r, over the prime field $\mathbb{F}_p$, deterministically, in time polynomial in r and $\log p$. This author was able to report [1] that this can be done if we know the trace of any one of the primitive r^{th} roots of unity over $\mathbb{F}_p$. However, it should be pointed out that the technique given, as it is not iterative, will not always yield a complete factorization of Φ_r.

To examine this situation a little more deeply recall that if r and p are distinct primes, d the order of p modulo r, $m = \frac{r-1}{d}$, α a generator of $\mathbb{F}_r^*$ and ζ a primitive r^{th} root of unity, then Φ_r will factor into the m d^{th} degree irreducible polynomials $g_0(x), \cdots, g_{m-1}(x)$ in $\mathbb{F}_p[x]$ where, for $i \in \mathbb{Z}/m\mathbb{Z}$,

$$g_i(x) = \prod_{j=0}^{d-1} \left(x - \zeta^{\alpha^i p^j}\right). \tag{1.1}$$

If we then define, for $i \in \mathbb{Z}/m\mathbb{Z}$,

$$T_i(x) = \sum_{j=0}^{d-1} x^{\alpha^i p^j} \in \mathbb{F}_p[x] \tag{1.2}$$

1991 *Mathematics Subject Classification.* Primary 11T06, 11Y05; Secondary 11T22, 11Y16, 12Y05, 13P05.

Key words and phrases. Finite field, factorization, cyclotomic polynomial,trace.

This paper is in final form and no version of it will be submitted for publication elsewhere.

© 1999 American Mathematical Society

then we saw in [1] that, for $i \in \mathbb{Z}/m\mathbb{Z}$,

$$T_i(x) \equiv t_{i+j} \bmod g_j(x) \tag{1.3}$$

where t_k is the trace of ζ^{α^k} over $\mathbb{F}_p$. If we were to know the value of some t_k in $\mathbb{F}_p$ then, since the traces cannot all be the same (see Lemma 13, p.46 of [2]), we have that (1.3) implies that $T_i(x) - t_k \equiv 0 \bmod g_{k-i}(x)$. Therefore, computing $\gcd(T_i(x) - t_k, \Phi_r(x))$ gives a nontrivial factor of $\Phi_r(x)$. If t_k is distinct from the other traces then $\gcd(T_i(x) - t_k, \Phi_r(x))$ is precisely $g_{k-i}(x)$ and in this way we get a complete factorization of $\Phi_r(x)$. In particular, if all of the traces are distinct then knowing any one of them necessarily yields a complete factorization. Further, if we know all of the traces then, whether or not they are distinct, the results of Chapter 2 in [2] gives a technique for the deterministic, polynomial time, complete factorization of $\Phi_r(x)$ over $\mathbb{F}_p$. Hence we have

Lemma 1.1. *Let r and p be distinct primes. If we know all of the traces of the primitive r^{th} roots of unity over $\mathbb{F}_p$, or if we know the trace of one primitive r^{th} root of unity which is distinct from all of the rest, then we may completely factor $\Phi_r(x)$ deterministically, in time polynomial in r and $\log p$,*

2. Ramifications of duplicate traces to the factorization problem

It should be noted that even if we know some trace, t, which is not distinct from all of the rest we will usually be able to completely factor $\Phi_r(x)$ by comparing $\gcd(T_i(x) - t, \Phi_r(x))$ and $\gcd(T_j(x) - t, \Phi_r(x))$ for the various i and j.

Example 2.1. *In the case $p = 47$, $r = 43$ we find $d = 7$, $m = 6$ and we have that the trace $t_0 = 38$ occurs twice among the primitive 43^{rd} roots of unity over $\mathbb{F}_{47}$. If we set $u_i(x) = \gcd(T_i(x) - 38, \Phi_{43}(x))$ we find that all six of these degree fourteen polynomials is a product of two of the irreducible factors of $\Phi_{43}(x)$. If we then compute $\gcd(u_0(x), u_2(x))$ we get a seventh degree polynomial, which must therefore be an irreducible factor of $\Phi_{43}(x)$. In this way we get the complete factorization of $\Phi_{43}(x)$.*

This, however, need not be the case.

Example 2.2. *In the case $p = 137$, $r = 101$, we find $d = 5$, $m = 20$ and that the trace $t_0 = 71$ occurs twice among the primitive 101^{st} roots of unity over $\mathbb{F}_{147}$. We then compute $u_i(x) = \gcd(T_i(x) - 71, \Phi_{101}(x))$ and again find that all twenty of these tenth degree polynomials is a product of two of the irreducible factors of Φ_{101}. In this case, however, computing $\gcd(u_i(x), u_j(x))$ always yields either a degree zero or a degree ten polynomial, so we cannot get an irreducible factor in this way.*

Note that the unseemly behavior encountered in the previous example cannot occur when m is prime.

It should be noted that if we know, a priori, for a particular choice of p and r, that two different primitive r^{th} roots of unity are the same, then we could very quickly deterministically compute a nontrivial factorization of Φ_r by finding $\gcd(T_0(x) - T_i(x), \Phi_r(x))$ for each $i \in \mathbb{Z}/m\mathbb{Z}$. It would be interesting to know if we could quickly determine, given p and r, whether or not the traces for two different primitive roots of unity will be the same. Certainly, when $m = 1$ there will be only one trace and when $m = 2$, Lemma 13 of [2] shows that these traces cannot be the same. Similarly, when $d = 1$ the traces will be the roots themselves and so, as these are necessarily distinct, no two traces will be the same.

3. Statistical Observations

In order to get some idea of how often to expect duplicate traces to occur we can compare what we would expect to occur, if we assumed that traces fell 'randomly' in $\mathbb{F}_p$, to what actually occurs. In such a situation one would expect that 'random' selection would produce a normal distribution in the number of occurrences with a certain expected value and standard deviation.

In Table 1 we have listed all 411 cases with $r < p < 1000$ where two different primitive r^{th} roots of unity over $\mathbb{F}_p$ have the same trace. It should be noted that this is out of the 4365 instances where there exist primes r and p where $r < p < 1000$ with $m > 2$ and $d > 1$. Statistically, if we were to assume that these traces fell more or less 'randomly' in $\mathbb{F}_p$ then we would expect about 498.39 such instances with a standard deviation of about 15.15. The actual number of occurrences is therefore about 5.77 standard deviations below the expected value, suggesting that there are further instances where traces cannot repeat. A cursory glance at Table 1 shows that, for $r < p < 1000$ there are no instances of duplicate traces when $m = 2, 3$ or when $d = 2$. Assuming again that the traces fall 'randomly' we would expect that we would get duplicate traces in this range for $m = 2$ about 6.03 times with a standard deviation of 2.94, for $m = 4$ about 12.23 times with a standard deviation of about 3.45, and for $d = 2$ about 50.76 times with a standard deviation of about 3.50, or roughly 2.04, 3.54 and 14.52 standard deviations below the expected value, respectively. Thus suggesting that when $m \leq 4$ or $d \leq 2$, no two primitive r^{th} roots of unity will have the same trace. However, even when we eliminate these cases we would still expect that double traces would occur about 429.37 times with a standard deviation of about 5.18, or roughly 3.74 standard deviations above the actual value, suggesting that there are more cases which can be eliminated.

Along the same lines, it should be pointed out that zero appears as a trace less often than would be expected in a random distribution. With $r < p < 1000$ we would expect at least one of the primitive r^{th} roots of unity

to have a trace of zero about 89.07 times with a standard deviation of about 9.12, but it in fact occurs only 58 times [see Table 2], or about 3.41 standard deviations below the expected value. In Table 2 we note that zero does not appear as a trace for $r < p < 1000$ when $m = 3$ or $d = 2$, though we would expect it in the case $m = 3$ about 5.99 times with a standard deviation of about 2.42, and in the case $d = 2$ about 8.94 times with a standard deviation of about 2.69, or about 2.47 and 3.32 standard deviations below the expected value, respectively. Thus suggesting that when $m \leq 3$ or $d \leq 2$ no primitive r^{th} root of unity can have a trace of zero.

Table 1 - Cases where duplicate traces occur: $r < p < 1000$

p	r	d	m	Dist[1]	p	r	d	m	Dist	p	r	d	m	Dist
43	37	4	9	$1^7 2^1$	229	97	3	32	$1^{30} 2^1$	313	181	3	60	$1^{52} 2^4$
47	37	3	12	$1^{10} 2^1$	229	181	3	60	$1^{46} 2^7$	313	199	11	18	$1^{16} 2^1$
47	43	7	6	$1^4 2^1$	233	89	4	22	$1^{18} 2^2$	317	311	5	62	$1^{42} 2^{10}$
67	31	3	10	$1^8 2^1$	233	137	8	17	$1^{15} 2^1$	331	307	17	18	$1^{16} 2^1$
79	43	3	14	$1^{12} 2^1$	239	67	6	11	$1^9 2^1$	337	43	3	14	$1^{12} 2^1$
83	53	4	13	$1^{11} 2^1$	241	97	8	12	$1^{10} 2^1$	337	239	7	34	$1^{32} 2^1$
83	73	8	9	$1^7 2^1$	241	113	4	28	$1^{24} 2^2$	337	277	4	69	$1^{57} 2^6$
101	89	8	11	$1^9 2^1$	251	43	3	14	$1^{12} 2^1$	347	283	47	6	$1^4 2^1$
103	79	6	13	$1^{11} 2^1$	251	109	4	27	$1^{25} 2^1$	347	311	5	62	$1^{60} 2^1$
107	67	11	6	$1^4 2^1$	257	61	3	20	$1^{18} 2^1$	347	331	15	22	$1^{20} 2^1$
131	127	7	18	$1^{16} 2^1$	257	241	6	40	$1^{38} 2^1$	353	307	9	34	$1^{32} 2^1$
137	73	3	24	$1^{20} 2^2$	263	109	3	36	$1^{34} 2^1$	359	211	7	30	$1^{28} 2^1$
137	101	5	20	$1^{12} 2^4$	263	181	15	12	$1^{10} 2^1$	367	181	15	12	$1^{10} 2^1$
139	41	5	8	$1^6 2^1$	263	223	6	37	$1^{31} 2^3$	367	281	5	56	$1^{54} 2^1$
149	103	3	34	$1^{27} 2^2 3^1$	263	239	7	34	$1^{30} 2^2$	373	73	3	24	$1^{20} 2^2$
149	127	9	14	$1^{12} 2^1$	269	97	4	24	$1^{22} 2^1$	373	349	12	29	$1^{25} 2^2$
163	67	3	22	$1^{20} 2^1$	269	151	3	50	$1^{38} 2^6$	379	61	3	20	$1^{18} 2^1$
167	71	5	14	$1^{12} 2^1$	269	211	7	30	$1^{28} 2^1$	379	163	9	18	$1^{16} 2^1$
167	103	17	6	$1^4 2^1$	271	241	8	30	$1^{26} 2^2$	389	127	7	18	$1^{16} 2^1$
173	109	6	18	$1^{16} 2^1$	271	251	5	50	$1^{35} 2^6 3^1$	389	191	10	19	$1^{17} 2^1$
173	131	10	13	$1^{11} 2^1$	277	193	3	64	$1^{38} 2^{11} 4^1$	389	251	10	25	$1^{23} 2^1$
179	79	13	6	$1^4 2^1$	277	241	10	24	$1^{22} 2^1$	389	337	7	48	$1^{46} 2^1$
181	79	3	26	$1^{24} 2^1$	281	109	3	36	$1^{32} 2^2$	397	181	20	9	$1^7 2^1$
181	139	3	46	$1^{38} 2^4$	281	241	20	12	$1^{10} 2^1$	397	281	14	20	$1^{18} 2^1$
191	127	7	18	$1^{16} 2^1$	281	271	5	54	$1^{50} 2^2$	401	127	6	21	$1^{19} 2^1$
193	149	4	37	$1^{31} 2^3$	283	73	3	24	$1^{22} 2^1$	401	337	7	48	$1^{34} 2^7$
197	73	8	9	$1^7 2^1$	283	239	7	34	$1^{28} 2^3$	409	337	12	28	$1^{26} 2^1$
211	37	3	12	$1^{10} 2^1$	293	101	4	25	$1^{23} 2^1$	421	151	6	25	$1^{23} 2^1$
211	113	4	28	$1^{22} 2^3$	293	277	23	12	$1^{10} 2^1$	421	307	17	18	$1^{16} 2^1$
211	197	4	49	$1^{35} 2^7$	307	43	3	14	$1^{12} 2^1$	421	401	4	100	$1^{83} 2^7 3^1$
223	79	13	6	$1^4 2^1$	307	131	13	10	$1^8 2^1$	431	67	3	22	$1^{20} 2^1$
223	199	18	11	$1^9 2^1$	311	137	4	34	$1^{30} 2^2$	431	163	6	27	$1^{25} 2^1$
227	73	3	24	$1^{20} 2^2$	311	197	7	28	$1^{24} 2^2$	431	191	5	38	$1^{32} 2^3$
227	97	8	12	$1^{10} 2^1$	313	97	4	24	$1^{20} 2^2$	431	293	4	73	$1^{65} 2^4$
227	151	15	10	$1^8 2^1$	313	101	4	25	$1^{23} 2^1$	431	317	4	79	$1^{62} 2^7 3^1$

[1]For the distribution of the traces. For example, $1^{141} 2^{16} 3^3$ means that of the one hundred and eighty two total traces, one hundred and forty one occur only once, 16 occur twice, and three occur three times.

Table 1 - Continued

p	r	d	m	Dist	p	r	d	m	Dist	p	r	d	m	Dist
431	379	6	63	$1^{59}2^{2}$	509	461	4	115	$1^{85}2^{15}$	587	547	3	182	$1^{141}2^{16}3^{3}$
431	397	3	132	$1^{110}2^{8}3^{2}$	521	283	3	94	$1^{86}2^{4}$	593	71	5	14	$1^{12}2^{1}$
433	37	3	12	$1^{10}2^{1}$	521	337	48	7	$1^{5}2^{1}$	593	163	3	54	$1^{49}2^{1}3^{1}$
433	431	43	10	$1^{8}2^{1}$	521	419	11	38	$1^{34}2^{2}$	593	229	6	38	$1^{36}2^{1}$
439	67	3	22	$1^{20}2^{1}$	523	139	23	6	$1^{4}2^{1}$	593	241	16	15	$1^{13}2^{1}$
439	173	4	43	$1^{37}2^{3}$	523	307	17	18	$1^{14}2^{2}$	593	313	13	24	$1^{22}2^{1}$
443	157	4	39	$1^{37}2^{1}$	541	101	5	20	$1^{18}2^{1}$	593	397	9	44	$1^{40}2^{2}$
449	97	3	32	$1^{30}2^{1}$	541	449	8	56	$1^{52}2^{2}$	593	541	4	135	$1^{111}2^{12}$
457	421	14	30	$1^{26}2^{2}$	547	163	3	54	$1^{48}2^{3}$	593	547	13	42	$1^{40}2^{1}$
457	431	10	43	$1^{39}2^{2}$	547	313	13	24	$1^{22}2^{1}$	593	577	36	16	$1^{14}2^{1}$
461	151	5	30	$1^{26}2^{2}$	547	431	5	86	$1^{78}2^{4}$	599	61	4	15	$1^{13}2^{1}$
461	373	3	124	$1^{92}2^{16}$	557	73	4	18	$1^{16}2^{1}$	599	139	6	23	$1^{21}2^{1}$
461	397	22	18	$1^{16}2^{1}$	557	337	12	28	$1^{26}2^{1}$	599	173	4	43	$1^{39}2^{2}$
463	379	9	42	$1^{38}2^{2}$	557	491	70	7	$1^{5}2^{1}$	601	157	13	12	$1^{10}2^{1}$
463	409	6	68	$1^{60}2^{4}$	563	233	8	29	$1^{27}2^{1}$	601	211	21	10	$1^{8}2^{1}$
467	193	4	48	$1^{46}2^{1}$	563	337	8	42	$1^{38}2^{2}$	601	241	15	16	$1^{14}2^{1}$
467	241	6	40	$1^{38}2^{1}$	563	421	10	42	$1^{36}2^{3}$	601	313	4	78	$1^{66}2^{6}$
467	449	7	64	$1^{54}2^{5}$	563	499	83	6	$1^{4}2^{1}$	601	491	10	49	$1^{43}2^{3}$
487	337	28	12	$1^{10}2^{1}$	569	241	5	48	$1^{44}2^{2}$	601	577	4	144	$1^{126}2^{9}$
491	101	5	20	$1^{18}2^{1}$	569	271	10	27	$1^{25}2^{1}$	607	461	20	23	$1^{21}2^{1}$
491	149	4	37	$1^{31}2^{3}$	569	281	20	14	$1^{12}2^{1}$	617	397	12	33	$1^{31}2^{1}$
491	151	15	10	$1^{8}2^{1}$	569	353	32	11	$1^{9}2^{1}$	617	431	10	43	$1^{38}2^{1}3^{1}$
491	191	5	38	$1^{36}2^{1}$	571	103	3	34	$1^{32}2^{1}$	617	523	9	58	$1^{52}2^{3}$
491	409	17	24	$1^{22}2^{1}$	571	151	3	50	$1^{46}2^{2}$	617	601	265	24	$1^{22}2^{1}$
499	137	17	8	$1^{6}2^{1}$	571	271	6	45	$1^{41}2^{2}$	619	139	23	6	$1^{4}2^{1}$
499	157	4	39	$1^{37}2^{1}$	571	311	31	10	$1^{8}2^{1}$	619	239	14	17	$1^{15}2^{1}$
499	401	8	50	$1^{42}2^{4}$	571	433	48	9	$1^{7}2^{1}$	619	443	34	13	$1^{11}2^{1}$
499	421	35	12	$1^{10}2^{1}$	571	449	8	56	$1^{52}2^{2}$	619	601	15	40	$1^{36}2^{2}$
499	443	13	34	$1^{30}2^{2}$	571	461	10	46	$1^{44}2^{1}$	631	307	3	102	$1^{90}2^{6}$
499	457	19	24	$1^{22}2^{1}$	571	491	49	10	$1^{8}2^{1}$	631	313	8	39	$1^{31}2^{4}$
503	401	40	10	$1^{8}2^{1}$	577	131	5	26	$1^{24}2^{1}$	631	331	6	55	$1^{53}2^{1}$
503	431	43	10	$1^{8}2^{1}$	577	197	4	49	$1^{45}2^{2}$	631	433	3	144	$1^{120}2^{12}$
503	443	26	17	$1^{15}2^{1}$	577	521	104	5	$1^{3}2^{1}$	631	457	19	24	$1^{22}2^{1}$
509	281	4	70	$1^{58}2^{6}$	577	541	18	30	$1^{28}2^{1}$	641	281	7	40	$1^{38}2^{1}$
509	349	12	29	$1^{27}2^{1}$	587	331	15	22	$1^{20}2^{1}$	641	463	21	22	$1^{20}2^{1}$

Table 1 - Continued

p	r	d	m	Dist	p	r	d	m	Dist	p	r	d	m	Dist
643	97	3	32	$1^{30}2^{1}$	719	401	5	80	$1^{68}2^{6}$	787	151	3	50	$1^{48}2^{1}$
643	193	16	12	$1^{10}2^{1}$	719	487	3	162	$1^{122}2^{20}$	787	163	27	6	$1^{4}2^{1}$
647	211	3	70	$1^{66}2^{2}$	719	547	26	21	$1^{19}2^{1}$	787	241	4	60	$1^{54}2^{3}$
653	139	6	23	$1^{21}2^{1}$	727	241	12	20	$1^{18}2^{1}$	787	257	4	64	$1^{58}2^{3}$
653	397	11	36	$1^{32}2^{2}$	727	521	8	65	$1^{61}2^{2}$	787	373	31	12	$1^{10}2^{1}$
659	241	4	60	$1^{56}2^{2}$	733	241	30	8	$1^{6}2^{1}$	787	409	8	51	$1^{47}2^{2}$
659	541	27	20	$1^{18}2^{1}$	733	601	24	25	$1^{23}2^{1}$	787	433	8	54	$1^{50}2^{2}$
661	571	10	57	$1^{53}2^{2}$	733	647	19	34	$1^{32}2^{1}$	787	457	12	38	$1^{36}2^{1}$
661	631	14	45	$1^{41}2^{2}$	739	599	26	23	$1^{21}2^{1}$	787	673	32	21	$1^{19}2^{1}$
673	421	5	84	$1^{76}2^{4}$	743	181	4	45	$1^{41}2^{2}$	787	683	31	22	$1^{20}2^{1}$
673	457	38	12	$1^{10}2^{1}$	743	547	21	26	$1^{24}2^{1}$	787	757	27	28	$1^{26}2^{1}$
673	523	29	18	$1^{16}2^{1}$	743	617	14	44	$1^{42}2^{1}$	797	157	3	52	$1^{48}2^{2}$
673	547	21	26	$1^{24}2^{1}$	743	643	107	6	$1^{4}2^{1}$	809	97	8	12	$1^{10}2^{1}$
673	659	47	14	$1^{12}2^{1}$	751	313	8	39	$1^{33}2^{3}$	809	229	4	57	$1^{53}2^{2}$
673	661	15	44	$1^{42}2^{1}$	751	433	12	36	$1^{34}2^{1}$	809	379	3	126	$1^{108}2^{9}$
677	373	12	31	$1^{27}2^{2}$	751	641	10	64	$1^{60}2^{2}$	809	461	23	20	$1^{18}2^{1}$
677	443	34	13	$1^{11}2^{1}$	751	647	19	34	$1^{32}2^{1}$	809	541	12	45	$1^{41}2^{2}$
677	571	5	114	$1^{102}2^{6}$	757	157	4	39	$1^{37}2^{1}$	809	769	8	96	$1^{88}2^{4}$
677	673	24	28	$1^{24}2^{2}$	757	163	6	27	$1^{25}2^{1}$	811	97	3	32	$1^{30}2^{1}$
683	229	19	12	$1^{10}2^{1}$	757	401	8	50	$1^{46}2^{2}$	811	281	7	40	$1^{36}2^{2}$
683	421	12	35	$1^{33}2^{1}$	757	449	28	16	$1^{14}2^{1}$	811	599	13	46	$1^{40}2^{3}$
683	541	54	10	$1^{8}2^{1}$	757	541	12	45	$1^{43}2^{1}$	811	613	17	36	$1^{34}2^{1}$
691	193	4	48	$1^{44}2^{2}$	761	239	7	34	$1^{32}2^{1}$	811	617	4	154	$1^{128}2^{13}$
691	211	7	30	$1^{28}2^{1}$	769	419	22	19	$1^{17}2^{1}$	821	211	5	42	$1^{40}2^{1}$
691	683	22	31	$1^{29}2^{1}$	769	541	5	108	$1^{94}2^{7}$	821	229	3	76	$1^{71}2^{1}3^{1}$
701	97	4	24	$1^{22}2^{1}$	769	617	44	14	$1^{12}2^{1}$	821	241	5	48	$1^{42}2^{3}$
701	137	17	8	$1^{6}2^{1}$	769	631	18	35	$1^{33}2^{1}$	821	349	6	58	$1^{54}2^{2}$
701	149	4	37	$1^{35}2^{1}$	773	331	11	30	$1^{28}2^{1}$	821	421	3	140	$1^{122}2^{9}$
701	379	21	18	$1^{14}2^{2}$	773	401	5	80	$1^{78}2^{1}$	821	631	14	45	$1^{39}2^{3}$
701	397	9	44	$1^{40}2^{2}$	773	449	7	64	$1^{58}2^{3}$	821	643	6	107	$1^{95}2^{6}$
701	433	48	9	$1^{7}2^{1}$	773	613	9	68	$1^{64}2^{2}$	821	677	26	26	$1^{24}2^{1}$
709	223	6	37	$1^{35}2^{1}$	773	631	21	30	$1^{24}2^{3}$	823	43	3	14	$1^{12}2^{1}$
709	397	9	44	$1^{38}2^{3}$	773	673	112	6	$1^{4}2^{1}$	823	409	17	24	$1^{22}2^{1}$
719	453	4	13	$1^{11}2^{1}$	773	727	11	66	$1^{60}2^{3}$	823	491	7	70	$1^{66}2^{2}$
719	331	22	15	$1^{13}2^{1}$	787	113	7	16	$1^{14}2^{1}$	823	601	50	12	$1^{10}2^{1}$

Table 1 - Continued

p	r	d	m	Dist	p	r	d	m	Dist	p	r	d	m	Dist
823	691	5	138	$1^{117}2^{9}3^{1}$	883	379	7	54	$1^{51}3^{1}$	953	181	3	60	$1^{54}2^{3}$
823	751	3	250	$1^{179}2^{34}3^{1}$	883	617	22	28	$1^{26}2^{1}$	953	379	7	54	$1^{50}2^{2}$
823	761	8	95	$1^{85}2^{5}$	883	881	55	16	$1^{14}2^{1}$	953	443	17	26	$1^{22}2^{2}$
827	109	6	18	$1^{16}2^{1}$	887	743	53	14	$1^{12}2^{1}$	953	541	6	90	$1^{86}2^{2}$
827	151	25	6	$1^{4}2^{1}$	907	419	11	38	$1^{34}2^{2}$	967	947	86	11	$1^{9}2^{1}$
827	521	40	13	$1^{11}2^{1}$	907	547	21	26	$1^{24}2^{1}$	971	71	7	10	$1^{8}2^{1}$
829	211	3	70	$1^{60}2^{5}$	907	661	12	55	$1^{51}2^{2}$	971	197	4	49	$1^{47}2^{1}$
829	397	6	66	$1^{62}2^{2}$	911	349	4	87	$1^{73}2^{4}3^{2}$	971	337	16	21	$1^{19}2^{1}$
829	461	5	92	$1^{77}2^{6}3^{1}$	911	701	5	140	$1^{123}2^{7}3^{1}$	971	397	12	33	$1^{29}2^{2}$
829	523	18	29	$1^{27}2^{1}$	919	113	4	28	$1^{26}2^{1}$	971	631	63	10	$1^{8}2^{1}$
853	193	4	48	$1^{46}2^{1}$	919	163	3	54	$1^{50}2^{2}$	971	677	26	26	$1^{24}2^{1}$
853	541	9	60	$1^{56}2^{2}$	919	271	9	30	$1^{28}2^{1}$	971	859	39	22	$1^{20}2^{1}$
853	709	59	12	$1^{10}2^{1}$	919	373	12	31	$1^{27}2^{2}$	971	881	11	80	$1^{70}2^{5}$
853	809	8	101	$1^{93}2^{4}$	919	691	15	46	$1^{44}2^{1}$	971	919	3	306	$1^{216}2^{39}3^{4}$
857	181	6	30	$1^{28}2^{1}$	919	751	15	50	$1^{44}2^{3}$	977	541	45	12	$1^{10}2^{1}$
857	193	6	32	$1^{30}2^{1}$	929	601	24	25	$1^{23}2^{1}$	983	199	33	6	$1^{4}2^{1}$
857	397	4	99	$1^{83}2^{8}$	929	659	14	47	$1^{45}2^{1}$	983	313	13	24	$1^{21}3^{1}$
857	547	26	21	$1^{19}2^{1}$	929	673	6	112	$1^{103}2^{3}3^{1}$	983	631	10	63	$1^{59}2^{2}$
857	601	25	24	$1^{22}2^{1}$	929	761	5	152	$1^{134}2^{9}$	983	691	46	15	$1^{13}2^{1}$
859	137	4	34	$1^{32}2^{1}$	937	599	13	46	$1^{44}2^{1}$	983	751	30	25	$1^{23}2^{1}$
859	181	5	36	$1^{34}2^{1}$	937	709	6	118	$1^{101}2^{7}3^{1}$	983	859	13	66	$1^{56}2^{5}$
859	211	6	35	$1^{33}2^{1}$	941	463	11	42	$1^{38}2^{2}$	991	277	3	92	$1^{86}2^{3}$
859	499	6	83	$1^{79}2^{2}$	941	521	26	20	$1^{18}2^{1}$	991	523	9	58	$1^{50}2^{4}$
859	631	5	126	$1^{103}2^{10}3^{1}$	941	577	6	96	$1^{88}2^{4}$	997	331	15	22	$1^{20}2^{1}$
863	337	4	84	$1^{69}2^{6}3^{1}$	941	631	15	42	$1^{38}2^{2}$	997	461	20	23	$1^{21}2^{1}$
863	421	6	70	$1^{58}2^{6}$	941	811	3	270	$1^{213}2^{24}3^{3}$	997	823	3	274	$1^{204}2^{26}3^{6}$
863	449	16	28	$1^{24}2^{2}$	941	911	13	70	$1^{59}2^{4}3^{1}$					
863	769	64	12	$1^{10}2^{1}$	947	181	5	36	$1^{34}2^{1}$					
877	421	15	28	$1^{26}2^{1}$	947	277	3	92	$1^{86}2^{3}$					
877	491	7	70	$1^{64}2^{3}$	947	463	3	154	$1^{132}2^{11}$					
881	311	10	31	$1^{29}2^{1}$	947	617	77	8	$1^{6}2^{1}$					
881	313	26	12	$1^{10}2^{1}$	947	647	17	38	$1^{32}2^{3}$					
881	461	23	20	$1^{18}2^{1}$	947	827	59	14	$1^{12}2^{1}$					
881	661	11	60	$1^{58}2^{1}$	947	859	11	78	$1^{72}2^{3}$					
883	337	6	56	$1^{48}2^{4}$	947	929	8	116	$1^{104}2^{6}$					

Table 2 - Cases where 0 is a trace: $r < p < 1000$

p	r	d	m	p	r	d	m	p	r	d	m
47	37	3	12	431	191	5	38	739	241	6	40
59	41	5	8	433	431	43	10	739	541	15	36
79	43	3	14	443	281	35	8	757	281	10	28
101	71	7	10	491	409	17	24	761	727	33	22
131	61	5	12	491	421	28	15	773	181	6	30
131	109	27	4	503	373	93	4	787	373	31	12
137	71	10	7	541	79	13	6	809	277	69	4
211	73	6	12	563	379	14	27	821	229	3	76
233	197	7	28	571	271	6	45	821	349	6	58
251	211	14	15	571	353	44	8	857	661	165	4
277	193	3	64	617	67	11	6	881	673	21	32
281	241	20	12	619	239	14	17	883	307	17	18
283	73	3	24	619	601	15	40	919	163	3	54
293	79	6	13	653	313	13	24	919	271	9	30
311	229	57	4	653	397	11	36	937	599	13	46
337	181	30	6	673	569	71	8	941	811	3	270
367	241	16	15	677	571	5	114	953	541	6	90
389	269	67	4	683	607	101	6	983	631	10	63
401	241	15	16	719	401	5	80				
431	163	6	27	727	151	25	6				

REFERENCES

[1] G. Stein, *Factoring cyclotomic polynomials over large finite fields*, **Finite Fields and Applications**, London Mathematical Society Lecture Note Series #233, S. Cohen & R. Niederreiter, eds., Cambridge University Press, pp.349-354 (1996).

[2] G. Stein, *Factoring Cyclotomic Polynomials over Finite Fields*, Ph.D. Thesis, (1997).

DEPARTMENT OF MATHEMATICS, NEW YORK CITY TECH, THE CITY UNIVERSITY OF NEW YORK, 300 JAY STREET, BROOKLYN, NY 11201-2983, USA

E-mail address: gstein@broadway.gc.cuny.edu

This page intentionally left blank

Contemporary Mathematics
Volume **225**, 1999

THE FERMAT CURVE IN CHARACTERISTIC p

HENNING STICHTENOTH

ABSTRACT. We discuss three topics, where Fermat curves over a field of characteristic $p > 0$ arise quite naturally: (1) Automorphisms of curves. (2) Curves over finite fields with the maximum number of rational points. (3) Sequences of curves over finite fields with asymptotically many rational points.

1. Introduction

Let K be a field, $\bar{K} \supseteq K$ be its algebraic closure. The *Fermat curve of exponent n over K* is the projective plane curve $\mathcal{F}_n \subseteq \mathbb{P}^2(\bar{K})$ defined by the homogeneous equation

$$X^n + Y^n + Z^n = 0. \tag{1.1}$$

In case $K = \mathbb{Q}$, Fermat curves are intimately related to Fermat's last theorem, and there is no further need to give reasons why one should study these curves. The aim of this paper is to point out that Fermat curves are very interesting mathematical objects also in the case where the characteristic of K is not zero. Namely, it turns out that they arise quite naturally in various areas of the theory of algebraic curves in positive characteristic. We will discuss some of these aspects, certainly not all of them. For instance, we will not deal with the role of *Hermitian* curves in finite geometry (Hermitian curves over a field of characteristic $p > 0$ are the Fermat curves of exponent $n = 1 + q$, where q is some power of p). For this topic we refer to [6].

If K has positive characteristic $p > 0$ and $n = mp$ is a multiple of p, then equation (1.1) can be written as $X^{mp} + Y^{mp} + Z^{mp} = (X^m + Y^m + Z^m)^p = 0$ and is therefore reducible. If however the characteristic of K is relatively prime to n, then equation (1.1) is absolutely irreducible. In this case the Fermat curve $\mathcal{F}_n$ over K is easily seen to be non-singular, and therefore its genus is

$$g(\mathcal{F}_n) = \frac{1}{2}(n-1)(n-2), \quad \text{if char } K \nmid n. \tag{1.2}$$

2. Automorphisms of Algebraic Curves

In this section we assume that K is an *algebraically closed* field, and $\mathcal{X}$ is an irreducible, projective, non-singular algebraic curve over K. Let $g = g(\mathcal{X})$ denote the genus of $\mathcal{X}$. We consider the set of automorphisms of $\mathcal{X}$,

$$\mathrm{Aut}(\mathcal{X}) := \{f : \mathcal{X} \to \mathcal{X} \mid f \text{ is a birational map}\}.$$

This is clearly a group, and a classical result of Hurwitz [7] states that, for $K = \mathbb{C}$,

$$g(\mathcal{X}) \geq 2 \Rightarrow \mathrm{Aut}(\mathcal{X}) \text{ is finite.} \tag{2.1}$$

1991 *Mathematics Subject Classification.* Primary 14H05, 14G15; Secondary 11G20.

© 1999 American Mathematical Society

Hurwitz gave also an estimate for the order of $\mathrm{Aut}(\mathcal{X})$ as follows:

$$g(\mathcal{X}) \geq 2 \Rightarrow \text{ord } \mathrm{Aut}(\mathcal{X}) \leq 84(g(\mathcal{X}) - 1) \quad (\text{for } K = \mathbb{C}). \tag{2.2}$$

In fact, most curves of genus $g \geq 3$ have a trivial automorphism group; i.e. $\mathrm{Aut}(\mathcal{X}) = \{\mathrm{id}_{\mathcal{X}}\}$. This statement can be made more precise, see [11].

On the other hand, for infinitely many integers $g \geq 2$ there exists a curve $\mathcal{X}$ over $\mathbb{C}$ of genus $g(\mathcal{X}) = g$ with ord $\mathrm{Aut}(\mathcal{X}) = 84(g-1)$, see [18].

The finiteness of $\mathrm{Aut}(\mathcal{X})$ holds for all curves $\mathcal{X}$ of genus $g(\mathcal{X}) \geq 2$, over any algebraically closed field K. The estimate (2.2) remains true, whenever K has characteristic zero or $\mathrm{char}(K) = p > 0$ is sufficiently large with respect to the genus of the curve [12]. In general, (2.2) fails.

As an example we consider the automorphisms of the Fermat curve $\mathcal{F}_n$ over K (as always we assume that n is relatively prime to the characteristic of K). For all $n \geq 4$, the group $\mathrm{Aut}(\mathcal{F}_n)$ is finite, as follows from (1.2) and (2.1). There are some obvious automorphisms $f \in \mathrm{Aut}(\mathcal{F}_n)$:

(i) $(a : b : c) \mapsto (\zeta a : \eta b : c)$ with $\zeta^n = \eta^n = 1$.

Here we denote by $(a : b : c) \in \mathbb{P}^2(K)$ a point of $\mathcal{F}_n$, hence $a^n + b^n + c^n = 0$.

(ii) The permutations of the 3 coordinates of $\mathbb{P}^2(K)$ yield automorphisms of $\mathcal{F}_n$.

There are n^2 automorphisms of type (i) and 6 automorphisms of type (ii); altogether they generate a subgroup

$$G \subseteq \mathrm{Aut}(\mathcal{F}_n) \text{ with } \mathrm{ord}(G) = 6n^2.$$

Since $g(\mathcal{F}_n) = \frac{1}{2}(n-1)(n-2)$, we have that $\mathrm{ord}(G) \approx 12 \cdot g(\mathcal{F}_n)$, so the Fermat curves have rather many automorphisms according to their genus.

For most values of n, the group G above is the full automorphism group of $\mathcal{F}_n$; more precisely one has the following result [9]:

For $n \neq 1 + q$, where q is a power of $p = \mathrm{char}\, K$, one has ord $\mathrm{Aut}(\mathcal{F}_n) = 6n^2$. (2.3)

In the "exceptional" case $n = 1 + q$ (q being a power of the characteristic of K), the Fermat curve $\mathcal{F}_{1+q}$ is often referred to as the *Hermitian* curve; this curve turns out to be particularly interesting (cf. also Sec. 3 below). The defining equation (1.1) of the Hermitian curve can be written as

$$X \cdot X^q + Y \cdot Y^q + Z \cdot Z^q = 0. \tag{2.4}$$

From (2.4) we see immediately that any 3×3-matrix A with coefficients in $\mathbb{F}_{q^2} \subseteq K$ satisfying the condition

$${}^tA \cdot A^q = E \tag{2.5}$$

defines an automorphism $f \in \mathrm{Aut}(\mathcal{F}_{1+q})$ via

$$f(a : b : c) = (a : b : c) \cdot {}^tA.$$

(${}^tA$ is the transpose of A, and for $A = (a_{ij})$ we write $A^q = (a_{ij}^q)$.) In this manner we find a subgroup $H \subseteq \mathrm{Aut}(\mathcal{F}_{1+q})$ being isomorphic to the projective unitary group $PGU(3, q^2)$ of order

$$\text{ord } H = q^3(q^2 - 1)(q^3 + 1). \tag{2.6}$$

Note that all automorphisms $f \in H$ are already defined over the finite field $\mathbb{F}_{q^2}$. One can show [9] that H is in fact the full automorphism group of the Hermitian curve $\mathcal{F}_{1+q}$. Comparing the order of H with the genus $g(\mathcal{F}_{1+q}) = q(q-1)/2$, we see that

$$\text{ord Aut}(\mathcal{F}_{1+q}) > 16 \cdot g(\mathcal{F}_{1+q})^4, \tag{2.7}$$

and hence there is no linear bound like (2.2) of the form

$$\text{ord Aut}(\mathcal{X}) \leq \text{const} \cdot g(\mathcal{X})$$

for the automorphism group of a curve $\mathcal{X}$ over a constant field of characteristic $p > 0$.

These examples of some Fermat curves with "many" automorphisms are noteworthy with regard to the following result [5], [15]:

Theorem 2.1 *Let K be an algebraically closed field, $\mathcal{X}$ an irreducible, projective, non-singular curve over K of genus $g(\mathcal{X}) \geq 2$. Then,*

$$\text{ord Aut}(\mathcal{X}) \leq 16 \cdot g(\mathcal{X})^4,$$

except $\mathcal{X}$ is isomorphic to an Hermitian curve $\mathcal{X} \simeq \mathcal{F}_{1+q}$, where q is some power of $p = \text{char } K$.

3. Rational Points on Curves over Finite Fields

From here on we work over a finite field $K = \mathbb{F}_q$, where $q = p^\nu$ is a power of a prime number p. The curve $\mathcal{X}$ is an absolutely irreducible, projective, non-singular curve defined over $\mathbb{F}_q$, and $\mathcal{X}(\mathbb{F}_q)$ denotes the set of $\mathbb{F}_q$-rational points on $\mathcal{X}$. Let $N(\mathcal{X}) = |\mathcal{X}(\mathbb{F}_q)|$ be the cardinality of $\mathcal{X}(\mathbb{F}_q)$. The Hasse-Weil theorem states that

$$|N(\mathcal{X}) - (q+1)| \leq 2g(\mathcal{X}) \cdot \sqrt{q}, \tag{3.1}$$

and we call $\mathcal{X}$ to be *maximal* if the upper bound in (3.1) is attained; i.e.,

$$N(\mathcal{X}) = q + 1 + 2g(\mathcal{X}) \cdot \sqrt{q}. \tag{3.2}$$

Unless $g(\mathcal{X}) = 0$ (in this case $\mathcal{X}$ is isomorphic to the projective line $\mathcal{X} \simeq \mathbb{P}^1(\mathbb{F}_q)$), maximal curves can exist only when q is a square (trivial from (3.2)).

We will now show that specific Fermat curves are maximal: let $q = l^2$ be a square, and consider the Hermitian curve $\mathcal{X} = \mathcal{F}_{1+l}$ over $\mathbb{F}_q$. We determine the points $P = (a : b : c) \in \mathcal{X}(\mathbb{F}_q)$.

(i) $c = 1$, so $P = (a : b : 1)$. We can choose $b \in \mathbb{F}_q$ arbitrarily; then a must satisfy the equation

$$a^{l+1} = -1 - b^{l+1}. \tag{3.3}$$

If $b^{l+1} = -1$, then $a = 0$ and

$$P = (0 : b : 1) \in \mathcal{X}(\mathbb{F}_q). \tag{3.4}$$

If $b^{l+1} \neq -1$, then $-1 - b^{l+1}$ is a non-zero element in $\mathbb{F}_l$, and equation (3.3) has $l+1$ distinct roots $a \in \mathbb{F}_q$. Hence we find for any $b \in \mathbb{F}_q$ with $b^{l+1} \neq -1$ exactly $l+1$ points

$$P = (a : b : 1) \in \mathcal{X}(\mathbb{F}_q). \tag{3.5}$$

Note that $b^{l+1} \neq -1$ holds for exactly $l^2 - (l+1)$ elements $b \in \mathbb{F}_q$.

(ii) $c = 0$, so $P = (a : 1 : 0)$. Since $a^{l+1} + 1 = 0$ has $l + 1$ roots $a \in \mathbb{F}_q$, we find exactly $l + 1$ points of the form

$$P = (a : 1 : 0) \in \mathcal{X}(\mathbb{F}_q). \tag{3.6}$$

Counting all points $P \in \mathcal{X}(\mathbb{F}_q)$ as given by (3.4), (3.5) and (3.6) we find that

$$\begin{aligned} N(\mathcal{X}) &= (l+1) + (l^2 - (l+1)) \cdot (l+1) + (l+1) \\ &= (l+1)(l^2 - l + 1) = l^3 + 1. \end{aligned}$$

On the other hand, since $g(\mathcal{X}) = l(l-1)/2$, we have that

$$q + 1 + 2g(\mathcal{X}) \cdot \sqrt{q} = l^2 + 1 + l(l-1) \cdot l = l^3 + 1.$$

Hence the Hermitian curve $\mathcal{X} = \mathcal{F}_{1+l}$ is maximal over $\mathbb{F}_{l^2}$ of genus $g(\mathcal{X}) = l(l-1)/2$.

Hermitian curves are not the only examples of maximal curves among the Fermat curves. One can show that for all exponents n dividing $l + 1$, the Fermat curve $\mathcal{F}_n$ is a maximal curve over the field $\mathbb{F}_{l^2}$.

In this context the following theorem is interesting, see [2], [13]:

Theorem 3.1 *Let $\mathcal{X}$ be any maximal curve over the field $K = \mathbb{F}_{l^2}$. Then we have:*

(i) $g(\mathcal{X}) \leq l(l-1)/2$.

(ii) *If $g(\mathcal{X}) > (l-1)^2/4$, then $\mathcal{X}$ is isomorphic to the Hermitian curve of exponent $l + 1$; i.e.,*

$$\mathcal{X} \simeq \mathcal{F}_{l+1} \quad \textit{and} \quad g(\mathcal{X}) = l(l-1)/2.$$

To conclude the results of Sections 2 and 3: Certain Fermat curves in characteristic $p > 0$ have "extremal" properties, and they are uniquely determined by these properties.

4. Asymptotically Good Sequences of Curves

As before, $K = \mathbb{F}_q$ is a finite field. We consider sequences $\underline{\mathcal{X}} = (\mathcal{X}_1, \mathcal{X}_2, \dots)$ of curves $\mathcal{X}_i$ over $\mathbb{F}_q$ with $g(\mathcal{X}_i) \to \infty$ and define

$$\lambda(\underline{\mathcal{X}}) := \limsup_{i \to \infty} N(\mathcal{X}_i)/g(\mathcal{X}_i). \tag{4.1}$$

From the Hasse-Weil bound (3.2) follows immediately that

$$0 \leq \lambda(\underline{\mathcal{X}}) \leq 2 \cdot \sqrt{q} \tag{4.2}$$

holds for any sequence $\underline{\mathcal{X}}$; however the upper bound in (4.2) is essentially improved by the Drinfeld-Vladut bound

$$\lambda(\underline{\mathcal{X}}) \leq \sqrt{q} - 1. \tag{4.3}$$

We call the sequence $\underline{\mathcal{X}} = (\mathcal{X}_1, \mathcal{X}_2, \dots)$ *asymptotically good* if $\lambda(\underline{\mathcal{X}}) > 0$, and *asymptotically optimal* if $\lambda(\underline{\mathcal{X}}) = \sqrt{q} - 1$. Otherwise, if $\lambda(\underline{\mathcal{X}}) = 0$, the sequence is *asymptotically bad.*

It seems to be difficult to find examples of asymptotically good sequences of curves. For instance, if all curves $\mathcal{X}_i$ are abelian coverings of a fixed curve $\mathcal{X}_0$ (for $i = 1, 2, \dots$), then the sequence $\underline{\mathcal{X}} = (\mathcal{X}_1, \mathcal{X}_2, \dots)$ is asymptotically bad [1].

The following two constructions of asymptotically good sequences of curves are known for some time:

A Ihara [8] and Tsfasman-Vladut-Zink [17] showed that certain sequences of (classical, resp. Shimura, resp. Drinfeld) modular curves over $\mathbb{F}_q$, where $q = l^2$ is a square, are asymptotically optimal. Tsfasman, Vladut and Zink observed that this implies the existence of "asymptotically good sequences of codes" which improve the Gilbert-Varshamov bound (a well-known bound in coding theory), for all $l^2 \geq 49$.

B Using infinite class field towers, Serre [14] constructed asymptotically good (not optimal) sequences of curves over any finite field. This method was later refined by several authors, cf. [10].

Now we present two recent constructions by Garcia and Stichtenoth of asymptotically good sequences of curves. Both constructions are based on Fermat curves; they are quite explicit and more elementary than A and B.

C 1 (see [4]) Assume that q is not a prime number. We set $m = (q-1)/(p-1)$ with $p = \text{char } \mathbb{F}_q$ and consider the affine curve $\mathcal{Z}_m \subseteq \mathbb{A}^n(\bar{\mathbb{F}}_q)$ which is defined by $n-1$ "Fermat equations"

$$X_{i+1}^m + (X_i + 1)^m = 1, \quad i = 1, \ldots, n-1. \tag{4.4}$$

Let $\mathcal{X}_n$ be the non-singular projective model of $\mathcal{Z}_n$. This sequence of curves $\underline{\mathcal{X}} = (\mathcal{X}_1, \mathcal{X}_2, \ldots)$ yields a tower of coverings

$$\ldots \to \mathcal{X}_{n+1} \to \mathcal{X}_n \to \ldots \to \mathcal{X}_2 \to \mathcal{X}_1. \tag{4.5}$$

The coverings $\mathcal{X}_{n+1} \to \mathcal{X}_n$ are tamely ramified Galois coverings of degree m, and the only points in $\mathcal{X}_1 = \mathbb{P}^1(\bar{\mathbb{F}}_q)$ which ramify in the covering $\mathcal{X}_n \to \mathcal{X}_1$ are $X_1 = \alpha$ with $\alpha \in \mathbb{F}_q$. It follows easily from the Riemann-Hurwitz genus formula that

$$g(\mathcal{X}_n) \leq \frac{1}{2}(q-2)m^{n-1}. \tag{4.6}$$

On the other hand, the point $X_1 = \infty$ splits completely in the covering $\mathcal{X}_n \to \mathcal{X}_1$, hence

$$N(\mathcal{X}_n) \geq m^{n-1}. \tag{4.7}$$

From the inequalities (4.6) and (4.7) follows immediately:

Theorem 4.1 *The sequence $\underline{\mathcal{X}} = (\mathcal{X}_1, \mathcal{X}_2, \ldots)$ of curves over $\mathbb{F}_q$ (q not a prime) which is defined by* (4.4) *is asymptotically good with*

$$\lambda(\underline{\mathcal{X}}) \geq 2/(q-2).$$

Note that the sequence $\underline{\mathcal{X}}$ in Theorem 4.1 is optimal for $q = 4$, since $2/(q-2) = 1 = \sqrt{q} - 1$ (the Drinfeld-Vladut bound) in this case.

We give yet another construction of a sequence of curves that is also based on Fermat curves.

C 2 (see [3]). We assume that $q = l^2$ is a square. The Fermat curve $\mathcal{F}_{l+1}$ over $K = \mathbb{F}_q$ (which is the Hermitian curve) is given by the homogeneous equation $X^{1+l} + Y^{1+l} + Z^{1+l} = 0$, so its function field is

$$F = \mathbb{F}_q(u, v) \quad \text{with} \quad u^{1+l} + v^{1+l} + 1 = 0. \tag{4.8}$$

We choose $\alpha, \beta \in \mathbb{F}_q$ such that $\alpha^l + \alpha = \beta^{l+1} = -1$ and set

$$z = (1+\alpha)u - \alpha\beta^{-1}v, \quad w = \beta(v - \beta u)^{-1}.$$

Then $\mathbb{F}_q(u,v) = \mathbb{F}_q(z,w)$, and one checks that $(zw)^l + zw = w^{l+1}$. The Fermat curve $\mathcal{F}_{1+l}$ is therefore birationally equivalent to the affine plane curve which is defined by

$$Z^l W^{l-1} + Z = W^l. \tag{4.9}$$

Now we proceed as in construction C 1. We consider the affine curve $\mathcal{Z}_n \subseteq \mathbb{A}^n(\bar{\mathbb{F}}_q)$ given by $n-1$ equations

$$X_{i+1}^l X_i^{l-1} + X_{i+1} = X_i^l, \quad i = 1, \ldots n-1. \tag{4.10}$$

Theorem 4.2 *Let $q = l^2$ and $\mathcal{X}_n$ be the non-singular model of the curve $\mathcal{Z}_n$ defined by* (4.10). *Then the sequence $\underline{\mathcal{X}} = (\mathcal{X}_1, \mathcal{X}_2, \ldots)$ is an asymptotically optimal sequence of curves over $\mathbb{F}_q$; i.e. $\lambda(\underline{\mathcal{X}}) = l - 1$.*

The idea of proof is similar as in Theorem 4.1. One has a tower of coverings

$$\ldots \to \mathcal{X}_{n+1} \to \mathcal{X}_n \to \ldots \to \mathcal{X}_2 \to \mathcal{X}_1.$$

Each step $\mathcal{X}_{n+1} \to \mathcal{X}_n$ is Galois of degree l, and all points $P \in \mathcal{X}_1 = \mathbb{P}^1(\bar{\mathbb{F}}_q)$ with $X_1 = \alpha \in \mathbb{F}_q \setminus \{0\}$ split completely in $\mathcal{X}_n \to \mathcal{X}_1$. Thus

$$N(\mathcal{X}_n) \geq (l^2 - 1) \cdot l^{n-1}. \tag{4.11}$$

Only two points of $\mathcal{X}_1$ are ramified in $\mathcal{X}_n \to \mathcal{X}_1$, namely $X_1 = 0$ and $X_1 = \infty$. As l is a power of the characteristic, ramification is wild. Due to this fact the computation of the genus $g(\mathcal{X}_n)$ is more difficult than in Theorem 4.1; the result is [3]

$$g(\mathcal{X}_n) = l^{n-1}(l+1) + \mathcal{O}(l^{n/2}), \tag{4.12}$$

as $n \to \infty$. From (4.11) and (4.12) we obtain $\lambda(\underline{\mathcal{X}}) = l - 1 = \sqrt{q} - 1$, as desired.

5. References

1. G. Frey, M. Perret, H. Stichtenoth, *On the different of abelian extensions of global fields*, in *Coding Theory and Algebraic Geometry*, H. Stichtenoth and M. A. Tsfasman, Eds., Springer LNM no. **1518** (1992), pp. 26 - 32.
2. R. Fuhrmann, F. Torres, *The genus of curves over finite fields with many rational points*, Manuscr. Math. **89** (1996), 103 - 106.
3. A. Garcia and H. Stichtenoth, *A tower of Artin-Schreier extensions of function fields attaining the Drinfeld-Vladut bound*, Invent. Math. **121** (1995), 211 - 222.
4. A. Garcia, H. Stichtenoth and M. Thomas, *On Towers and Composita of Towers of Function Fields over Finite Fields*, Finite Fields and Appl. **3** (1997), 257 - 274.
5. H.-W. Henn, *Funktionenkörper mit großer Automorphismengruppe*, J. Reine Angew. Math. **172** (1978), 96 - 115.
6. J. W. P. Hirschfeld, *Projective Geometries over Finite Fields*, Oxford Univ. Press, Oxford, 1979.
7. A. Hurwitz, *Über algebraische Gebilde mit eindeutigen Transformationen in sich*, Math. Ann. **41** (1893), 403 - 442.
8. Y. Ihara, *Some remarks on the number of rational points of algebraic curves over finite fields*, J. Fac. Sci. Tokyo **28** (1981), 721 - 724.
9. H.-W. Leopoldt, *Über die Automorphismengruppe des Fermatkörpers*, J. Number Th. **56** (1996), 256 - 282.
10. H. Niederreiter, C. P. Xing, *Global function fields with many rational places and their applications*, this volume.
11. H. Popp, *The Singularities of the Moduli Schemes of Curves*, J. Number Th. **1** (1969), 90 - 107.
12. P. Roquette, *Abschätzung der Automorphismenanzahl von Funktionenkörpern bei Primzahlcharakteristik*, Math. Z. **117** (1970), 157 - 163.
13. H. G. Rück, H. Stichtenoth, *A characterization of Hermitian function fields over finite fields*, J. Reine Angew. Math. **457** (1994), 185 - 188.
14. J.-P. Serre, *Rational Points on Curves over Finite Fields*, Notes by F. Q. Gouvéa from Lectures given at Harvard Univ., 1985.
15. H. Stichtenoth, *Über die Automorphismengruppe eines algebraischen Funktionenkörpers von Primzahlcharakteristik I, II*, Arch. Math. **24** (1973), 527 - 544 and 615 - 631.
16. H. Stichtenoth, *Algebraic Function Fields and Codes*, Springer, Berlin-Heidelberg-New York, 1993.
17. M. A. Tsfasman, S. G. Vladut, T. Zink, *Modular curves, Shimura curves and Goppa codes, better than the Varshamov-Gilbert bound*, Math. Nachr. **109** (1982), 21 - 28.
18. P. Turbek, *On compact Riemann surfaces with a maximal number of automorphisms*, Manuscr. Math. **80** (1993), 113 - 130.

FACHBEREICH 6, MATHEMATIK UND INFORMATIK, UNIVERSITÄT GH ESSEN, UNIVERSITÄTSSTRASSE 3, 45117 ESSEN, GERMANY

E-mail address: stichtenoth@uni-essen.de

This page intentionally left blank

Contemporary Mathematics
Volume **225**, 1999

Computing Zeta Functions Over Finite Fields

Daqing Wan

ABSTRACT. In this report, we discuss the problem of computing the zeta function of an algebraic variety defined over a finite field, with an emphasis on computing the reduction modulo p^m of the zeta function of a hypersurface, where p is the characteristic of the finite field.

1991 Mathematics Subject Classification: 11Y16, 11T99, 14Q15.

1. Introduction

Let p be a prime number. Let $\mathbb{F}_q$ be a finite field of q elements of characteristic p. Let X be an algebraic variety defined over $\mathbb{F}_q$, say an affine variety defined by the vanishing of r polynomials in n variables:

$$f_1(x_1, \cdots, x_n) = \cdots = f_r(x_1, \cdots, x_n) = 0,$$

where the polynomials f_i have coefficients in $\mathbb{F}_q$. Let $N(X)$ denote the number of $\mathbb{F}_q$-rational points on X.

PROBLEM I. *Compute $N(X)$ efficiently.*

In addition to its intrinsic theoretical interest, this fundamental algorithmic problem has important applications in diverse areas such as coding theory, cryptography, primality testing, sphere packing, quasi-random number generator and fast multiplication. It is also very useful in bounding the number of torsion points of an abelian variety over a number field.

In principal, one can always check all the q^n possibilities for $(x_1, \cdots, x_n)$. This is apparently very slow if either q or n is large. One would like to have faster non-trivial algorithms. In this paper, we discuss only deterministic algorithms in theoretical sense and we shall frequently use less precise but intuitive description.

For varieties with large automorphism groups (such as diagonal hypersurfaces), it is possible to find efficient elementary methods (such as Gauss sums) to compute $N(X)$. We shall, however, restrict to those methods which have potential to extend to general varieties.

In the special case that X is an elliptic curve

$$E: \ y^2 = x^3 + ax + b, \ a, b \in \mathbb{F}_q,$$

© 1999 American Mathematical Society

a polynomial time algorithm was obtained by Schoof [Sc1]. More practical but probabilistic versions were obtained later by Atkin, Elkies, Couveignes and a few other authors, see [Sc2] for an updated exposition. Schoof 's algorithm was generalized to abelian varieties and curves by Pila [Pi] with some improvements by Adleman-Huang [AH]. Curves and abelian varieties are the cases which have been studied most extensively in the literature. For more general varieties, no non-trivial algorithm is known unless the variety is defined over a small subfield of $\mathbb{F}_q$. It is shown in [GKS] that this problem is #P-hard (at least NP-hard) for sparse plane curves if one uses sparse input size. Thus, in order to get efficient algorithms to compute $N(X)$, one might need to put some restrictions on some of the parameters of $X/\mathbb{F}_q$, such as the dimension, degree, characteristic p, etc.

For each positive integer k, let $\mathbb{F}_{q^k}$ be the finite field of q^k elements. This is the unique extension field of $\mathbb{F}_q$ of degree k. Let $N_k(X)$ denote the number of $\mathbb{F}_{q^k}$-rational points on X. We shall consider the following harder problem.

PROBLEM II. *Compute the sequence* $\{N_k(X)\}_{k=1}^{\infty}$ *efficiently.*

For fixed n, Problem I is easy if q is small. One can simply check all q^n possibilities for $x \in \mathbb{F}_q^n$. On the other hand, Problem II can already be hard even for small q as q^k will be large for large k. Nevertheless, one can still hope to find efficient algorithms in important cases that arise from various applications.

The sequence $N_k(X)$ has a nice structure. In fact, by Dwork's theorem [Dw], the generating zeta function

$$Z(X,T) = \exp(\sum_{k=1}^{\infty} \frac{N_k(X)}{k} T^k)$$

is a rational function. Thus, the sequence $N_k(X)$ satisfies a linear recurrence relation. Write

$$Z(X,T) = \frac{g(T)}{h(T)}$$

for some polynomials $g(T), h(T) \in \mathbb{Z}[T]$. Taking logarithmic derivative, one finds

$$\sum_{k=1}^{\infty} N_k(X) T^{k-1} = \frac{g'(T)}{g(T)} - \frac{h'(T)}{h(T)}.$$

Thus, Problem II is equivalent to

PROBLEM III. *Compute the zeta function* $Z(X,T)$ *efficiently.*

If an efficient algorithm to compute $N(X)$ is known, then one can continue to compute $N_k(X)$ for all positive integers k up to something like the "degree" of the zeta function $Z(X,T)$. This easily leads to what I called the naive algorithm to compute $Z(X,T)$. It works well if the degree of $Z(X,T)$ is small and if one knows how to compute $N(X)$ efficiently. In particular, one obtains a good algorithm if the degree of $Z(X,T)$ is small and if X is defined over a small subfield of $\mathbb{F}_q$ (q can be large). But the degree of the zeta function can be very large. For a smooth projective hypersurface of dimension n and large degree d, the degree of the zeta function is about the size d^{n+1}.

For an elliptic curve E, the zeta function is determined by $N_1(E)$:

$$Z(E,T) = \frac{1 + c(E)T + qT^2}{(1-T)(1-qT)},$$

where $c(E) = N_1(E) - (q+1)$. Thus, the zeta function $Z(E,T)$ can be computed efficiently by Schoof's work. More generally, when X is an abelian variety of a fixed dimension embedded in a fixed projective space, the zeta function $Z(X,T)$ can also be computed efficiently by the work of Pila and Adleman-Huang.

For a non-singular plane curve of large degree d over a small finite field $\mathbb{F}_q$ ($q = 2$ or 3 for instance), computing $N_1(X)$ is easy since q is small. Even in this special case, computing $Z(X,T)$ already seems to be difficult as Katz-Sarnak pointed out [Po]. This case was motivated by their investigation of the distribution of the zeros and poles of zeta functions. The results of Adleman-Huang give a doubly exponential algorithm for a general plane curve, although they have a significantly faster algorithm for hyperelliptic curves (still exponential in terms of the degree). This is far from being practical if the degree is large.

Computing the zeta function of a hyperellitptic curve is very useful in the hyperelliptic curve cryptosystem proposed by Koblitz [Ko1-2]. Additional applications may be found in [AH2], [AG] and [Ts]. Computing zeta functions of algebraic varieties should also be the first key step in computing zeta functions of more general Hilbert sets and definable sets, see [Wa1] and [FHJ]. A very special case is already considered in [GKS].

Our purpose here is to give a brief general discussion of the modular approach for computing zeta functions, indicating some theoretical tools that are available and some realistic results that one might hope. As supporting evidence, we shall also describe some elementary theorems on computing the reduction of $Z(X,T)$ modulo p^m.

2. Modular approach for computing zeta functions

Let X be an algebraic variety defined over a finite field $\mathbb{F}_q$. The degree of $Z(X,T)$ can be estimated explicitly using p-adic methods as done by Bombieri [Bo]. The size of the coefficients in $Z(X,T)$ can also be bounded easily using trivial estimate. In nicer cases, one can use Deligne's deep result [De] to get better bounds. The general modulo idea to compute $Z(X,T)$ consists of two steps. The first step is to compute $Z(X,T)$ modulo various small primes (or prime powers). The second step is to use the Chinese remainder theorem to recover $Z(X,T)$ from its various reductions. The second step is pretty easy and standard. The difficulty lies in the first step, namely, computing the reduction of $Z(X,T)$ modulo various small primes or prime powers.

Zeta functions of higher dimensional varieties over finite fields have been studied extensively from theoretic point of view, motivated by Weil's conjectures. Several theories are available but all of them are highly non-trivial and fairly difficult. They can be broadly classified as ℓ-adic methods and p-adic methods, where ℓ is any prime number different from p. In this section, we give a brief speculative discussion and perspective about the potential of these methods in computing zeta functions. No results and/or theorems are given in this section.

ℓ-adic methods. One can try to use Grothendieck's ℓ-adic trace formula [Gr] modulo ℓ^m:

$$Z(X,T) \equiv \prod_{i=0}^{2\dim(X)} \det(I - FT | H_c^i(X \otimes_{\mathbb{F}_q} \bar{\mathbb{F}}_q, \mathbb{Z}/\ell^m\mathbb{Z})^{(-1)^{i-1}} \pmod{\ell^m},$$

where H_c^i denotes the ℓ-adic étale cohomology with compact support and F is the geometric Frobenius map acting on H_c^i. Unfortunately, in the general case, one does not know how to explicitly construct the ℓ-adic cohomology and its Frobenius map. In fact, for singular or open varieties, one does not even know any explicit bound for the dimension of the ℓ-adic cohomology H_c^i. Thus, a major future research problem is to make the ℓ-adic theory constructive and explicit. If successful, it would have dramatic consequence on the problem of counting the number of rational points of a variety over a finite field.

In the special case of elliptic curves and abelian varieties, the ℓ-adic cohomology can be constructed quite explicitly using torsion points and division polynomials. This immediately leads to the algorithms of Schoof for elliptic curves and Pila for abelian varieties. For a smooth curve X of genus g, one can use its Jacobian variety (an abelian variety) and Pila's algorithm to compute the zeta function $Z(X,T)$ of the curve X, as done by Adleman-Huang. This algorithm is in general at least doubly exponential in g. In the case of hyperelliptic curve, the running time has been improved to be exponential in g. Thus it is still a very slow algorithm if g is large. If g is very small, this gives a good polynomial time algorithm. To conclude, even for smooth plane curves of large degrees over a small finite field, there is still no efficient algorithm to compute the zeta function. If X is singular, there is also a problem of resolving the singularities if one wants to use this approach.

p-adic methods. There are various p-adic formulas for $Z(X,T)$. All of them can be made to be explicit in some sense. The earliest one is due to Dwork, with generalizations by Reich-Monsky [Mo]. There are also p-adic cohomological formulas in terms of formal cohomology, crystalline cohomology and rigid cohomology [Ber]. We believe that some of these formulas and their variants can be very useful in computing the zeta function in the general case if the characteristic p is not too large. In particular, we expect it to be plausible to construct a p-adic algorithm to compute $Z(X,T)$, which runs in polynomial time (in the input and output size) if X is sparse and the characteristic p is small (q can be large). This is exactly the case that is most useful in coding theory and cryptography. A weak corollary would be a polynomial time algorithm to compute $N(X)$ for X of low degrees over a large finite field of small characteristic. Note that an elliptic curve is sparse and of low degree. If p is very large, we do not even know how to efficiently compute the reduction $Z(X,T)$ modulo p.

It is worthwhile to mention that the p-adic étale cohomological approach is not suitable for computing the whole zeta function. This is because the p-adic étale formula gives only the p-adic unit root part of the zeta function, not the whole thing, as conjectured by Katz [Ka1] and proved in the zeta case by Etesse-Le Stum [ES].

Our general feeling is as follow. If p is small (q can be large), p-adic methods should be much more efficient. If p is large and the degree of X is small, then ℓ-adic methods should be better assuming that the ℓ-adic cohomology can be constructed explicitly. If both p and the degree are large, it is not clear if the p-adic methods or the ℓ-adic methods would work very well. A combination of both p-adic methods and ℓ-adic methods could be useful in certain situations.

For p-adic methods, the major advantage is that everything can be made to be explicit. This at least provides explicit algorithms which work in the general case

and which are faster in many cases than the trivial counting method. Another possible advantage is that p-adic methods easily extend to L-functions of exponential sums with the same complexity bound. The drawback is that one does not have any flexibility to choose any other (small) prime to work with (unlike the ℓ-adic case). Thus, if p is large, one is stuck and even the modulo p information is already something quite substantial.

For ℓ-adic methods, the major advantage is that one can always choose many small primes $\ell \neq p$ to work with. One expects that it would be easier and more efficient to compute $Z(X,T)$ modulo a small prime. However, the ℓ-adic cohomology is not explicit yet and thus one does not even know how to compute $Z(X,T)$ using ℓ-adic methods in general. Even if the ℓ-adic methods are made explicit, the resulting algorithm could be very slow if the degree of the zeta function is large. For L-functions of exponential sums over a finite field of large characteristic p, it is not clear if the ℓ-adic methods would work well. This corresponds to the case of zeta functions of large degrees.

In the rest of this paper, we discuss the weaker problem of computing the reduction of zeta functions modulo p or a power of p. In section 3, we consider the geometrically trivial case of zero dimensional hypersurfaces. In section 4, we consider the general problem of computing the zeta function modulo p for higher dimensional varieties focusing on hypersurfaces. Finally, in section 5, we compute $Z(X,T)$ modulo a higher but small power of p.

3. Zero dimensional hypersurfaces

Let X be the zero dimensional hypersurface defined by a polynomial $f(x) \in \mathbb{F}_q[x]$ in one variable of degree d. Geometrically, X is trivial. It is a disjoint union of several closed points. Computing the zeta function in this simplest case is already non-trivial although it can be done efficiently as we shall see below.

Let

$$f(x) = \prod_{i=1}^{k} f_i(x)^{a_i}, \ a_i \geq 1$$

be the standard factorization of $f(x)$ over $\mathbb{F}_q$. Let d_i $(1 \leq i \leq k)$ be the degree of the irreducible factor $f_i(x)$. An irreducible factor of $f(x)$ of degree d_i corresponds to a closed point of X of degree d_i. The Euler product form of $Z(X,T)$ shows that

$$Z(X,T) = \prod_{i=1}^{k} \frac{1}{1-T^{d_i}}. \tag{3.1}$$

QUESTION 3.1. *Compute the zeta function $Z(X,T)$ directly from $f(x)$ without factoring $f(x)$ over $\mathbb{F}_q$.*

By formula (3.1), an algorithm for factoring $f(x)$ easily gives an algorithm for computing $Z(X,T)$. It is interesting to note that the converse seems also true quite often. In this section, we shall discuss three elementary formulas for $Z(X,T)$ modulo p, related to each other by duality and conjugacy. These lead to three simple polynomial time algorithms to compute $Z(X,T)$. Each formula leads to an efficient algorithm for factoring $f(x)$ if p is small. One formula leads to the classical algorithm of Berlekamp. Another formula leads to the more recent algorithm of

Niederreiter. The third one leads to a new algorithm, which has the advantage to extend to obtain higher dimensional zeta functions modulo p.

3.1. Zeta function and Berlekamp's algorithm

Let $R = \mathbb{F}_q[x]/(f)$ be the coordinate ring of the variety $X/\mathbb{F}_q$. This is an $\mathbb{F}_q$-vector space of dimension d. Let F be the q-th power Frobenius map on $\mathbb{F}_q[x]$:

$$F : h(x) \longrightarrow h(x)^q.$$

It fixes the ideal (f) and thus induces a map on R. Using the Chinese remainder theorem and normal basis, one can easily prove the following result due to Petr (1937).

THEOREM 3.1.1. *We have the congruence formula*

$$Z(X,T)^{-1} \equiv \det(I - FT|R) \ (\mod p).$$

The proof immediately gives the following result of Butler (1954):

THEOREM 3.1.2. *Let $R_1(F)$ denote the subspace of R which is fixed by F. Namely, $R_1(F)$ is the eigenspace of F at the eigenvalue 1. Then*

$$\dim_{\mathbb{F}_q} R_1(F) = k,$$

where k is the number of distinct irreducible factors of $f(x)$ over $\mathbb{F}_q$.

Applying this result to $f(x)$ over the extension field $\mathbb{F}_{q^j}$, we obtain the following result of Schwarz (1956).

THEOREM 3.1.3. *Let $k(j)$ be the number of distinct irreducible factors of $f(x)$ over $\mathbb{F}_{q^j}$. Let s_i be the number of distinct irreducible factors of degree i of $f(x)$ over the ground field $\mathbb{F}_q$. Then, we have*

$$\begin{aligned} \dim_{\mathbb{F}_q} R_1(F^j) &= k(j) \\ &= \sum_{i=1}^{d} (i,j) s_i, \end{aligned}$$

where (i,j) denotes the g.c.d. of the positive integers i and j.

Let A be the $d \times d$ matrix whose ij entry is (i,j), where $1 \leq i,j \leq d$. As indicated by Schwarz, the matrix A is invertible. In fact, an explicit formula for the inverse matrix of A can also be found, see [GA].

The map F acting on R can be computed efficiently by repeated squaring. The above theorems show that all the $k(i)$ and hence all the s_i $(1 \leq i \leq d)$ can be computed in polynomial time. Thus, the zeta function

$$Z(X,T) = \prod_{i=1}^{d} \frac{1}{(1-T^i)^{s_i}}$$

can be computed in polynomial time. It turns out that the subspace $R_1(F)$ is also useful for the harder problem of factoring $f(x)$ into irreducible factors over $\mathbb{F}_q$.

THEOREM 3.1.4. *(Berlekamp [Be]). The eigenspace $R_1(F)$ can be used to factor $f(x)$ over $\mathbb{F}_q$.*

The idea is as follows. By the Chinese remainder theorem, the eigenspace $R_1(F)$ has a basis of the form

$$\{y_1(x)\frac{f(x)}{f_1(x)^{a_1}}, \cdots, y_k(x)\frac{f(x)}{f_k(x)^{a_k}}\}$$

where $y_i(x) \in R$ satisfies

$$y_i(x)\frac{f(x)}{f_i(x)^{a_i}} \equiv 1 \ (\mod f_i(x)^{a_i}).$$

This basis shows that if $h_1(x)$ and $h_2(x)$ are two elements of $R_1(F)$ which are linearly independent over $\mathbb{F}_q$, then

$$f(x) = \prod_{c\in\mathbb{F}_q} (f(x), h_1(x) - ch_2(x)) \tag{3.1.1}$$

gives a non-trivial factorization of $f(x)$. This algorithm clearly runs in polynomial time if q is small. It can be extended to the case when p is small (q can be large). At present, no deterministic polynomial time algorithm is known to factor $f(x)$ in general if p is large even under the assumption of the Generalized Riemann Hypothesis.

A subspace R_1 of R is called **admissible** if any two linearly independent elements h_1 and h_2 of R_1 satisfy (3.1.1). It is clear that if an admissible subspace of R can be constructed efficiently, then one can proceeds in the same way to construct a new factorization algorithm. In the next two subsections, we describe two more such admissible subspaces and hence two more such algorithms for factoring polynomials. Admissible subspaces are studied in some details in Lee-Vanstone [LV]. In particular, the congruence formula in section 3.3 gives a new admissible subspace and hence answers a question in [LV].

3.2. Zeta function and Niederreiter's algorithm

Let ψ_q be the $\mathbb{F}_q$-linear operator on $\mathbb{F}_q[x]$ defined by

$$\psi_q(x^u) = \begin{cases} x^{u/q}, & \text{if } q|u, \\ 0, & \text{otherwise.} \end{cases}$$

This is a one sided inverse of the Frobenius map. It arises in various contexts such as Dwork's operator in p-adic theory of zeta functions, Cartier's operator in algebraic geometry and Hecke's U-operator in modular forms.

Let $H^{(q-1)}$ denote the $(q-1)$-th Hasse derivative on $\mathbb{F}_q[x]$ defined by

$$H^{(q-1)}(x^u) = \binom{u}{q-1} x^{u-(q-1)}.$$

Let D be the $\mathbb{F}_q$-linear differential operator on $\mathbb{F}_q[x]$:

$$D = \psi_q \circ H^{(q-1)} \circ f^{(q-1)},$$

where f^{q-1} is the multiplication operator. Since

$$\psi \circ f^q = f \circ \psi_q, \ f^q \circ H^{(q-1)} = H^{(q-1)} \circ f^q,$$

the ideal (f) of $\mathbb{F}_q[x]$ is stable under the action of D. Thus, the operator D induces a well defined map on $R = \mathbb{F}_q[x]/(f)$. The subspace $R_1(D)$ of R fixed by D has the admissible basis

$$\{f_1'(x)\frac{f(x)}{f_1(x)}, \cdots, f_k'(x)\frac{f(x)}{f_k(x)}\},$$

where $f_i'(x)$ denotes the derivative of $f(x)$. It follows that we have

THEOREM 3.2.1. *(Niederreiter [Ni]). The eigenspace $R_1(D)$ can be used to factor $f(x)$ over $\mathbb{F}_q$ in a way similar to Berlekamp's algorithm.*

Using the Chinese remainder theorem, normal basis and basic properties of the operators ψ_q and $H^{(q-1)}$, it is elementary to prove directly

THEOREM 3.2.2. *We have the congruence formula*

$$Z(X,T)^{-1} \equiv \det(I - DT|R) \ (\mod p).$$

As before, the eigenspaces $R_1(D^j)$ can be used to determine the integers s_i and hence gives a polynomial time algorithm to compute the zeta function $Z(X,T)$.

3.3. A new congruence formula

Let G be the composition of ψ_q and the multiplication operator f^{q-1} acting on $\mathbb{F}_q[x]$:

$$G = \psi_q \circ f^{(q-1)}.$$

Again, the ideal (f) of $\mathbb{F}_q[x]$ is stable under the action of G. Thus, the operator G induces a well defined map on $R = \mathbb{F}_q[x]/(f)$. Using the Chinese remainder theorem, normal basis and basic property of the operators ψ_q, we deduce

THEOREM 3.3.1. *Assume that $f(0) \neq 0$. Then,*

$$Z(X,T)^{-1} \equiv \det(I - GT|R) \ (\mod p).$$

Note that this result is false in general if $f(0) = 0$. Similarly, the eigenspaces $R_1(G^j)$ can be used to determine the integers s_i and hence yields a polynomial time algorithm to compute the zeta function $Z(X,T)$. For $f(0) \neq 0$, the eigenspace $R_1(G)$ has the admissible basis

$$\{xf_1'(x)\frac{f(x)}{f_1(x)}, \cdots, xf_k'(x)\frac{f(x)}{f_k(x)}\}.$$

Thus, we obtain

THEOREM 3.3.2. *The eigenspace $R_1(G)$ can be used to factor $f(x)$ over $\mathbb{F}_q$ in a way similar to the algorithms of Berlekamp and Niederreiter.*

3.4. Duality and conjugacy

The above three operators are closely related to each other. Using the definitions of D and G, one can easily check that they are conjugate to each other via the element x if x is invertible. Namely, we have

THEOREM 3.4.1. *If $f(0) \neq 0$, then $D = x^{-1}Gx$.*

The relation to the Frobenius map is given by duality. The proof is elementary.

THEOREM 3.4.2. *There are two non-singular pairings on $R \times R$ such that F and D (resp. F and G) are dual with respect to the first (resp. the second) pairing.*

The advantage of the operator $E = \psi_q \circ f^{q-1}$ is that it extends to higher dimensional varieties. We shall discuss this in next section.

4. Higher dimensional varieties

For simplicity, we restrict to the case of a hypersurface. The method works for an arbitrary variety. Thus, let X be the affine hypersurface defined by a polynomial $f(x_1, \cdots, x_n)$ over $\mathbb{F}_q$ of total degree d in n variables. Let $R(d)$ be the $\mathbb{F}_q$-vector space

$$R(d) = (x_1 \cdots x_n \mathbb{F}_q[x_1, \cdots, x_n])_{\leq d}.$$

Namely, $R(d)$ is the $\mathbb{F}_q$-vector space generated by those monomials of degree at most d and divisible by the product $x_1 \cdots x_n$. One computes that

$$\dim_{\mathbb{F}_q} R(d) = \binom{d}{n}.$$

The operator ψ_q extends easily to several variable case. We shall see that the operator $\psi_q \circ f^{q-1}$ can be used to compute the zeta function $Z(X, T)$ modulo p.

PROPOSITION 4.1. *The operator $\psi_q \circ f^{q-1}$ is stable on the subspace $R(d)$.*

Proof. Let $h \in R(d)$. Then, h is a polynomial of degree at most d. One checks that the degree of $f^{q-1}h$ is at most $d(q-1) + d = dq$. Thus, the degree of $\psi_q(f^{q-1}h)$ is at most d. Furthermore, if h is divisible by $x_1 \cdots x_n$, then $\psi_q(f^{q-1}h)$ is also divisible by $x_1 \cdots x_n$. This proves that $\psi_q(f^{q-1}h) \in R(d)$.

The following simple congruence formula for zeta functions can be easily proved using the reduction of the Dwork trace formula. It is implicit in section 7 of [Wa2].

THEOREM 4.2. *We have the congruence formula*

$$Z(X, T)^{(-1)^n} \equiv \det(I - (\psi_q \circ f^{q-1})T | R(d)) \pmod{p}.$$

In the projective case, a similar congruence formula but with a much harder proof is given by Katz [Ka2]. Very general congruence formulas but acting on infinite dimensional space can be found in [TW1] and [TW2]. Using Theorem 4.2, we get

COROLLARY 4.3. *The zeta function $Z(X, T)$ modulo p can be computed in time that is a polynomial in $\binom{d}{n} \log q$ (the input and output size) if p is small and n is fixed.*

This follows directly from Theorem 4.2 if q is small. If q is large but p is small, one needs to use a little semi-linear algebra and Galois theory. If p is large, we do not get a polynomial time algorithm. In computing the high power f^{q-1}, we have to expand it without reduction and the size simply gets larger and larger if p is large.

5. Higher power congruences

The congruence result in section 4 can be improved to get finer information by using congruences modulo a higher power of p. For this purpose, we need to use

p-adic liftings. Let K be an unramified finite extension of $\mathbb{Q}_p$ with residue field $\mathbb{F}_q$. Let $\mathcal{O}_K$ be the ring of integers in K. For a positive integer m, Let $\mathcal{O}_m$ be the residue class ring $\mathcal{O}_K/(p^m)$, which is a finite ring of q^m elements.

We still restrict to the case of a hypersurface. For simplicity of description, we shall only consider those solutions with $x_1 \cdots x_n \neq 0$. Thus, let X be the affine hypersurface in the torus $\mathbb{G}_m^n/\mathbb{F}_q$ defined by a polynomial $f(x_1, \cdots, x_n)$ over $\mathbb{F}_q$ of total degree d in n variables. We assume that the polynomial f has already been lifted to $\mathcal{O}_m$ for some $m > 0$. We shall consider the question of computing $Z(X,T)$ modulo p^m.

Let $R_{m,d}$ be the free $\mathcal{O}_m$-module:

$$R_{m,d} = \mathcal{O}_m[x_1, \cdots, x_n]_{\leq dp^{m-1}}.$$

Namely, $R_{m,d}$ is the free $\mathcal{O}_m$-module generated by those monomials of degree at most dp^{m-1}. One computes that

$$\dim_{\mathcal{O}_m} R_{m,d} = \binom{dp^{m-1}+n}{n}.$$

The operator ψ_q is defined as before. It is easy to check that we have

PROPOSITION 5.1. *The operator $\psi_q \circ f^{(q-1)p^{m-1}}$ is stable on the finite dimensional free $\mathcal{O}_m$-module $R_{m,d}$.*

The operator $\psi_q \circ f^{(q-1)p^{m-1}}$ modulo p^m is clearly independent of the choice of the lifting of f to $\mathcal{O}_m$. The following simple congruence formula for zeta functions can be proved using the reduction modulo p^m of the Dwork trace formula.

THEOREM 5.2. *We have the congruence formula*

$$\left(\frac{Z(X,T)}{Z(\mathbb{G}_m^n,T)}\right)^{(-1)^n} \equiv \prod_{i=0}^{n} \det(I - q^i(\psi_q \circ f^{(q-1)p^{m-1}})T|R_{m,d})^{(-1)^i\binom{n}{i}} \pmod{p^m}.$$

Since the zeta function of the n-torus $\mathbb{G}_m^n$ is very simple, we are reduced to computing $\det(I - (\psi_q \circ f^{(q-1)p^{m-1}})T|R_{m,d})$ modulo p^m. Using the above formula, we can show

COROLLARY 5.3. *$Z(X,T)$ modulo p^m can be computed in polynomial time if p^m is small and n is fixed.*

This follows from Theorem 5.2 if q is also small. If q is large but p^m is small, it involves a little extra work. If p^m is large, we do not get a polynomial time algorithm as the dimension of $R_{m,d}$ is already exponential.

The approach we take in this section is the most elementary one. It has the advantage to be a polynomial time algorithm for any hypersurface as long as p^m is small and as long as we only want modulo p^m information for $Z(X,T)$. We shall consider another deeper p-adic approach in a future article, which seem to work well in some interesting cases even when we want the full information for $Z(X,T)$.

References

[AH] L.M. Adleman and M.D. Huang, Counting rational points on curves and abelian varieties over finite fields, Lecture Notes in Computer Science, 1122 (1996), 1-16.

[AG] M. Anshel and D. Goldfeld, Zeta functions, one-way functions and pseudorandom number generators, Duke, Math., J., 88(1997), no.2, 371-390.

[Be] E.R. Berlekamp, Factoring polynomials over finite fields, Bell System Technical J., 46(1967), 1853-1859.

[Ber] P. Berthelot, Géométrie rigide et cohomologie des variétés algébriques de caractéristique p, Mém. Soc. Math. France (N.S.) No. 23(1986), 3, 7–32.

[Bo] E. Bombieri, On exponential sums in finite fields, II, Invent. Math., 47(1978), 29-39.

[De] P. Deligne, La conjecture de Weil, I, Publ. Math., IHES 43(1974), 273-307.

[Dw] B. Dwork, On the rationality of the zeta function of an algebraic variety, Amer. J. Math., 82(1960), 631-648.

[ES] J. -Y. Etesse and B. Le Stum, Fonctions L associées aux F-isocristaux surconvergents II, zéros et pôles unités, Invent. Math., 127(1997), no.1, 1-31.

[FHJ] M. Fried, D. Haran and M. Jarden, Effective counting of the points of definable sets over finite fields, Israel J. Math., 85(1994), no. 1-3, 103-133.

[Gr] A. Grothendieck, Formule de Lefschetz et rationalité des fonctions L, Séminaire Bourbaki, exposé 279, 1964/65.

[GA] H. Gunji and D. Arron, On polynomial factorization over finite fields, Math. Comp., 36(1981), 281-287.

[GKS] J. von zur Gathen, M. Karpinski and I. Shparlinski, Counting curves and their projections, Comput. Complexity, 6(1996/97), no.1, 64-99.

[Ka1] N. Katz, Travaux de Dwork, Séminaire Bourbaki, Exp. 409(1971/72), Lecture Notes in Math. 317, 1973, 167-200.

[Ka2] N. Katz, Une formule de congruence pour la fonction ζ, in: Groupes de monodromie en géométrie algébrique (SGA 7 II), Exp. XXII, 401-438, Lecture Notes in Math. 340, Springer-Verlag, 1973

[Ko1] N. Koblitz, Elliptic curve cryptosystems, Math. Comp., 48(1987), 203-209.

[Ko2] N. Koblitz, Hyperelliptic cryptosystems, J. Cryptology, 1(1989), 139-150.

[LV] T.C.Y. Lee and S.A. Vanstone, Subspaces and polynomial factorizations over finite fields, AAECC, 6(1995), 147-157.

[Mo] P. Monsky, Formal cohomology III, Ann. Math., 93(1971), 315-343.

[Ni] H. Niederreiter, Factoring polynomials over finite fields using differential equations and normal bases, Math. Comp., 62(1994), 819-830.

[Pi] J. Pila, Frobenius maps of abelian varieties and finding roots of unity in finite fields, Math. Comp., 55(1990), 745-763.

[Po] B. Poonen, Computational aspects of curves of genus at least 2, Lecture Notes in Computer Science, 1122 (1996), 283-306.

[Sc1] R. Schoof, Elliptic curves over finite fields and the computation of square roots modulo p, Math. Comp., 44(1985), 483-494.

[Sc2] R. Schoof, Counting points on elliptic curves over finite fields, Journal de Théorie des Nombres de Bordeaux, 7(1995), 219-254.

[TW1] Y. Taguchi and D. Wan, L-functions of Drinfeld modules and φ-sheaves, J. Amer. Math. Soc., 9(1996), 755-781.

[TW2] Y. Taguchi and D. Wan, Entireness of L-functions of φ-sheaves on affine complete intersections, J. Number Theory, 63(1997), no.1, 170-179.

[Ts] M.A. Tsfasman, Algebraic geometry lattices and codes, Lecture Notes in Computer Science, 1122 (1996), 385-389.

[Wa1] D. Wan, Hilbert sets and zeta functions over finite fields, J. Reine Angew. Math., 427(1992), 193-207.

[Wa2] D. Wan, Meromorphic continuation of L-functions of p-adic representations, Ann. Math., 143(1996), 469-498.

Department of Mathematics, University of California, Irvine, CA 92697-3875
E-mail address: dwan@math.uci.edu

This page intentionally left blank

Contemporary Mathematics
Volume **225**, 1999

Cyclic Alternant codes induced by an automorphism of a GRS code

Thierry P. Berger

ABSTRACT. Classically, permutations on codes over an extension field imply permutations on the corresponding subfield subcode over the prime field. In this paper, we show that some semi-linear automorphisms of a code also induce permutations of the subfield subcode.

Using this fact and the knowledge of automorphism groups of Generalized Reed-Solomon codes (GRS codes), we classify all the cyclic Alternant codes, the cyclicity of which is induced by a semi-linear automorphism of the corresponding GRS code.

1. Preliminaries.

1.1. Automorphism groups of a code. The reader can refer to [**7**] for basic definitions on linear codes, and [**6**] for more on automorphism groups of codes. Let C be a linear code of length n over the finite fied $K = GF(p^m)$ (p is a prime number). There exist three kinds of automorphism groups for a code in the litterature:

DEFINITION 1.1. The permutation group $Per(C)$ of a code is the group of permutations of the support of a code C which leave the code globally invariant.

A permutation $\sigma \in Sym(n)$ on the set of index $\{1, \ldots, n\}$ acts on a codeword as follows:
If $x = (x_1, \ldots, x_n)$, then $\sigma(x) = (x_{\sigma^{-1}(1)}, \ldots, x_{\sigma^{-1}(n)})$.

DEFINITION 1.2. The linear automorphism group $Aut(C)$ of a code is the group of linear transformations on K^n which preserve the Hamming weight and leave the code C globally invariant.

It is well-known that the group of linear transformations on K^n which preserve the Hamming weight is the monomial group $\mathcal{M}_n(K) = K^{*n} \rtimes Sym(n)$, consisting of non-zero scalar multiplications on each component followed by permutations of the support: If $\mathbf{a} = (a_1, \ldots, a_n) \in K^{*n}$ and $\sigma \in Sym(n)$, then
$(\mathbf{a}; \sigma)(x) = \sigma(ax) = (a_{\sigma^{-1}(1)} x_{\sigma^{-1}(1)}, \ldots, a_{\sigma^{-1}(n)} x_{\sigma^{-1}(n)})$.

DEFINITION 1.3. The semi-linear automorphism group $SAut(C)$ of a code is the group of semi-linear transformations on K^n which preserve the Hamming weight and leave the code C globally invariant.

1991 *Mathematics Subject Classification.* 94B15.
This work was supported by projet CODES, INRIA-Rocquencourt.

© 1999 American Mathematical Society

The group of semi-linear transformations on K^n which preserve the Hamming weight is the group $\mathcal{W}_n(K) = K^{*n} \rtimes (Sym(n) \times Gal(K))$ generated by the monomial group and the automorphism group $Gal(K)$ acting on the components of the codewords (cf. [**4, 6**]): if $\gamma_{p^i} : a \to a^{p^i}$ is an element of $Gal(K)$, then $(\mathbf{a}; \sigma, \gamma_{p^i})(x) == (a^{p^i}_{\sigma^{-1}(1)} x^{p^i}_{\sigma^{-1}(1)}, \dots, a^{p^i}_{\sigma^{-1}(n)} x^{p^i}_{\sigma^{-1}(n)})$.

REMARK 1.4. If $K = GF(p)$ is a prime field, then $Aut(C) = SAut(C)$, moreover, if $K = GF(2)$, then $Per(C) = Aut(C)$.

1.2. Subfield subcodes.

DEFINITION 1.5. The subfield subcode A over $GF(p)$ of a code C over $K = GF(p^m)$ is the $GF(p)$-linear code $A = C \cap GF(p)^n$.

Clearly, a permutation of $Per(C)$ leaves the code A globally invariant, and then $Per(C) \subseteq Per(A)$. But in general, an element of $Aut(C)$ (or $SAut(C)$) does not induces an element of $Aut(A)$. However, we have the following result:

PROPOSITION 1.6. *Suppose that there exist an element* $(\mathbf{a}; \sigma, \gamma)$ *in* $SAut(C)$ *such that* $\mathbf{a} = \lambda \mathbf{1} = (\lambda, \dots, \lambda)$ *(with the notation* $\mathbf{1} = (1, \dots, 1)$*), then* σ *is an element of* $Per(A)$.

PROOF. Let $x \in A$, then $y = (\mathbf{a}; \sigma, \gamma)(x) = \gamma(\lambda)(\gamma(x_{\sigma^{-1}(1)}), \dots, \gamma(x_{\sigma^{-1}(n)}))$ is an element of C. Since $x \in A \subseteq GF(p)^n$, for all i, $\gamma(x_i) = x_i$ and $\sigma(x) = \gamma(\lambda)^{-1} y$ is an element of C with components on $GF(p)$. This proves that σ is a permutation of $Per(A)$. □

REMARK 1.7. Such permutations are well-known for cyclic codes: if a code C on K is cyclic, its permutation group contains the shift $\sigma_1 : i \to i + 1 \pmod n$, but the cyclic subfield subcode contains also the permutation $\gamma_p : i \to pi \pmod n$ which is induced by a semi-linear automorphism of C (for examples cf.[**1, 2**]).

1.3. Cauchy codes. Cauchy codes where introduced by A. Dür in 1987 [**4**]. The definition given here is simpler than it given by A. Dur: he uses homogenous polynomials in two variables. His approach is fundamental for proving the results on automorphism group. However, in this paper we will give these without proof. The reader can refer to [**4**] or [**6**].

Let $\overline{K} = K \cup \{\infty\}$ be the projective line on K and $\boldsymbol{\alpha} = (\alpha_1, \dots, \alpha_n)$ be an ordered set of n distinct points of $\overline{K}$. Let $\mathbf{v} = (v_1, \dots, v_n) \in K^{*n}$ be a n-uple of non-zero scalars in K and k be an integer, $1 \leq k \leq n$. The matrix $M_{k,\mathbf{v},\boldsymbol{\alpha}}$ is defined as follows:

$$M_{k,\mathbf{v},\boldsymbol{\alpha}} = \begin{pmatrix} v_1 & v_2 & v_3 & \dots & v_{n-1} & 0 \\ 0 & v_2\alpha_2 & v_3\alpha_3 & \dots & v_{n-1}\alpha_{n-1} & 0 \\ 0 & v_2\alpha_2^2 & v_3\alpha_3^2 & \dots & v_{n-1}\alpha_{n-1}^2 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & v_2\alpha_2^{k-2} & v_3\alpha_3^{k-2} & \dots & v_{n-1}\alpha_{n-1}^{k-2} & 0 \\ 0 & v_2\alpha_2^{k-1} & v_3\alpha_3^{k-1} & \dots & v_{n-1}\alpha_{n-1}^{k-1} & v_n \end{pmatrix}$$

Where by convenience we suppose $\alpha_1 = 0$ and $\alpha_n = \infty$.

DEFINITION 1.8. The Cauchy code $\mathcal{C}_k(\mathbf{v}, \boldsymbol{\alpha})$ of dimension k, scalar $\mathbf{v}$ and ordered support $\boldsymbol{\alpha}$ is the linear code on K generated by the matrix $M_{k,\mathbf{v},\boldsymbol{\alpha}}$. The set $L_{\boldsymbol{\alpha}} = \{\alpha_1, \dots, \alpha_n\}$ is called the support of the Cauchy code.

These codes are a slight generalization of Generalized Reed-Solomon codes, since it is possible to add a column associated with the infinity point.

If all the scalars v_i are equal to 1 and the support $L_{\boldsymbol{\alpha}}$ is the whole projective line $\overline{K}$, this code is the doubly-extended Reed-Solomon code of dimension k (cf.[**7**] p.323).

1.4. Action of the projective linear group on Cauchy codes. Let f be an element of the linear group $GL(2,K)$, that is an invertible 2×2 matrix with entries in K: $f = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$.

Let $\tilde{f}$ be the corresponding element of the projective linear group $PGL(2,K)$ in its standard action on the projective line: $\tilde{f}(g) = \dfrac{ag+b}{cg+d}$.

It is well-known that $\tilde{f}_1 = \tilde{f}_2$ if and only if there exist a scalar $\lambda \in K^*$ such that $f_2 = \lambda f_1$.

With each element f of $GL(2,K)$, we associate an application $\mathbf{u}_f$ from $\overline{K}$ to K defined by

- if $g \in K$ and $cg+d \neq 0$, $\mathbf{u}_f(g) = cg+d$.
- if $g \in K$ and $cg+d = 0$, $\mathbf{u}_f(g) = ag+b$.
- if $g = \infty$ and $c \neq 0$, $\mathbf{u}_f(\infty) = c$.
- if $g = \infty$ and $c = 0$, $\mathbf{u}_f(\infty) = a$.

With each $f \in GL(2,K)$, we associate an operator $\mathcal{H}_f$ on Cauchy codes as follows:
$\mathcal{H}_f(\mathcal{C}_k(\mathbf{v},\boldsymbol{\alpha})) = \mathcal{C}_k(\mathbf{w},\boldsymbol{\beta})$ with, for all i, $\beta_i = \tilde{f}(\alpha_i)$ and $w_i = u_f(\alpha_i)^{k-1} v_i$.

REMARK 1.9. The operator $\mathcal{H}_f$ is in fact associated with $\tilde{f} \in PGL(2,K)$, indeed, if $\mathcal{H}_f(\mathcal{C}_k(\mathbf{v},\boldsymbol{\alpha})) = \mathcal{C}_k(\mathbf{w},\boldsymbol{\beta})$ and $\mathcal{H}_{\lambda f}(\mathcal{C}_k(\mathbf{v},\boldsymbol{\alpha})) = \mathcal{C}_k(\mathbf{w}',\boldsymbol{\beta}')$, then $\mathbf{w}' = \lambda^{k-1}\mathbf{w}$ and $\boldsymbol{\beta}' = \boldsymbol{\beta}$. Consequently, $M_{k,\mathbf{w},\boldsymbol{\beta}} = \lambda^{k-1} M_{k,\mathbf{w}',\boldsymbol{\beta}'}$ and $\mathcal{C}_k(\mathbf{w},\boldsymbol{\beta}) = \mathcal{C}_k(\mathbf{w}',\boldsymbol{\beta}')$. If the context is clear, we will identify f and $\tilde{f}$.

The following result is the fundamental Theorem 4 in [**4**].

THEOREM 1.10. *The Cauchy codes $C_k(\mathbf{v},\boldsymbol{\alpha})$ and $C_k(\mathbf{w},\boldsymbol{\beta})$ are equal if and only if there exist an element $f \in GL(2,K)$ and a scalar $\lambda \in K^*$ such that $H_f(C_k(\mathbf{v},\boldsymbol{\alpha})) = C_k(\mathbf{v}',\boldsymbol{\beta})$ and $\mathbf{w} = \lambda\mathbf{v}'$.*

Note that in this case $\boldsymbol{\beta} = \tilde{f}(\boldsymbol{\alpha})$.

Let $f \in GL(2,K)$ such that $f(L_{\boldsymbol{\alpha}}) = L_{\boldsymbol{\alpha}}$. It induces a permutation σ_f on $\{1,..,n\}$: $i = \sigma_f(j) \Leftrightarrow \alpha_j = f(\alpha_i)$. This definition of σ_f is in accordance with the definition $\sigma_f(\boldsymbol{\alpha}) = (\alpha_{\sigma_f^{-1}(1)}, \ldots, \alpha_{\sigma_f^{-1}(n)}) = f(\boldsymbol{\alpha})$. Conversely, if a permutation $\sigma \in Sym(n)$ is induced by an element $\tilde{f} \in PGL(2,K)$ and if $L_{\boldsymbol{\alpha}}$ contains at least three elements, then $\tilde{f}$ is completely determined by σ since the permutation group $PGL(2,K)$ is sharply three-transitive on $\overline{K}$.

In the sequel, we will identify σ_f and f when there is no ambiguity.

1.5. Automorphism groups of Cauchy codes. The semi-linear automorphism groups of Cauchy codes were determined by A. Dür in [**4**]. Since semi-linear transformations are allowed, we have to consider the projective semi-linear group $P\Gamma L(2,K)$ instead of $PGL(2,K)$. The elements of $P\Gamma L(2,K)$ are the permutations of $\overline{K}$ of the form $f'(g) = \left(\dfrac{ag+b}{cg+d}\right)^{p^j}$.

THEOREM 1.11. *Let $C = C_k(\mathbf{v}, \boldsymbol{\alpha})$ be a Cauchy code, $1 < k < n-1$. An element $(\mathbf{a}; \sigma, \gamma) \in \mathcal{M}_n(K)$ is an element of $SAut(C)$ if and only if there exists an element $f \in GL(2, K)$ such that, if $\tilde{f}(g) = \dfrac{ag+b}{cg+d}$ and $f'(g) = \gamma \circ \tilde{f}(g) = \left(\dfrac{ag+b}{cg+d}\right)^{p^j}$ then*

- *$f'(L_{\boldsymbol{\alpha}}) = L_{\boldsymbol{\alpha}}$ and σ is the permutation induced by f'.*
- *There exists a $\lambda \in K^*$ such that $\mathbf{a} = \lambda \sigma^{-1}(\mathbf{v})^{p^{m-j}} (u_f(\alpha_i)^{k-1}\mathbf{v})^{-1}$, that is $a_i = \lambda v_{\sigma^{-1}(i)}^{p^{m-j}} (v_i u_f(\alpha_i)^{k-1})^{-1}$.*

This theorem is a version of Theorem 5 in [4] using our notation (cf. also [6]).

As an example of these formulas, we give the generators of the semi-linear automorphism groups of doubly extended Reed-Solomon code. In that case, $\mathbf{v} = \mathbf{1}$, which simplifies the formulas. Moreover, each element of $P\Gamma L(2, K)$ produces an automorphism. The group $P\Gamma L(2, K)$ is generated by the translations: $\tau_b(g) = g + b$, the homotheties $\sigma_a(g) = ag$, the inversion $\xi_{-1}(g) = g^{-1}$ and the Frobenius map $\gamma_p(g) = g^p$.

With the convention $\alpha_1 = 0$ and $\alpha_n = \infty$, the corresponding generators are

1. $(\lambda\mathbf{1}; 1,)$, $\lambda \in K^*$, the scalar multiplications
2. $(\mathbf{1}; \tau_b, 1)$.
3. $(\mathbf{a}_k, \sigma_a, 1)$, a is a primitive root of K, $\mathbf{a}_k = (1, \ldots, 1, a^{1-k})$.
4. $(\mathbf{b}_k; \xi_{-1}, 1)$, $\xi_{-1}(x) = x^{-1}$, $b_{k,i} = (1, \alpha_2^{1-k}, \ldots, \alpha_{n-1}^{1-k}, 1)$.
5. $(\mathbf{1}; \gamma_p, \gamma_p)$.

Note that the first four generate the linear automorphism group $Aut(C)$.

2. Cyclic Alternant codes

In the literature (see e.g. [7]) Alternant codes are subfield subcodes of Generalized Reed-Solomon codes. Here, we generalize this notion to subfield subcodes of Cauchy codes.

DEFINITION 2.1. The Alternant code $\mathcal{A}_k(\mathbf{v}, \boldsymbol{\alpha})$ is the subfield subcode over the prime field $GF(p)$ of the Cauchy code $\mathcal{C}_k(\mathbf{v}, \boldsymbol{\alpha})$.

2.1. How to construct cyclic Alternant codes. The aim of our work is to use the knowledge of automorphism groups of Cauchy codes to construct cyclic Alternant codes via Proposition 1.6. We call such a code an induced-cyclic Alternant code.

A Cauchy code induces a permutation σ on the corresponding Alternant code if and only if its automorphism group contains an element of the form $(\lambda\mathbf{1}; \sigma, \gamma)$. The following result characterize all the induced-cyclic Alternant codes.

THEOREM 2.2. *An Alternant code $\mathcal{A}_k(\mathbf{v}, \boldsymbol{\alpha})$ is induced-cyclic if and only if*

1. *there exists an element $f' \in P\Gamma L(2, K)$ such that the support $\boldsymbol{\alpha}$ is the orbit of an element $\alpha_0 \in \overline{K}$ under f'.*
2. *if $f' = \gamma_{p^j} \circ \tilde{f}$, $f \in PGL(2, K)$, then there exists a scalar $\lambda \in K^*$ such that, for all i, $v_{i+1} = (\lambda v_i u_f(\alpha_i)^{k-1})^{p^j}$ and $v_n = v_0$.*

PROOF. The assertion 1. is clear: if a permutation σ of the Alternant code $\mathcal{A}_k(\mathbf{v}, \boldsymbol{\alpha})$ is induced by an automorphism $(\mathbf{a}; \sigma, \gamma)$ of $\mathcal{C}_k(\mathbf{v}, \boldsymbol{\alpha})$, then σ is a permutation induced by an element $f' \in P\Gamma L(2, K)$, moreover, since σ is a cycle of length n, the support $\boldsymbol{\alpha}$ must be an orbit under f'.

As classically for cyclic codes, the index of $x \in K^n$ are $\{0, \ldots, n-1\}$, i.e. if $x \in K^n$, then $x = (x_0, \ldots, x_{n-1})$. Now, we suppose that $\boldsymbol{\alpha}$ is the orbit of α_0 under f' and $\sigma = \sigma_{f'}$ is the shift $i \to i - 1 \pmod n$. From Theorem 1.11, there exists a $\lambda \in K^*$ such that $\mathbf{a} = (a_0, \ldots, a_{n-1})$ verifies $a_i = \lambda v_{\sigma^{-1}(i)}^{p^{m-j}} (v_i u_f(\alpha_i)^{k-1})^{-1}$.

From proposition 1.6, $\mathbf{a}$ must be equal to $\mathbf{1}$ (up to the scalar λ). Then $(\mathbf{a}; \sigma, \gamma)$ induces the permutation σ if and only if $\lambda v_{\sigma^{-1}(i)}^{p^{m-j}} (v_i u_f(\alpha_i)^{k-1})^{-1} = 1$ for all i.

This gives the relation $v_{i+1} = (\lambda^{-1} v_i u_f(\alpha_i)^{k-1})^{p^j}$, with the convention $v_n = v_0$. Substituting $\lambda' = \lambda^{-1}$ in this formula, we prove our theorem.

□

If there is no ambiguity, we denote such a code as a cyclic Alternant code induced by $f' \in P\Gamma L(2, K)$.

2.2. Classification of the projective semi-linear group. Using Theorem 2.2, we are able to construct all the induced-cyclic Alternant codes by exploring all the possible orbits under all elements of the projective semi-linear group, and then constructing adequate scalars $\mathbf{v}$. However, from Theorem 1.10, we know that many parameters of Cauchy codes give the same Cauchy code.

PROPOSITION 2.3. *Suppose that $C = \mathcal{C}_k(\mathbf{v}, \boldsymbol{\alpha})$ is a Cauchy code such that $\boldsymbol{\alpha}$ is the orbit of α_1 under an element $f \in P\Gamma L(2, K)$. Let $h \in PGL(2, K)$ and $\mathcal{C}_k(\mathbf{w}, \boldsymbol{\beta}) = \mathcal{H}_h(\mathcal{C}_k(\mathbf{v}, \boldsymbol{\alpha}))$ be the image of C by the operator $\mathcal{H}_h$, then $\boldsymbol{\beta}$ is the orbit of $\beta_1 = h(\alpha_1)$ under $h \circ f \circ h^{-1}$.*

The proof of this proposition is straightforward, but it implies that we have to consider the elements of $P\Gamma L(2, K)$ up to conjugation.

The following theorem gives a classification of $P\Gamma L(2, K)$ up to conjugation using the number of fixed-points under f.

THEOREM 2.4. *Up to conjugation under an element of $PGL(2, K)$, a permutation $f \in P\Gamma L(2, K)$ in its standard action on the projective line $\overline{K}$ is one of the following (j is an integer smaller than m):*

1. *at least three fixed points: $f(g) = g^{p^j}$.*
2. *two fixed points: $f(g) = (ag)^{p^j}$, with $N_{GF(p^\ell)}(a) \neq 1$ (where $\ell = (j, m)$ is the greatest common divisor of j and m).*
3. *one fixed point: $f(g) = (g + b)^{p^j}$, with $Tr_{GF(p^\ell)}(b) \neq 0$ ($\ell = (j, m)$).*
4. *no fixed point: $f(g) = \dfrac{1}{(cg + d)^{p^j}}$, the polynomial $P(X) = cX^{p^{m-j+1}} + dX - 1$ has no root in K. Moreover, if K' is a finite extension of K containing a root of $P(X)$, then f is conjugated in $PGL(2, K')$ to an element of $PGL(2, K')$ of the form 1. or 2.*

PROOF. Recall that the general form for f is $f(g) = \left(\dfrac{ag + b}{cg + d}\right)^{p^j}$. Moreover $PGL(2, K)$ is three transitive as permutation group on $\overline{K}$.

1. If f has at least three fixed points, we can assume that these are 0, 1 and ∞, this yields $f(g) = g^{p^j}$.
2. Similarly for the two fixed points case, we assume that the fixed points are 0 and ∞, and then $f(g) = (ag)^{p^j}$. Since we assume that there is no other fixed point, a^{p^j} (and hence a) must be different from g^{1-p^j} for all $g \in K$.

   Let ℓ be the greatest common divisor of j and m.There exists an integer s prime to $p^m - 1$ such that $s(p^r - 1) \equiv p^\ell - 1 \pmod{p^m - 1}$, and then a must be distinct of g^{1-p^ℓ} for all $g \in K$, that is $N_{GF(p^\ell)}(a) \neq 1$.
3. If there is a single fixed point, we assume that it is the infinity point and $f(g) = (ag + b)^{p^j}$.

   Since there is no other fixed point, the polynomial $P(X) = a^{p^j} X^{p^j} - X + b^{p^j}$ has no root in K. This is an affine polynomial. Let $Q(X) = a^{p^j} X^{p^j} - X$ be the linear associated polynomial. The kernel of $Q(X)$ must be non trivial, if not $Q(X)$ (and $P(X)$) defines a bijective map of K in K, and then f has one more fixed point. This implies there exists a $c \in K^*$ such that $a = c^{1-p^j}$. Let $\sigma_c(g) = cg$ and $f' = \sigma_c \circ f \circ \sigma_c^{-1}$, that is $f'(g) = (g + c^{-p^j} b)^{p^j}$. Without loss of generality, we can assume $f(g) = (g + b)^{p^j}$.

   Since f has no more fixed point in K, b must be distinct of $g^{p^j} - g$ for all $g \in K$, that is equivalent to $Tr_{GF(p^\ell)}(b) \neq 0$.
4. Suppose now that f has no fixed point in $\overline{K}$. Using the 3-transitivity, it is possible to assume that $f(\infty) = 0$, and then $f(g) = \dfrac{1}{(cg + d)^{p^j}}$.

   The polynomial $P(X)$ has a root in K if and only if f has a fixed point in $\overline{K}$. Let K' be an extension of K containing a root ε of $P(X)$. It contains at least two roots, since it contains the conjugates of ε under $\gamma_{p^m}(g) = g^{p^m}$. The permutation $f(g)$ can be considered as an element of $P\Gamma L(2, K')$ wich have at least two fixed points in $\overline{K'}$, and then is conjugated in $PGL(2, K')$ to an element of the form $f(g) = g^{p^j}$ or $f(g) = (ag)^{p^j}$.

□

2.3. Classification of induced-cyclic Alternant codes. The previous results on the classification of $P\Gamma L(2, K)$ give us a good tool for classifying induced-cyclic Alternant codes. In some cases, it is possible to obtain more simplifications if we consider the Alternant codes up to permutations of the support.

We will use the following lemma for restricting the choice of j in Theorem 2.4 to a divisor of m and for given a more canonical form to the support $\boldsymbol{\alpha}$.

LEMMA 2.5. *Let $C = \mathcal{A}_k(\mathbf{v}, \boldsymbol{\alpha})$ be a cyclic Alternant code induced by $f \in P\Gamma L(2, K)$. $\boldsymbol{\alpha} = (\alpha_0, \ldots, \alpha_{n-1})$ is the orbit of α_0 under f. Let s be an integer coprime with the length n of the code (that is the length of the orbit of α_0). Let σ_s be the permutation of the support defined by $\sigma_s^{-1}(i) = si \pmod{n}$. Then the image C' of C by σ_s is the induced-cyclic Alternant code $\mathcal{A}_k(\sigma_s(\mathbf{v}), \sigma_s(\boldsymbol{\alpha}))$ where $\sigma_s(\boldsymbol{\alpha})$ is the orbit of α_0 under f^s.*

PROOF. It is clear that the image of C by the permutation σ_s is the Alternant code $\mathcal{A}_k(\sigma_s(\mathbf{v}), \sigma_s(\boldsymbol{\alpha}))$. Note that, as usual for cyclic codes, the set of index is $\{0, \ldots, n-1\}$ instead of $\{1, \ldots, n\}$. Since $\boldsymbol{\alpha}$ is the orbit of α_0 under f,

$f(\alpha_i) = \alpha_{i+1}$ for all i, and then $f^s(\alpha_i) = \alpha_{i+s}$. The orbit of α_0 under f^s is $\boldsymbol{\beta} = (\alpha_0, \alpha_s, \alpha_{2s}, \ldots, \alpha_{(n-1)s}) = \sigma_s(\boldsymbol{\alpha})$.

The indices are calculated modulo n. Note that σ_s is a permutation, since s is coprime to n. In our hypothesis, we assume that C is induced-cyclic, which means that $(\mathbf{1}; f, \gamma)$ (for some $\gamma \in Gal(K)$) is in the semi-linear automorphism group of $\mathcal{C}_k(\mathbf{v}, \boldsymbol{\alpha})$. It is easy to verify what $(\mathbf{1}; f^s, \gamma^s)$ is in the semi-linear automorphism group of $\mathcal{C}_k(\sigma_s(\mathbf{v}), \sigma_s(\boldsymbol{\alpha}))$, and then C' is an cyclic Alternant code induced by f^s. □

LEMMA 2.6. *Let $\mathcal{A}_k(\mathbf{v}, \boldsymbol{\alpha})$ be a cyclic Alternant code induced by $f \in P\Gamma L(2, K)$ and assume in addition that $f(g) = (ag + b)^{p^j}$ (i.e. ∞ is a fixed point for f). Then, up to a scalar multiplication of $\mathbf{v}$, there exists $\lambda \in K^*$ such that $\mathbf{v} = (1, \lambda, \lambda^{p^j+1}, \lambda^{p^{2j}+p^j+1}, \ldots, \lambda^{\sum_{i=0}^{n-2} p^{ij}})$ and $\lambda^{\sum_{i=0}^{n-1} p^{ij}} = 1$.*

Conversely, if $\boldsymbol{\alpha}$ is the orbit of an element under $f(g) = (ag + b)^{p^j}$ of length n, for each $\lambda \in K^*$ such that $\lambda^{\sum_{i=0}^{n-1} p^{ij}} = 1$, then $\mathcal{A}_k(\mathbf{v}_\lambda, \boldsymbol{\alpha})$ is cyclic induced by f, with $\mathbf{v}_\lambda = (1, \lambda, \lambda^{p^j+1}, \lambda^{p^{2j}+p^j+1}, \ldots, \lambda^{\sum_{i=0}^{n-2} p^{ij}})$.

PROOF. We suppose $n > 1$. $\boldsymbol{\alpha}$ does not contain the infinity point. The special form $(ag + b)^{p^j}$ for f implies $u_f(\alpha_1) = 1$ for all i. The necessary and sufficient condition of Theorem 2.2 becomes $v_{i+1} = (\lambda v_i)^{p^j}$. Choosing $v_0 = 1$, this gives $\mathbf{v} = (1, \lambda^{p^j}, \lambda^{p^j+p^{2j}}, \lambda^{p^j+p^{2j}+p^{3j}}, \ldots, \lambda^{\sum_{i=1}^{n-1} p^{ij}})$, under the assumption $\lambda^{\sum_{i=1}^{n} p^{ij}} = v_0 = 1$. Let $\lambda' = \lambda^{p^j}$, this becomes
$\mathbf{v} = (1, \lambda', \lambda'^{p^j+1}, \lambda'^{p^{2j}+p^j+1}, \ldots, \lambda'^{\sum_{i=0}^{n-2} p^{ij}})$ and $\lambda'^{\sum_{i=0}^{n-1} p^{ij}} = 1$. □

Our main result is the following theorem

THEOREM 2.7. *Let C be a cyclic Alternant code of length $n > 2$ induced by a Cauchy code over $K = GF(p^m)$. Then C is equivalent by permutation to an Alternant code $\mathcal{A}_k(\mathbf{v}, \boldsymbol{\alpha})$ satisfying one of the following conditions:*

1. *r divides m, $n = m/r$,*
   $\boldsymbol{\alpha} = (\alpha, \alpha^{p^r}, \alpha^{p^{2r}}, \ldots, \alpha^{p^{(n-1)r}})$, is the orbit of α under $f(g) = g^{p^r}$,
   $\mathbf{v} = (1, \lambda, \lambda^{p^r+1}, \ldots, \lambda^{\sum_{i=0}^{n-2} p^{ir}})$ with $\lambda^{\sum_{i=0}^{n-2} p^{ir}} = 1$.
2. *r divides m, n divides $(p^r - 1)m/r$, $\boldsymbol{\alpha} = (1, a, a^{p^r+1}, \ldots, a^{\sum_{i=0}^{n-2} p^{ir}})$, is the orbit of 1 under $f(g) = ag^{p^r}$, $N_{GF(p^r)}(a) \neq 1$*
   $\mathbf{v} = (1, \lambda, \lambda^{p^r+1}, \ldots, \lambda^{\sum_{i=0}^{n-2} p^{ir}})$ with $\lambda^{\sum_{i=0}^{n-2} p^{ir}} = 1$.
3. *r divides m, n divides pm/r, $\boldsymbol{\alpha} = (0, b, b^{p^r} + b, \ldots, \sum_{j=0}^{n-2} b^{p^{jr}})$ is the orbit of 0 under $f(x) = x^{p^r} + b$, with $Tr_{GF(p^r)}(b) \neq 0$.*
   $\mathbf{v} = (1, \lambda, \lambda^{p^r+1}, \ldots, \lambda^{\sum_{i=0}^{n-2} p^{ir}})$ with $\lambda^{\sum_{i=0}^{n-2} p^{ir}} = 1$.
4. *$\boldsymbol{\alpha}$ is the orbit of an element α under $f(g) = \dfrac{1}{cg^{p^j} + d}$ without fixed point.*
   The scalar $\mathbf{v}$ is given by $v_{i+1} = (\lambda^{-1} v_i) u_f(\alpha_i)^{k-1})^{p^j}$ for all scalar $\lambda \in K^*$ verifying $v_n = v_0$.

PROOF. It is sufficient to explore the permutations of $P\Gamma L(2, K)$ given in Theorem 2.4.

1. $f(g) = g^{p^j}$: j is not necessarily a divisor of m. Let r be the greatest divisor of m and j. Let ℓ be an integer coprime to m such that $r \equiv j\ell \pmod m$. Since the length n is the orbit of an element α under f, n is a divisor of m, we can apply Lemma 2.5, replace f by $f^\ell : g \to g^{p^r}$, and then assume that $j = r$ is a divisor of m.

The length n is then a divisor of m/r. Assume that $n < m/r$. Let $r' = m/n$. Clearly $L_{\boldsymbol{\alpha}} = \{\alpha, \alpha^{p^r}, \dots, \alpha^{p^{(n-1)r}}\} = \{\alpha, \alpha^{p^{r'}}, \dots, \alpha^{p^{(n-1)r'}}\}$. Reordering $\boldsymbol{\alpha}$ by an appropriated permutation, we can assume that $\boldsymbol{\alpha}$ is the orbit of α under $f'(g) = g^{p^{r'}}$, substitute f' to f, and then assume that $n = m/r$. The values of the scalars v_i are the consequence of Lemma 2.6.

2. $f(g) = ag^{p^j}$: • *We can assume that $\boldsymbol{\alpha}$ is the orbit of 1 under f:*
$\boldsymbol{\alpha}$ is the orbit of an element $\alpha \in K^*$. Let $\varphi(g) = \alpha^{-1}g$. Let $\mathcal{A}_k(\mathbf{w}, \boldsymbol{\beta})$ be the image of $\mathcal{A}_k(\mathbf{v}, \boldsymbol{\alpha})$ by the operator $\mathcal{H}_\varphi$. This is the same Alternant code, but $\boldsymbol{\beta} = (1, f'(1), \dots, f'^{n-1}(1))$ is the orbit of 1 under $f'(g) = \varphi \circ f \circ \varphi^{-1}(g) = a'g^{p^j}$ with $a' = a\alpha^{1-p^j}$.

• *The length n is a divisor of $(p^r - 1)m/r$, where r is the greatest common divisor of j and m:*
Since the support is the orbit of 1 under f, n is the smaller integer such that $a^{\sum_{i=0}^{n-1} p^{ij}} = 1$. It is easy to verify that the set $J = \left\{ s \mid a^{\sum_{i=0}^{s-1} p^{ij}} = 1 \right\}$ is the set of multiples of n.

We will prove that $n' = (p^r - 1)m/r$ is an element of J and then n a divisor of $(p^r - 1)m/r$. Since r is the greatest divisor of j and m, there exists an integer s, coprime to m, such that $j \equiv sr \pmod m$. Let $N \equiv \sum_{i=0}^{n'-1} p^{ij} = \sum_{i=0}^{n'-1} p^{isr} \pmod{p^m}$, then $N \equiv \sum_{i=0}^{n'-1} p^{(is \bmod m/r)r} \pmod{p^m}$. This implies $N \equiv \sum_{i \bmod m/r, i \in \{0, n'-1\}} p^{(is \bmod m/r)r} \pmod{p^m}$.
The map $i \to is \pmod{m/r}$ is a permutation of the set $\{0, \dots, m/r - 1\}$. Moreover $n' = (p^r - 1)m/r$, and then finally $N \equiv (p^r - 1) \sum_{i=0}^{m/r-1} p^{ir} \pmod{p^m}$.

As a consequence, we obtain $a^N = a^{\sum_{i=0}^{n'-1} p^{ij}} = N_{GF(p^r)}(a)^{p^r-1} = 1$ and $n' \in J$ is a multiple of n.

• *We can assume that $j = r$ divides m:*
Let $n = uv$, where u is the greatest divisor of n coprime to m. Let w be the inverse of m modulo u. Let s be the integer coprime to m such that $sj \equiv r \pmod m$ and $s' = s + (1 - s)wm$. s' is coprime to n, indeed, by construction, $s' \equiv 1 \pmod u$, and each divisor of v divides m and cannot divide s and then s'. Moreover, $s'j \equiv s \pmod m$. Applying Lemma 2.5 and replacing f by $f^{s'} : g \to a'g^{p^r}$, we can suppose that $j = r$ is a divisor of m.

• The values of the scalars v_i are clear from Lemma 2.6.

3. $f(g) = g^{p^j} + b$:

• *We can assume that $\boldsymbol{\alpha}$ is the orbit of 0 under f:*

$\boldsymbol{\alpha}$ is the orbit of an element $\alpha \in K^*$. Let $\tau(g) = g - \alpha$. Let $\mathcal{A}_k(\mathbf{w}, \boldsymbol{\beta})$ be the image of $\mathcal{A}_k(\mathbf{v}, \boldsymbol{\alpha})$ by the operator $\mathcal{H}_\tau$. This is the same Alternant code, but $\boldsymbol{\beta} = (0, f'(0), \ldots, f'^{n-1}(0))$ is the orbit of 0 under $f'(g) = \tau \circ f \circ \tau^{-1}(g) = g^{p^j} + b'$ with $b' = b + \alpha^{p^j} - \alpha$.

In the sequel, we assume $\boldsymbol{\alpha} = (0, b, b+b^{p^j}, \ldots, \sum_{i=0}^{n-2} b^{p^{ij}})$, and $\sum_{i=0}^{n-1} b^{p^{ij}} = 0$.

• *The length n is a divisor of pm/r, where r is the greatest common divisor of j and m:*

The length n is the smaller integer such that $\sum_{i=0}^{n-1} b^{p^{ij}} = 0$. In that case, the set $J = \left\{ s \mid \sum_{i=0}^{s-1} b^{p^{ij}} = 0 \right\}$ is the set of multiples of n. We will prove that $n' = pm/r$ is an element of J and then n a divisor of pm/r. Since r is the greatest divisor of j and m, there exists an integer s, coprime to m, such that $j \equiv sr \pmod{m}$. Let $S = \sum_{i=0}^{n'-1} b^{p^{ij}} = \sum_{i=0}^{n'-1} b^{p^{isr}}$. Clearly, $b^{p^{isr}} = b^{p^{(is \bmod m/r)r}}$. Since $i \to si \pmod{m/r}$ is a permutation of $\{0, \ldots, m/r - 1\}$, we obtain $S = \sum_{i=0}^{n'-1} b^{p^{ir}}$, and then $S = pTr_{GF(p^r)(b)} = 0$.

The length n is a divisor of pm/r.

• *We can assume that $j = r$ divides m:*

Let s be an integer coprime to m such that $sj \equiv r \pmod{m}$. If p divides s, then p does not divide m, since s and m are coprime. Then $s' = s + m/r$ is coprime to m/r and is not divisible by p, hence, s' is prime to n. Then, it is always possible to find a s coprime to $n = pm/r$ such that $sj \equiv r \pmod{m}$. Using Lemma 2.5 and replacing f by $f^s : g \to g^{p^r} + b'$, we can assume that $j = r$ is a divisor of m.

• The values of the scalars v_i are clear from Lemma 2.6.

4. $f(g) = \dfrac{1}{cg^{p^j} + d}$: This case is a direct consequence of Theorem 2.2 and Theorem 2.4.

REMARK 2.8. If we look at the particular case $r = m$ in the second class, the length is a divisor of $p^m - 1$, and we obtain all the BCH codes over $GF(p)$ (non-narrow sense, not necessary primitive). In that case, the corresponding Cauchy codes are the cyclic codes of defining-sets $\{i+1, \ldots, i+n-k\}$ for some i and for $d = n - k + 1$, that is the BCH codes over $GF(p^m)$ of length dividing $p^m - 1$.

2.4. Some examples. In these examples, K is the finite field $GF(64) = GF(2)(\alpha)$ with $\alpha^6 = \alpha + 1$. The tables give a generator polynomial of the cyclic Alternant codes depending on values of λ and k.

Note that in these examples, there are many repeated-root cyclic codes.

• $f(g) = g^2$: We choose for support the orbit of α under f

$$\boldsymbol{\alpha} = (\alpha, \alpha^2, \alpha^4, \alpha^8, \alpha^{16}, \alpha^{32})$$

The length is $n = 5$. The scalar $\mathbf{v}$ depends on the value of $\lambda \in K$:

$$\mathbf{v} = (1, \lambda, \lambda^3, \lambda^7, \lambda^{15}, \lambda^{31})$$

λ	$k = 3$	$k = 4$	$k = 5$
1	$1 + x + x^2 + x^3 + x^4 + x^5$	$1 + x + x^2 + x^3 + x^4 + x^5$	$1 + x$
α^7	0	0	$1 + x^2 + x^4$
α^9	0	0	$1 + x + x^2$
α^{27}	0	$(1 + x)(1 + x^3)$	$1 + x^3$
α^{36}	0	$1 + x^2 + x^4$	$1 + x + x^2$

• $f(g) = \alpha g^8$: The support is the orbit of 1 under f.

$$\boldsymbol{\alpha} = (1, \alpha, \alpha^9, \alpha^{10}, \alpha^{18}, \alpha^{19}, \alpha^{27}, \alpha^{28}, \alpha^{36}, \alpha^{37}, \alpha^{45}, \alpha^{46}, \alpha^{54}, \alpha^{55})$$

The length is $n = 14$. The scalar $\mathbf{v}$ depends on the value of $\lambda \in K$:

$$\mathbf{v} = (1, \lambda, \lambda^9, \lambda^{10}, \lambda^{18}, \lambda^{19}, \lambda^{27}, \lambda^{28}, \lambda^{36}, \lambda^{37}, \lambda^{45}, \lambda^{46}, \lambda^{54}, \lambda^{55})$$

λ	$k = 11$	$k = 12$	$k = 13$
1	$(1 + x^2x^6)(1 + x^4 + x^6)$	$1 + x^4 + x^6$	$1 + x^4 + x^6$
α	$(1 + x^2)(1 + x^4 + x^6)$	$(1 + x^2)(1 + x^4 + x^6)$	$1 + x^2$
α^2	0	$(1 + x^2)(1 + x^2 + x^6)$	$1 + x^2 + x^6$
α^3	$(1 + x^2)(1 + x^2 + x^6)$	$1 + x^2 + x^6$	$1 + x + x^3$
α^4	$(1 + x^2 + x^6)(1 + x^4 + x^6)$	$(1 + x + x^3)(1 + x^4 + x^6)$	$1 + x^4 + x^6$

• $f(g) = g^2 + \alpha^5$: The support is the orbit of 0 under f.

$$\boldsymbol{\alpha} = (0, \alpha^5, \alpha^4, \alpha^{37}, \alpha^6, \alpha^{31}, 1, \alpha^{62}, \alpha^{24}, \alpha^{44}, \alpha^{34})$$

The length is $n = 12$. The scalar $\mathbf{v}$ depends on the value of $\lambda \in K$:

$$\mathbf{v} = (1, \lambda, \lambda^3, \lambda^7, \lambda^{15}, \lambda^{31}, 1, \lambda, \lambda^3, \lambda^7, \lambda^{15}, \lambda^{31})$$

λ	$k = 9$	$k = 10$	$k = 11$
1	$1 + x + \ldots + x^{11}$	$1 + x + \ldots + x^{11}$	$(1 + x)(1 + x + x^2)^2$
α	$1 + x + \ldots + x^{11}$	$(1 + x)(1 + x + x^2)^4$	$(1 + x + x^2)^2$
α^2	$1 + x + \ldots + x^{11}$	$1 + x + \ldots + x^{11}$	$(1 + x)(1 + x + x^2)^2$
α^3	$1 + x + \ldots + x^{11}$	$1 + x + \ldots + x^{11}x^i$	$(1 + x)(1 + x + x^2)^2$
α^4	$(1 + x)(1 + x^3)^2$	$(1 + x)(1 + x^3)^2$	$1 + x$
α^5	0	0	$(1 + x^3)^2$

• $f(g) = (\alpha g^2)^{-1}$: The support is the orbit of 1 under f.

$$\boldsymbol{\alpha} = (1, \alpha, \alpha^{62}, \alpha^3, \alpha^{58}, \alpha^{11}, \alpha^{42}, \alpha^{43}, \alpha^{41}, \alpha^{45}, \alpha^{37}, \alpha^{53}, \alpha^{21}, \alpha^{22}, \alpha^{20}, \alpha^{24}, \alpha^{16}, \alpha^{32})$$

The length is $n = 18$. The scalar $\mathbf{v}$ depends on the values of $\lambda \in K$ and k and is calculated by the recurrence relation $v_{i+1} = (\lambda v_i \alpha_i^{k-1})^2$.

For $\lambda = 1$

• $k = 16$,

$$\mathbf{v} = (1, 1, \alpha^{30}, \alpha^{30}, \alpha^{24}, \alpha^{24}, 1, 1, \alpha^{30}, \alpha^{30}, \alpha^{24}, \alpha^{24}, 1, 1, \alpha^{30}, \alpha^{30}, \alpha^{24}, \alpha^{24})$$

generator polynomial: $g(x) = 1 + x^6 + x^{12}$.

• $k = 17$,

$$\mathbf{v} = (1, 1, \alpha^{32}, \alpha^{32}, \alpha^{34}, \alpha^{34}, \alpha^{11}, \alpha^{11}, 1, 1, \alpha^{32}, \alpha^{32}, \alpha^{34}, \alpha^{34}, \alpha^{11}, \alpha^{11})$$

generator polynomial: $g(x) = 1 + x^2 + x^4$.

For $\lambda = \alpha$

- $k = 16$,

$$\mathbf{v} = (1, \alpha^2, \alpha^{36}, \alpha^{44}, \alpha^{54}, \alpha^{23}, 1, \alpha^2, \alpha^{36}, \alpha^{44}, \alpha^{54}, \alpha^{23}, 1, \alpha^2, \alpha^{36}, \alpha^{44}, \alpha^{54}, \alpha^{23})$$

generator polynomial: $g(x) = 1 + x^6 + x^{12}$.

- $k = 17$,

$$\mathbf{v} = (1, \alpha^2, \alpha^{38}, \alpha^{46}, \alpha, \alpha^{33}, \alpha^{42}, \alpha^{44}, \alpha^{17}, \alpha^{25}, \alpha^{43}, \alpha^{12}, \alpha^{21}, \alpha^{23}, \alpha^{59}, \alpha^4, \alpha^{22}, \alpha^{54})$$

generator polynomial: $g(x) = 1 + x^6$.

2.5. More about the no-fixed point case.

Let $f' \in P\Gamma L(2, K)$ defined by $f'(g) = \dfrac{1}{cg^{p^j} + d}$, such that f' has no fixed point in $\overline{K}$. Let $P(X) = X^{p^j+1} + uX + v = c^{-1}(cX^{p^j+1} + dX - 1$. The polynomial $P(X)$ has no root in K. Let K' be a finite split-extension of $P(X)$ over K. If $P(X)$ has at least three roots in K', f' is conjugated to $\gamma_{p^j} : g \to g^{p^j}$ in $PGL(2, K')$.

We will determine when f' has only two roots in K'. In that case, K' is an extension of degree two of K.

PROPOSITION 2.9. *The polynomial $P(X)$ has exactly two roots in K' if and only if $j \equiv 0 \pmod m$ (i.e; $f'(g) = (cg + d)^{-1}$).*

PROOF. Clearly, if $j = 0$, then $deg(P(X)) = 2$, let ε be a root of $P(X)$, $K' = K(\varepsilon) = K[X]/P(X)$ is an extension of degree two.

Suppose now that $0 < j < m$ and $P(X)$ has only two roots ε and ε^{p^m} in K'. Let $X^2 + aX + b$ be the minimal polynomial of ε, then $P(X) = (X^2 + aX + b)^{(p^j+1)/2}$. Note that, since $j > 0$, p must be odd. The monomial of degree p^j in the second member is $(p^j + 1)/2aX^{p^j}$ and must be zero. $(p^j - 1)/2$ is not zero modulo p and $a = 0$. The monomial of degree $p^j - 1$ in the second member is then $(p^j+1)/2bX^{p^j-1}$ and must be zero, that is impossible. □

THEOREM 2.10. *Let $\mathcal{A}_k(\mathbf{v}, \boldsymbol{\alpha})$ be a cyclic Alternant code induced by f such that $f \in PGL(2, K)$. Assume that f has no fixed points in $\overline{K}$. Then $\mathcal{C}_k(\mathbf{v}, \boldsymbol{\alpha})$ is a cyclic Cauchy code and the length n divides $p^m + 1$.*

More precisely, if ζ is a nth primitive root of unity in an extension K' of degree 2 of K, the code $\mathcal{C}_k(\mathbf{v}, \boldsymbol{\alpha})$ is one of the following BCH codes over K:

- *defining set:* $T = \left\{ -\dfrac{n-k-1}{2}, \ldots, \dfrac{n-k-1}{2} \right\}$,
  generator polynomial: $g(X) = \prod_{i \in T} (X - \zeta^i)$. *In that case, $k + n$ must be odd.*
- *defining set:* $T = \left\{ \dfrac{k+1}{2}, \ldots, n - \dfrac{k+1}{2} \right\}$,
  generator polynomial: $g(X) = \prod_{i \in T} (X - \zeta^i)$. *In that case, k must be odd.*

PROOF. Since $j = 0$, the automorphism group of $\mathcal{C}_k(\mathbf{v}, \boldsymbol{\alpha})$ contains the element $(\mathbf{1}; \sigma_f, 1)$ and $\boldsymbol{\alpha}$ is the orbit of an element α under f: the Cauchy code $\mathcal{C}_k(\mathbf{v}, \boldsymbol{\alpha})$ is cyclic. Let C' be the code over K' generated by the matrix $M_{k,\mathbf{v},\boldsymbol{\alpha}}$. If $g(X)$ is the generator polynomial of the cyclic code $\mathcal{C}_k(\mathbf{v}, \boldsymbol{\alpha})$ over K, it is also the generator

polynomial of C' over K'. Moreover, since $K \subset K'$, considering v_i and α_i as elements of K', C' is the Cauchy code $\mathcal{C}_k(\mathbf{v}, \boldsymbol{\alpha})$ over K'.

From Theorem 2.7 and Remark 2.8, these codes over K' are cyclic codes of defining-set $\{i+1, \ldots, i+d-1\}$ relative to a nth primitive root $\zeta \in K'$.

LEMMA 2.11. *The length n is a divisor of p^m+1.*

PROOF. The permutation $f \in PGL(2, K')$ is conjugate to ζg. All the orbits under f have the same length n. Moreover, since f leaves $\overline{K}$ globally invariant, $\overline{K}$ is a union of orbit under f and n must divide $|\overline{K}| = p^m + 1$. □

Let T be the defining-set of C' relatively to ζ. By definition, its monic generator polynomial of smallest degree is $g(X) = \prod_{j \in T}(X - \zeta^j) = \prod_{j=i+1}^{i+d-1}(X - \zeta^j)$. From preceeding remarks, $g(X)$ is the generator polynomial of $\mathcal{C}_k(\mathbf{v}, \boldsymbol{\alpha})$ over K, and then its coefficients are in K. If ζ^j is a root of $g(X)$, ζ^{jp^m} must be a root of $g(X)$. Note that $\zeta^{jp^m} = \zeta^{n-j}$ since $p^m \equiv -1 \pmod{n}$ (n divides p^m+1). The only possibilities for T are those given in our theorem.

□

REMARK 2.12. The class of BCH codes over K that are MDS codes is well-known, see for example [**3**] or [**5**] p.293.

References

[1] T.BERGER & P.CHARPIN, *The permutation group of affine-invariant extended cyclic codes,* Transactions on Information Theory IEEE, vol.42, n.6, p.2194-2209, 1996.

[2] T. Berger : *The automorphism group and the permutation group of an affine-invariant code.* "Finite fields and their application" (Glasgow, july 1995) edited by S. Cohen, H. Niederreiter, London Math. Society, Lecture Note Series 233, p.32-45, 1996.

[3] V.C. DA ROCHA JR., *Maximum distance separable multilevel codes,* IEEE Trans. on Info. Theory 30 p.547-548, (1984).

[4] A. DÜR *The Automorphism Group of Reed Solomon Codes,* J. of Combinatorial Theory, series A, vol. 4, 1 (1987).

[5] W. HEISE & P. QUATTROCCHI, *Informations und Codierungstheorie,* Springer, Berlin, 1983. Plus précis?

[6] C. HUFFMAN, Codes and Groups, *Handbook of Coding Theory, (V. Pless, C. Huffman, and R. Brualdi eds.*, To appear.

[7] F.J. MACWILLIAMS & N.J.A. SLOANE *The theory of Error Correcting Codes*, North-Holland 1986.

[8] H. Stichtenoth : *Which extended Goppa codes are cyclic?*, J. of Combinatorial Theory, A 51, p.205-220 (1989).

THIERRY P. BERGER, UFR DES SCIENCES DE LIMOGES, 123 AV. A. THOMAS, 87060 LIMOGES CEDEX, FRANCE

E-mail address: thierry.berger@unilim.fr

Contemporary Mathematics
Volume **225**, 1999

On Kerdock codes

Claude Carlet

ABSTRACT. The Kerdock codes have been characterized as $\mathbf{Z}_4$-linear codes by A. R. Hammons Jr., P. V. Kumar, A. R. Calderbank, N. J. A. Sloane and P. Solé. We show how their weight distributions can be derived by connecting sums over the Teichmuller sets to sums over the full Galois rings. We show also how the best known upper bound on their covering radii can be simply deduced from the computation of higher moments. We finally generalize a result from A.R. Calderbank and Gary McGuire concerning their projections on hyperplanes.

1. Introduction

The Kerdock code $\mathcal{K}_n$ (cf. [**8**], chap. 15), viewed as a set of Boolean (i.e. $GF(2)$-valued) functions on the set V_n of all binary words of even length $n \geq 4$, is a union of cosets of the Reed-Muller code of order 1, $R(1,n)$, in the Reed-Muller code of order 2, $R(2,n)$, and has the following property, that we will denote by $\mathcal{P}_{\mathcal{K}}$:

If the sum (i.e. the difference) of two elements of $\mathcal{K}_n$ is not affine, then this sum is bent.

Recall that a Boolean function on V_n is called *bent* if its Hamming distance to $R(1,n)$ is maximum. This distance – the covering radius of $R(1,n)$ – is known, since n is even, and is equal to $2^{n-1} - 2^{\frac{n}{2}-1}$.

A Boolean function f on V_n is bent if and only if (cf. [**8, 9**]) the Walsh (i.e. the discrete Fourier or Hadamard) transform of the real-valued function $f_\chi(x) = (-1)^{f(x)}$, that is[1]:

$$\widehat{f_\chi}(s) = \sum_{x \in V_n} (-1)^{f(x) \oplus x \cdot s}$$

has constant magnitude $2^{\frac{n}{2}}$.

f is bent if and only if, for any nonzero word s, the Boolean function $f(x) \oplus f(x+s)$ is balanced (i.e. takes the values 0 and 1 equally often).

$\mathcal{K}_n$ has the largest cardinality as a code of length 2^n that is the union of cosets of

---

1991 *Mathematics Subject Classification.* 94B65, 51E22.

[1]We denote by $\oplus$ the addition of Boolean functions, i.e. the addition mod 2; we need below to distinguish it from the addition of $\mathbf{Z}_4$-valued functions, denoted by $+$; however, the addition in V_n will be simply denoted by $+$ since all the words in this paper will be binary; we denote by $x \cdot s$ the usual dot product between two words s and x

© 1999 American Mathematical Society

$R(1,n)$ in $R(2,n)$ and whose minimum Hamming distance is equal to the covering radius of $R(1,n)$. It has more elements than any known linear code of the same length and minimum distance.
There exist other binary codes with the same distance enumerators (cf. [**5**]). All of them are subcodes of $R(2,n)$.
Hammons et al. give in [**4**] a characterization of $\mathcal{K}_n$ as a $\mathbf{Z}_4$-linear code:
. Let $\mathcal{R}$ be the Galois ring of order 4^m, where $m = n-1$. The Teichmuller set is denoted by $\mathcal{T}$ and has cardinality 2^m. It is equal to the set of the squares of all the elements of $\mathcal{R}$. There exists in $\mathcal{T}$ an element ξ such that $\xi^{2^m} = \xi$ and $\mathcal{T} = \{0, 1, \xi, \xi^2, \ldots, \xi^{2^m-2}\}$. The Galois ring $\mathcal{R}$ is equal to $\mathcal{T} + 2\mathcal{T}$. The set of its units is $\mathcal{R}^\star = \mathcal{T}^\star + 2\mathcal{T}$, where $\mathcal{T}^\star = \mathcal{T} - \{0\}$. We denote by ϕ the Frobenius automorphism on $\mathcal{R}$:

$$\phi(u + 2v) = u^2 + 2v^2,\ u, v \in \mathcal{T}$$

and by Tr the trace function from $\mathcal{R}$ to $\mathbf{Z}_4$:

$$Tr(z) = z + \phi(z) + \ldots + \phi^{m-1}(z),\ z \in \mathcal{R}.$$

. The Gray map is a mapping from $\mathbf{Z}_4$ to $(GF(2))^2$, that can be extended to a mapping from the set of all $\mathbf{Z}_4$-valued functions on a given set $\mathcal{E}$ to the set of all Boolean functions on $\mathcal{E} \times GF(2)$: any $\mathbf{Z}_4$-valued function can be written $2f(x) + g(x)$, where f and g take the values 0 and 1 only; the image of the function $2f(x) + g(x)$ by the Gray map is the function $(x, \epsilon) \in \mathcal{E} \times GF(2) \rightarrow f(x) \oplus \epsilon g(x)$, where f and g are considered as valued in $GF(2)$. Take $\mathcal{E} = \mathcal{T}$. We identify $\mathcal{T} \times GF(2)$ with $GF(2^m) \times GF(2)$, so that the functions $f(x) \oplus \epsilon g(x)$ are Boolean functions on $GF(2^m) \times GF(2) \simeq V_n$.
. It is proved in [**4**] that $\mathcal{K}_n$ is the set of the images by the Gray map of the restrictions to $\mathcal{T}$ of all the functions of the form: $F(x) = Tr(ax + b)$ (where a ranges over $\mathcal{R}$ and b over $\mathbf{Z}_4$). We will denote the set of these functions by $R_4(1,m)$. This interpretation of the Kerdock codes leads to an algebraic explanation of the formal duality between them and the Preparata codes.
It gives also a rather simple explanation of property $\mathcal{P}_\mathcal{K}$ of $\mathcal{K}_n$.

2. An explanation of property $\mathcal{P}_\mathcal{K}$ in terms of $\mathbf{Z}_4$-linear codes

The usual way to prove that $\mathcal{K}_n$ has property $\mathcal{P}_\mathcal{K}$ consists (cf. [**8**], chap. 15) in checking that every non-affine difference f of two elements of $\mathcal{K}_n$ has nondegenerate symplectic form $\varphi_f(x,y) = f(0) + f(x) + f(y) + f(x+y)$.
Hammons et al. [**4**] (resp. Calderbank et al. [**2**]) give a new proof of property $\mathcal{P}_\mathcal{K}$ by using the characterization of Kerdock codes as $\mathbf{Z}_4$-linear codes and by computing the squared magnitude (resp. the square) of the character sum $\sum_{x \in \mathcal{T}} i^{Tr(ax+b)}$; $i = \sqrt{-1}$.
We give now briefly a slightly different insight on the reasons why $\mathcal{P}_\mathcal{K}$ is satisfied.

It is well known that, if $f(x) \oplus \epsilon g(x)$ is a Boolean function on $GF(2^m) \times GF(2)$ and if $F(x)$ is the $\mathbf{Z}_4$-valued function equal to $2f(x) + g(x)$, then we have:

$$\sum_{(x,\epsilon) \in GF(2^m) \times GF(2)} (-1)^{f(x) \oplus \epsilon g(x)} = \sum_{x \in \mathcal{T}} i^{F(x)} + \sum_{x \in \mathcal{T}} i^{-F(x)}. \tag{2.1}$$

This property is still valid if we replace $f(x) \oplus \epsilon g(x)$ by a sum $f(x) \oplus \epsilon g(x) \oplus f'(x) \oplus \epsilon g'(x)$ and $F(x)$ by $F(x) - F'(x)$ (despite the fact that $f(x) \oplus \epsilon g(x) \oplus f'(x) \oplus \epsilon g'(x)$ is not the image of $F(x) - F'(x)$ by the Gray map).
This corresponds to the fact that the Gray map is a distance-preserving mapping from the set of $\mathbf{Z}_4$-valued functions (with Lee distance) on $\mathcal{T}$ to the set of Boolean functions on V_n (with Hamming distance).
We have, straightforwardly:

LEMMA 2.1. *For any $\mathbf{Z}_4$-valued function F on $\mathcal{T}$:*

$$\left(\sum_{x\in\mathcal{T}} i^{F(x)} + \sum_{x\in\mathcal{T}} i^{-F(x)}\right)^2 =$$

$$2^n + 2 \sum_{x\in\mathcal{T},\, y\in\mathcal{T},\, x\neq y} i^{F(x)-F(y)} + \sum_{x\in\mathcal{T},\, y\in\mathcal{T}} \left[i^{F(x)+F(y)} + i^{-F(x)-F(y)}\right].$$

We obtain now a relation between this expression and character sums computed over the whole rings $\mathcal{R}$ and $2\mathcal{R}$.

LEMMA 2.2. *If F is in $R_4(1,m)$ and $n = m+1$ is even, then:*

$$\left(\sum_{x\in\mathcal{T}} i^{F(x)} + \sum_{x\in\mathcal{T}} i^{-F(x)}\right)^2 = 2^n + 2\,[i^{F(0)} + i^{-F(0)}] \sum_{x\in\mathcal{R}} i^{F(x)} - 2\, i^{-F(0)} \sum_{x\in 2\mathcal{R}} i^{F(x)}.$$

PROOF. Set $F(x) = Tr(ax+b)$. We have, for any x, y in $\mathcal{R}$:

$$F(x) - F(y) = Tr(a(x-y)) = F(x-y) - F(0);$$

$$F(x) + F(y) = Tr(a(x+y) + 2b) = F(x+y) + F(0) \text{ and}$$

$$-F(x) - F(y) = Tr(a(-x-y) - 2b) = Tr(a(-x-y) + 2b) = F(-x-y) + F(0).$$

Thus, according to lemma 2.1:

$$\left(\sum_{x\in\mathcal{T}} i^{F(x)} + \sum_{x\in\mathcal{T}} i^{-F(x)}\right)^2 =$$

$$2^n + 2 \sum_{x\in\mathcal{T},\, y\in\mathcal{T},\, x\neq y} i^{F(x-y)-F(0)} + \sum_{x\in\mathcal{T},\, y\in\mathcal{T}} \left[i^{F(x+y)+F(0)} + i^{F(-x-y)+F(0)}\right] =$$

$$2^n + 2\, i^{-F(0)} \sum_{x\in\mathcal{T},\, y\in\mathcal{T},\, x\neq y} i^{F(x-y)} + i^{F(0)} \sum_{x\in\mathcal{T},\, y\in\mathcal{T}} \left[i^{F(x+y)} + i^{F(-x-y)}\right]. \tag{2.2}$$

The following lemma (cf. [**1, 4**]) completes the proof:

LEMMA 2.3. *For any m, let x and y range over $\mathcal{T}$ and $x \neq y$. Then:*

- *$x - y$ ranges once over $\mathcal{R}^\star$;*
- *if m is odd, then $\pm(x+y)$ ranges twice over $\mathcal{R}^\star$.*

□

We have therefore a simple explanation of the fact that every non-affine difference of two elements of $\mathcal{K}_n$ is bent:
let $f(x) \oplus \epsilon g(x)$ and $f'(x) \oplus \epsilon g'(x)$ be two elements of $\mathcal{K}_n$ and $F(x) = 2f(x) + g(x)$, $F'(x) = 2f'(x) + g'(x)$.
Accordingly to the definition of bent functions and to what has been recalled in the introduction of this section, we have to show that

$$\left(\sum_{x \in \mathcal{T}} i^{F(x)-F'(x)} + \sum_{x \in \mathcal{T}} i^{-F(x)+F'(x)} \right)^2$$

is equal to 2^n.
According to lemma 2.2 and since the image of the function $Tr(ax+b)$ by the Gray map is affine if and only if a belongs to $2\mathcal{R}$, cf. [**4**], it is enough to show that, for any a in $\mathcal{R}^\star$ and any b in $\mathbf{Z}_4$, both sums $\sum_{x \in \mathcal{R}} i^{Tr(ax+b)}$ and $\sum_{x \in 2\mathcal{R}} i^{Tr(ax+b)}$ are equal to zero, which is obvious.

3. Bounds on the covering radius of the Kerdock codes

The covering radius of a code C of length N is the maximum Hamming distance from any word of length N to C:

$$\rho(C) = max_{x \in V_N} \, min_{c \in C} \, w(x + c)$$

(we denote by $w(x)$ the Hamming weight of a word x).
When C is defined as a set of Boolean functions on V_n, its covering radius is the maximum Hamming distance from any Boolean function on V_n to C.
Recall that the weight of a Boolean function g on V_n is equal to $2^{n-1} - \frac{1}{2} \sum_{x \in V_n} (-1)^{g(x)}$.
Thus, if we denote by $\mathcal{B}_n$ the set of all the Boolean functions on V_n, $\rho(C)$ is equal to the number:

$$max_{g \in \mathcal{B}_n} \, min_{f \in C} \left(2^{n-1} - \frac{1}{2} \sum_{x \in V_n} (-1)^{g(x) \oplus f(x)} \right) =$$

$$2^{n-1} - \frac{1}{2} min_{g \in \mathcal{B}_n} \, max_{f \in C} \left(\sum_{x \in V_n} (-1)^{g(x) \oplus f(x)} \right).$$

If for any f in C, the function $f \oplus 1$ also belongs to C, we have:

$$\rho(C) = 2^{n-1} - \frac{1}{2} min_{g \in \mathcal{B}_n} \, max_{f \in C} \left| \sum_{x \in V_n} (-1)^{g(x) \oplus f(x)} \right|.$$

The covering radius of $\mathcal{K}_n$ is unknown.
There exists a straightforward lower bound for $\rho(\mathcal{K}_n)$:
since $\mathcal{K}_n$ is a strict subcode of the Delsarte-Goethals code $\mathcal{DG}(n, \frac{n}{2} - 1)$ (cf. [**8**] chap. 15, page 461), its covering radius is at least equal to the minimum distance of $\mathcal{DG}(n, \frac{n}{2} - 1)$ (cf. [**8**] chap. 15, page 465):

$$\rho(\mathcal{K}_n) \geq 2^{n-1} - 2^{\frac{n}{2}}.$$

An upper bound can be derived from the results by A. Tietavainen [**10**] and the fact that the dual distance of the Kerdock codes is 6:

$$\rho(\mathcal{K}_n) \leq 2^{n-1} - \frac{1}{2} \cdot \sqrt{3 \cdot 2^n - 2}. \tag{3.1}$$

Notice that $2^{n-1} - \frac{1}{2} \cdot \sqrt{3 \cdot 2^n - 2}$ is smaller than the minimum distance of $\mathcal{K}_n$, that is equal to $2^{n-1} - 2^{\frac{n}{2}-1}$. This bound implies that $\mathcal{K}_n$ is maximal.

We shall give here a direct proof of this upper bound, by using once again the definition of $\mathcal{K}_n$ as a $\mathbf{Z}_4$-linear code.
Accordingly to what has been recalled above, we have:

$$\rho(\mathcal{K}_n) = 2^{n-1} - \frac{1}{2} min_{g \in \mathcal{B}_n} \, max_{f \in \mathcal{K}_n} \, |\mu_g(f)|$$

where $\mu_g(f) = \sum_{x \in V_n} (-1)^{g(x) \oplus f(x)}$.
We shall derive our upper bound from the computation of the sums:

$$\sum_{f \in \mathcal{K}_n} (\mu_g(f))^2 \quad \text{and} \quad \sum_{f \in \mathcal{K}_n} (\mu_g(f))^4.$$

LEMMA 3.1. *For any Boolean function g on V_n, we have:*

$$\sum_{f \in \mathcal{K}_n} (\mu_g(f))^2 = 2^{3n}$$

and

$$\sum_{f \in \mathcal{K}_n} (\mu_g(f))^4 = 3 \cdot 2^{4n} - 2^{3n+1}.$$

PROOF. Set $k = 2$ (resp. 4). Let G be the $\mathbf{Z}_4$-valued function whose image by the Gray map is g. Function f is the image by the Gray map of $Tr(ax + b)$. According to the observation following relation (2.1), we have:

$$\sum_{f \in \mathcal{K}_n} (\mu_g(f))^k =$$

$$\sum_{a \in \mathcal{R}, b \in \mathbf{Z}_4} \; \sum_{x_1, \ldots, x_k \in \mathcal{T}} \; \sum_{\lambda_1, \ldots, \lambda_k \in \{-1, +1\}} i^{\sum_{j=1}^k \lambda_j (G(x_j) - Tr(ax_j + b))} =$$

$$\sum_{x_1, \ldots, x_k \in \mathcal{T}} \; \sum_{\lambda_1, \ldots, \lambda_k \in \{-1, +1\}} \left(i^{\sum_{j=1}^k \lambda_j G(x_j)} \sum_{a \in \mathcal{R}, b \in \mathbf{Z}_4} i^{Tr\left(a\left(\sum_{j=1}^k \lambda_j x_j\right) + \sum_{j=1}^k \lambda_j b\right)} \right).$$

The sum:

$$\sum_{a \in \mathcal{R}, b \in \mathbf{Z}_4} i^{Tr\left(a\left(\sum_{j=1}^k \lambda_j x_j\right) + \sum_{j=1}^k \lambda_j b\right)}$$

is nonzero if and only if it is constant, i.e.:

$$\sum_{j=1}^k \lambda_j x_j = 0 \quad \text{and} \quad \sum_{j=1}^k \lambda_j = 0 \, [\text{mod } 4], \tag{3.2}$$

in which case it is equal to $4^{m+1} = 2^{2n}$.
Assume first that $k = 2$. Then condition (3.2) is equivalent to $\lambda_2 = -\lambda_1$ and

$x_2 = x_1$, which implies: $\sum_{j=1}^{2} \lambda_j G(x_j) = 0$.

We deduce:

$$\sum_{f \in \mathcal{K}_n} (\mu_g(f))^2 = 2^{2n} \cdot 2^{m+1} = 2^{3n}.$$

Assume now that $k = 4$. Then:
- either all the λ_j's are equal to each other, in which case $x_1 + x_2 = -x_3 - x_4$; according to lemma 2.3, this is possible if $x_1 = x_2 = x_3 = x_4$ only;
- or two of them are equal to 1 and the others are equal to -1, in which case we can reorder the x_j's so that $x_1 - x_2 = x_3 - x_4$, and according to lemma 2.3, this is possible if $x_1 = x_2$ and $x_3 = x_4$ or if $x_1 = x_3$ and $x_2 = x_4$ only.

Thus, either we have $x_1 = x_2 = x_3 = x_4$ and the λ_j's can take any values ± 1 such that $\sum_{j=1}^{k} \lambda_j = 0 \bmod 4$ (which gives 8 possibilities), or there is a reordering of the x_j's such that $x_1 = x_2 \neq x_3 = x_4$ in which case $\lambda_1 = -\lambda_2$ and $\lambda_3 = -\lambda_4$ (which gives 4 possibilities).

In all cases, we have then: $\sum_{j=1}^{4} \lambda_j G(x_j) = 0$.

Thus:

$$\sum_{f \in \mathcal{K}_n} (\mu_g(f))^4 = 2^{2n} \left(2^m \cdot 8 + 3 \cdot 2^m (2^m - 1) \cdot 4\right) = 3 \cdot 2^{4n} - 2 \cdot 2^{3n}.$$

□

Obviously, the equality of lemma 3.1 corresponding to $k = 2$ can also be deduced from (binary) Parseval's relation: $\sum_{s \in V_n} \widehat{g_\chi}^2(s) = 2^{2n}$, that is valid for any Boolean function g on V_n. In the case $k = 4$, it can be considered as a generalization to $\mathbf{Z}_4$ of binary Parseval's relation (a generalization different from Parseval's relation on $\mathbf{Z}_4$).

We can now deduce the upper bound (3.1) from lemma 3.1:
for every Boolean function g, we have:

$$max_{f \in \mathcal{K}_n} \ (\mu_g(f))^2 \geq \frac{\sum_{f \in \mathcal{K}_n} (\mu_g(f))^4}{\sum_{f \in \mathcal{K}_n} (\mu_g(f))^2}.$$

Thus, according to lemma 3.1:

$$max_{f \in \mathcal{K}_n} \ (\mu_g(f))^2 \geq 3 \cdot 2^n - 2.$$

4. The projections of the Kerdock codes on hyperplanes

In [**2**], Calderbank and McGuire study the codes that are the projections on hyperplanes $h^\perp \times GF(2)$ ($h \neq 0$) of the elements of $\mathcal{K}_n$. By computing once again character sums over $\mathbf{Z}_4$, they prove that these codes have same distance distributions as the duals of the extended 2-error correcting BCH codes.
We show in theorem 4.1 that this property is not directly related to the $\mathbf{Z}_4$-linearity of $\mathcal{K}_n$ (notice that the proof of this theorem is simpler than in [**2**]).

THEOREM 4.1. *Let C be a union of cosets of $R(1,n)$, whose distance enumerator is same as that of $\mathcal{K}_n$. Let H be any hyperplane of V_n. Let C_H be the set of all the restrictions to H of the functions belonging to C. Then C_H has same distance distribution as the dual of the extended 2-error correcting BCH code of length 2^{n-1}.*

PROOF. The hypothesis implies that C has cardinality 2^{2n} and that it satisfies property $\mathcal{P}_{\mathcal{K}}$.

Thus: $C = \bigcup_{i=1}^{2^m} (f_i \oplus R(1,n))$, where $m = n-1$ and where the f_i's are Boolean functions on V_n such that $f_i \oplus f_j$ is bent for any $i \neq j$.

We give the proof in the case of a linear hyperplane. The general case is similar.

Let $u \neq 0$ be the unique vector in V_n such that $H = u^{\perp}$.

For any Boolean function f on V_n, we have, denoting by f_H its restriction to H and by $w(f_H)$ the Hamming weight of this restriction (considered as a function on V_m):

$$2^m - 2w(f_H) = \sum_{x \in H} (-1)^{f(x)} = \frac{1}{2}\left(\sum_{x \in V_n} (-1)^{f(x)} + \sum_{x \in V_n} (-1)^{f(x) \oplus u \cdot x} \right). \tag{4.1}$$

Assume now that f belongs to the coset $f_i \oplus f_j \oplus R(1,n)$, $i \neq j$.

f is bent. Thus, $\sum_{x \in V_n} (-1)^{f(x)}$ and $\sum_{x \in V_n} (-1)^{f(x) \oplus u \cdot x}$ are equal to $\pm 2^{\frac{n}{2}}$. According to (4.1), $w(f_H)$ is equal to $2^{m-1} \pm 2^{\frac{m-1}{2}}$ or to 2^{m-1}.

Notice that this implies that f_H cannot be equal to zero. So, if two elements of C belong to different cosets of $R(1,n)$, then their restrictions to H are different from each other. We can already assert that the cardinality of C_H is 2^{2n-1} (the restriction of R(1,n) to H is equivalent to the Reed-Muller code R(1,m)) and that C_H has same length, cardinality and minimum distance as the dual of the extended 2-error correcting BCH code, that is a $[2^m, 2m+1, 2^{m-1} - 2^{\frac{m-1}{2}}]$ linear code.

Let us prove now that it has same distance distribution: for every bent function f on V_n, let $\tilde{f}$ be the Boolean function such that (cf. [**3**]) $\widehat{f_\chi} = 2^{\frac{n}{2}} \tilde{f}_\chi$. For every word a in V_n, we have, according to (4.1) applied to the function $f(x) \oplus a \cdot x$:

$$\sum_{x \in H} (-1)^{f(x) \oplus a \cdot x} = 2^{\frac{n}{2}-1} \left((-1)^{\tilde{f}(a)} + (-1)^{\tilde{f}(a+u)} \right)$$

$$= 2^{\frac{n}{2}-1} (-1)^{\tilde{f}(a)} \left(1 + (-1)^{\tilde{f}(a) \oplus \tilde{f}(a+u)} \right).$$

We know that $\tilde{f}$ is bent too. Therefore, the function

$$a \to \tilde{f}(a) \oplus \tilde{f}(a+u)$$

is balanced. Hence, when a ranges over V_n and when ϵ ranges over $GF(2)$, the sum

$$\sum_{x \in H} (-1)^{f(x) \oplus a \cdot x \oplus \epsilon}$$

is equal to $\pm 2^{\frac{n}{2}}$ the same number of times as it is equal to 0.

Thus, among the 2^n restrictions to H of the elements of the coset $f \oplus R(1,n)$, 2^{m-1} have weight $2^{m-1} + 2^{\frac{n}{2}-1} = 2^{m-1} + 2^{\frac{m-1}{2}}$, 2^{m-1} have weight $2^{m-1} - 2^{\frac{m-1}{2}}$ and 2^m have weight 2^{m-1}.

Therefore, the distance distribution of C_H is:

$2^{m-1}+2^{\frac{m-1}{2}}$ for $2^{3m}(2^m-1)$ ordered pairs of elements of C_H,
$2^{m-1}-2^{\frac{m-1}{2}}$ for $2^{3m}(2^m-1)$ ordered pairs,
0 for 2^{2m+1} ordered pairs,
2^m for 2^{2m+1} ordered pairs,
and 2^{m-1} for $2^{3m+1}(2^m-1)+2^{2m+1}(2^{m+1}-2)=2^{4m+1}+2^{3m+1}-2^{2m+2}$ ordered pairs.
This is the distance distribution of the dual of the extended 2-error correcting BCH code of length 2^m. □

REMARK 4.2. If we assume as in [**2**] that C is a $\mathbf{Z}_4$-linear code and that $H = h^\perp \times GF(2)$, then this proof can be shortened:
C and C_H being $\mathbf{Z}_4$-linear, they are distance-invariant and admit $\mathbf{Z}_4$-duals. It is enough to prove that the nonzero weights in C_H are $2^{m-1}\pm 2^{\frac{m-1}{2}}$, 2^{m-1} and 2^m only, without checking what are the numbers of words of each weight. Indeed, it is a simple matter to show that the minimum weight of the $\mathbf{Z}_4$-dual of C_H is at least equal to that of the $\mathbf{Z}_4$-dual of C, which is 6; this provides 6 equations on the numbers of words of each weight, that determine them uniquely.

REMARK 4.3. In [**2**] is proved that, if H is the hyperplane $h^\perp \times GF(2)$ and $\mathcal{DG}$ is the Delsarte-Goethals code of length 2^n and minimum distance $2^m-2^{\frac{m+1}{2}}$, then $\mathcal{DG}_H$ has same distance distribution as the extended 3-error correcting BCH code of same length.
This can be very shortly checked by using relation (4.1).
Indeed, we have already seen that if $f \in \mathcal{DG}$ is bent, then, $\sum_{x\in V_n}(-1)^{f(x)}$ and $\sum_{x\in V_n}(-1)^{f(x)\oplus u\cdot x}$ are equal to $\pm 2^{\frac{n}{2}}$ and that $w(f_H)$ is equal to $2^{m-1}\pm 2^{\frac{m-1}{2}}$ or to 2^{m-1}.
Otherwise, and if $f \in \mathcal{DG}$ is not affine, then $\sum_{x\in V_n}(-1)^{f(x)}$ and $\sum_{x\in V_n}(-1)^{f(x)\oplus u\cdot x}$ are equal either to $\pm 2^{\frac{n}{2}+1}$ or to 0 and $w(f_H)$ is then equal to $2^{m-1}\pm 2^{\frac{m+1}{2}}$, to $2^{m-1}\pm 2^{\frac{m-1}{2}}$ or to 2^{m-1}.
It is shown in [**2**] that these facts give the desired conclusion.

Acknowledgement

We thank V.I. Levenshtein, Simon Litsyn and Jean-Pierre Tillich for helpful discussions.

References

[1] A. BONNECAZE & I. DUURSMA, *Translates of Linear Codes over* $\mathbf{Z}_4$, IEEE Trans. on Inf. Theory, vol. 43, n° 4, p. 1218-1230 (1997)
[2] A.R. CALDERBANK & GARY MCGUIRE, $\mathbf{Z}_4$*-linear codes obtained as projections of Kerdock and Delsarte-Goethals codes*, Linear Algebra and its Applications 226/228, p. 647-665 (1995).
[3] J. F. DILLON, *Elementary Hadamard Difference Sets*, Ph. D. Thesis, Univ. of Maryland (1974).
[4] A. R. HAMMONS JR., P. V. KUMAR, A. R. CALDERBANK, N. J. A. SLOANE & P. SOLÉ, *The* Z_4*-linearity of Kerdock, Preparata, Goethals and related codes* IEEE Transactions on Information Theory, vol 40, p. 301-320, (1994)
[5] W. KANTOR, *An Exponential Number of Generalized Kerdock Codes*, Inf. and Contr. 53, p. 74-80 (1982).

[6] B.R. MacDonald, *Finite rings with identity*, Marcel Dekker, NY, 1974
[7] A.A. Nechaev, *The Kerdock code in a cyclic form*, Discrete Math. Appl., vol 1, p. 123-139 (1989).
[8] F. J. Mac Williams & N. J. Sloane, *The theory of error-correcting codes*, Amsterdam, North Holland 1977.
[9] O. S. Rothaus, *On bent functions*, J. Comb. Theory, 20A, p. 300-305 (1976)
[10] A. Tietavainen, *An upper bound on the covering radius of codes as a function of the dual distance*, IEEE Trans. on Inf. Theory 36, N° 6, p. 1472-1474 (1990).

Claude Carlet, INRIA Projet CODES, Domaine de Voluceau, BP 105, 78153 Le Chesnay Cedex, France; and GREYC, Université de Caen, France.
E-mail address: Claude.Carlet@inria.fr

This page intentionally left blank

Contemporary Mathematics
Volume **225**, 1999

Permutation Group of the q-ary Image of Some q^m-ary Cyclic Codes

Jérôme Lacan and Emmanuelle Delpeyroux

ABSTRACT. We are interested in the q-ary image of some q^m-ary cyclic code C of length N equal to $q^m - 1$. For some bases $\underline{\alpha}$, we give a construction of a generator matrix of the q-ary image of C as a block matrix where each block is a generator matrix of a cyclic code of length N over F_q.

For some codes C and using the particular form of the constructed generator matrix of its q-ary image, we define a group of permutations such that its q-ary image is invariant under the action of these permutations.

Then, we prove that if the code C is such that its q-ary image is invariant under the action of the previous group then its q-ary image is equivalent to a 2-D abelian code. When $(N, m) = 1$, it is equivalent to a cyclic code.

1. Introduction

One important area in coding theory is concerned with codes invariant under some permutations.

As an illustration, any linear code of length N over F_{q^r} (i.e. vector subspace of $(F_{q^r})^N$) which has the property to be invariant under the cyclic permutation (shift) is called cyclic code. This property permits to consider this code as a principal ideal in the algebra $F_{q^r}[z]/(z^N - 1)$. When $(N, q) = 1$, a cyclic code is entirely defined by the set of its nonzeroes which are the N^{th} roots of unity which not vanish at least one codeword. This code is usually denoted by $[N, K]$, where K is the dimension of the code considered as a F_{q^r}-vector subspace. But K is also the number of nonzeroes. In this paper, we need to split up two codes of same dimension. So we denote by $[N, NZ]_{q^r}$ a such code, where NZ is the set of nonzeroes. Moreover, if $g(z)$ is a generator of this code then $\{g(z), zg(z), \ldots, z^{K-1}g(z)\}$ is a F_{q^r}-basis of the code generated by $g(z)$, and we call generator matrix of this code the matrix equal to :

$$\begin{bmatrix} g(z) \\ zg(z) \\ \cdots \\ z^{K-1}g(z) \end{bmatrix}.$$

1991 *Mathematics Subject Classification.* 11T71.

Similary, an abelian code over F_{q^r} is a vector subspace of $(F_{q^r})^{mN}$ invariant under the shift of the rows and the columns when we consider each codeword as a $m \times N$-matrix [**6**].

Many researchers have worked on codes invariant under some groups of permutations as for example the general linear group [**3**] [**2**] [**1**] or the Mathieu group [**5**, chap. 20].

The use of permutations has repercussions on the minimal distance [**3**] [**2**] or on the decoding [**3**] [**9**] of the codes.

The problem we adress in this paper is that of determining a group of permutations such that the q-ary image of some q^m-ary cyclic codes is invariant under the action of these permutations.

Let us introduce the q^s-ary image of a q^r-ary cyclic code when F_{q^s} is a subfield of F_{q^r}.

Let β be an element of F_{q^r}. The elements $\beta, \beta^{q^s}, \ldots, \beta^{q^{s(\frac{r}{s}-1)}}$ are called the conjugates of β with respect to F_{q^s} ([**4**, chap. 2, def. 2.17]). The set of these elements is denoted by $\mathcal{C}_{q^s}(\beta)$.

Let $a(z)$ be in $F_{q^r}[z]/(z^N-1)$ such that $a(z) = \sum_{j=0}^{N-1} a_j z^j$. Let $\underline{\alpha}$ be a basis of F_{q^r} over F_{q^s}. Let us denote this basis by $\{\alpha_0, \alpha_1, \ldots, \alpha_{\frac{r}{s}-1}\}$. Then the polynomial $a(z)$ may be also expressed as $\sum_{j=0}^{N-1} \sum_{i=0}^{\frac{r}{s}-1} a_{i,j}\alpha_i z^j$, where $a_{i,j} \in F_{q^s}$.

We define the q^s-ary image of $a(z)$ with respect to the basis $\underline{\alpha}$ by the bijective module homomorphism :

$$\mathcal{D}_{\underline{\alpha}} \; : \; \left\{ \begin{array}{ccc} F_{q^r}[z]/(z^N-1) & \longrightarrow & (F_{q^s}[x]/(x^N-1))^{\frac{r}{s}} \\ a(z) & \longrightarrow & (a_0(x), a_1(x), \ldots, a_{\frac{r}{s}-1}(x)) \end{array} \right.$$

where $a_i(x) = \sum_{j=0}^{N-1} a_{i,j}x^j$.

The q^s-ary image of $[N, NZ]_{q^r}$ with respect to the basis $\underline{\alpha}$ is denoted by $\mathcal{D}_{\underline{\alpha}}([N, NZ]_{q^r})$, and we have : $\mathcal{D}_{\underline{\alpha}}([N, NZ]_{q^r}) = \{\mathcal{D}_{\underline{\alpha}}(c(z))/c(z) \in [N, NZ]_{q^r}\}$. Then $\mathcal{D}_{\underline{\alpha}}([N, NZ]_{q^r})$ is a submodule of the $F_{q^s}[x]/(x^N-1)$-module $(F_{q^s}[x]/(x^N-1))^{\frac{r}{s}}$.

Recently, G. E. Seguin has solved the well known problem which consists in determining the conditions such that $\mathcal{D}_{\underline{\alpha}}([N, NZ]_{q^r})$ is a cyclic code. This result is proved under the only restriction $(N, q) = 1$. When $(N, q) = p^l$ (p is the characteristic of F_q) a part of this problem is solved in [**8**].

If $\{(c_0^{(i)}(x), c_1^{(i)}(x), \ldots, c_{\frac{r}{s}-1}^{(i)}(x))$, for $i = 0, \ldots, \frac{r}{s}K - 1\}$ is a F_{q^s}-basis of $\mathcal{D}_{\underline{\alpha}}([N, NZ]_{q^r})$, we call F_{q^s}-generator matrix of $\mathcal{D}_{\underline{\alpha}}([N, NZ]_{q^r})$ the matrix :

$$\begin{bmatrix} c_0^{(0)}(x) & \ldots & c_{\frac{r}{s}-1}^{(0)}(x) \\ & \ldots & \\ c_0^{(\frac{r}{s}K-1)}(x) & \ldots & c_{\frac{r}{s}-1}^{(\frac{r}{s}K-1)}(x) \end{bmatrix}.$$

Now, let C be some code equal to $[N = q^m - 1, NZ]_{q^m}$ and let $\underline{\alpha}$ be a basis of F_{q^m} over F_q.

This paper is divided in five parts. In part 2 we give a construction of a F_q-generator matrix of $\mathcal{D}_{\underline{\alpha}}(C)$ as a block matrix. Such a construction is made in [**9**], but in our paper we completely characterize each block as a generator matrix of a cyclic code of length N over F_q. This characterization is necessary to show the invariance of some $\mathcal{D}_{\underline{\alpha}}(C)$ under the action of some groups of permutations.

In part 3 we define some sets of permutations, and we prove that each one is a group.

Then we consider the particular code C_1 equal to $[N, \{\beta\}]_{q^m}$, where β a primitive element of F_{q^m}. In part 4 we prove that there exists a group of permutations such that $\mathcal{D}_{\underline{\alpha}}(C_1)$ is invariant under the action of this group. Moreover we characterize some other code C such that $\mathcal{D}_{\underline{\alpha}}(C)$ is also invariant under the action of some of these groups.

Finally, in part 5 we give some consequences of these results. We prove that if C is such that $\mathcal{D}_{\underline{\alpha}}(C)$ is invariant under the action of some of these groups then $\mathcal{D}_{\underline{\alpha}}(C)$ is equivalent to a 2-D abelian codes. When $(N, m) = 1$, $\mathcal{D}_{\underline{\alpha}}(C)$ is equivalent to a cyclic code and this result solves a part of an open problem given by G. E. Seguin in [7].

2. Generator matrix of $\mathcal{D}_{\underline{\alpha}}(C)$

Let C be some code equal to $[N = q^m - 1, NZ]_{q^m}$ and let $\underline{\alpha}$ be a basis of F_{q^m} over F_q. We give a construction of a F_q-generator matrix of $\mathcal{D}_{\underline{\alpha}}(C)$ as a block matrix where each block is a generator matrix of a cyclic code of length N over F_q.

2.1. Preliminaries and idea of the construction. In order to construct this matrix we need to construct a partition of NZ (the set of nonzeroes of C). This construction is the following :

Let $F_{q^{r_1}}$ be the smallest subfield of F_{q^m} in which we can construct the largest (non empty) union of full sets of conjugates with elements of NZ with respect to $F_{q^{r_1}}$. Denote this union by NZ_1.

At the step i, let $F_{q^{r_i}}$ be the smallest subfield of F_{q^m} with $r_1 < r_2 < \ldots < r_i$ in which we can construct the largest (non empty) union of full sets of conjugates with elements of $NZ \setminus \cup_{j=1}^{i-1} NZ_j$ with respect to $F_{q^{r_i}}$. Denote this union by NZ_i.

Then the partition is : $NZ_1 \cup NZ_2 \cup \ldots NZ_t$.

EXAMPLE 2.1. Let β be a primitive element of F_{2^6}. Suppose that $NZ = \{\beta, \beta^2, \beta^4, \beta^8, \beta^{16}, \beta^{32}, \beta^3, \beta^6, \beta^{12}, \beta^{24}, \beta^{48}, \beta^{33}, \beta^9, \beta^{18}, \beta^5\}$. Then we have : $r_1 = 1$, $NZ_1 = \mathcal{C}_0(\beta) \cup \mathcal{C}_0(\beta^3)$, $r_2 = 3$, $NZ_2 = \mathcal{C}_{2^3}(\beta^9) \cup \mathcal{C}_{2^3}(\beta^{18})$, and $r_3 = 6$, $NZ_3 = \mathcal{C}_{2^6}(\beta^5)$.

In fact each subfield $F_{q^{r_i}}$ is associated to a subset NZ_i of NZ and this pair leads us to consider the subfield subcode $[N, NZ_i]_{q^{r_i}}$ of C. We denote this subfield subcode by C_i.

For each $i = 1, ..., t$, we construct in part 2.2 a particular F_q-generator matrix of the q-ary image of C_i. The part 2.3 is the construction of a particular $F_{q^{r_i}}$-generator matrix of the q^{r_i}-ary image of the code $[N, NZ_i]_{q^m}$. Finally $C = \oplus_{i=1}^{t} [N, NZ_i]_{q^m}$. We will see in part 2.4 how these two parts permit us to construct a F_q-generator matrix of $\mathcal{D}_{\underline{\alpha}}([N, NZ_i]_{q^m})$ and thus a F_q-generator matrix of $\mathcal{D}_{\underline{\alpha}}(C)$.

2.2. Generator matrix of the q-ary image of C_i. For each $i = 1, \ldots, t$, consider the subfield subcode C_i. The subset NZ_i is an union of full sets of conjugates with respect to $F_{q^{r_i}}$:

$$NZ_i = \bigcup_{j=1}^{t_i} \mathcal{C}_{q^{r_i}}(\beta_{i,j}), \text{ where } \beta_{i,j} \in NZ_i.$$

Let $C_{i,j}$ be the code $[N, \mathcal{C}_{q^{r_i}}(\beta_{i,j})]_{q^{r_i}}$. Clearly, $C_i = \oplus_{j=1}^{t_i} C_{i,j}$. Let $\theta_{i,j}(z)$ be the primitive idempotent of $[N, \mathcal{C}_q(\beta_{i,j})]_q$. Then a generator of $C_{i,j}$ may be expressed as :

$$g_{i,j}(z) = \theta_{i,j}(z) \prod_{b \in \mathcal{C}_q(\beta_{i,j}) \setminus \mathcal{C}_{q^{r_i}}(\beta_{i,j})} (z - b).$$

Let $\underline{\delta} = \{\delta_0, \ldots, \delta_{r_i - 1}\}$ be a basis of $F_{q^{r_i}}$ over F_q. Then the previous generator may be also expressed as :

$$g_{i,j}(z) = \theta_{i,j}(z)[b_{i,j}^{(0)}(z)\delta_0 + b_{i,j}^{(1)}(z)\delta_1 + \ldots + b_{i,j}^{(r_i-1)}(z)\delta_{r_i-1}]$$

where each $b_{i,j}^{(l)}(z)$ has its coefficients in F_q.

PROPOSITION 2.2. *For $j = 1, \ldots, t_i$, let $B_{i,j}$ be the matrix :*

$$\begin{bmatrix} \theta_{i,j}(x)b_{i,j}^{(0)}(x) & \ldots & \theta_{i,j}(x)b_{i,j}^{(r_i-1)}(x) \\ x\theta_{i,j}(x)b_{i,j}^{(0)}(x) & \ldots & x\theta_{i,j}(x)b_{i,j}^{(r_i-1)}(x) \\ & \ldots & \\ x^{|\mathcal{C}_q(\beta_{i,j})|-1}\theta_{i,j}(x)b_{i,j}^{(0)}(x) & \ldots & x^{|\mathcal{C}_q(\beta_{i,j})|-1}\theta_{i,j}(x)b_{i,j}^{(r_i-1)}(x) \end{bmatrix}.$$

Then $B_{i,j}$ is the F_q-generator matrix of $\mathcal{D}_{\underline{\delta}}(C_{i,j})$.

PROOF. The first row of $B_{i,j}$ is equal to $\mathcal{D}_{\underline{\delta}}(g_{i,j}(z))$. Thus each row of $B_{i,j}$ is in $\mathcal{D}_{\underline{\delta}}(C_{i,j})$.

Let us prove that these $|\mathcal{C}_q(\beta_{i,j})|$ rows are linearly independant. Clearly, there exists at least one $\theta_{i,j}(x)b_{i,j}^{(l_0)}(x)$ non equal to 0. On the other hand, the code $[N, \mathcal{C}_q(\beta_{i,j})]_q$ (generated for example by $\theta_{i,j}(x)$) is irreducible (see [**6**, chap. 5]), it follows that it is also generated by $\theta_{i,j}(x)b_{i,j}^{(l_0)}(x)$, and $\{x^k\theta_{i,j}(x)b_{i,j}^{(l_0)}(x), k = 0, \ldots, |\mathcal{C}_q(\beta_{i,j})| - 1\}$ is a F_q-basis of $[N, \mathcal{C}_q(\beta_{i,j})]_q$. This proves that the $|\mathcal{C}_q(\beta_{i,j})|$ rows are linearly independant.

Moreover, $dim_{F_q}\mathcal{D}_{\underline{\delta}}(C_{i,j}) = r_i dim_{F_{q^{r_i}}} C_{i,j} = r_i dim_{F_{q^{r_i}}}[N, \mathcal{C}_{q^{r_i}}(\beta_{i,j})]_{q^{r_i}} = r_i|\mathcal{C}_{q^{r_i}}(\beta_{i,j})| = |\mathcal{C}_q(\beta_{i,j})|$ $(= dim_{F_q}[N, \mathcal{C}_q(\beta_{i,j})]_q)$. This completes the proof. □

As $C_i = \oplus_{j=1}^{t_i} C_{i,j}$, a F_q-generator matrix of $\mathcal{D}_{\underline{\delta}}(C_i)$ may be expressed as :

$$M_i = \begin{bmatrix} B_{i,1} \\ \ldots \\ B_{i,t_i} \end{bmatrix} = \begin{bmatrix} b_{i,1}^{(0)}(x)M_{i,1} & \ldots & b_{i,1}^{(r_i-1)}(x)M_{i,1} \\ & \ldots & \\ b_{i,t_i}^{(0)}(x)M_{i,t_i} & \ldots & b_{i,t_i}^{(r_i-1)}(x)M_{i,t_i} \end{bmatrix},$$

where $M_{i,j}$ is the following particular generator matrix of $[N, \mathcal{C}_q(\beta_{i,j})]_q$:

$$\begin{bmatrix} \theta_{i,j}(x) \\ x\theta_{i,j}(x) \\ \ldots \\ x^{|\mathcal{C}_q(\beta_{i,j})|-1}\theta_{i,j}(x) \end{bmatrix}.$$

When $b_{i,j}^{(l)}(x)$ is not equal to 0, the matrix $b_{i,j}^{(l)}(x)M_{i,j}$ is also a generator matrix of $[N, \mathcal{C}_q(\beta_{i,j})]_q$ (it is because $[N, \mathcal{C}_q(\beta_{i,j})]_q$ is irreducible).

Thus M_i is compound of block matrices generating cyclic codes over F_q.

2.3. Generator matrix of the q^{r_i}-ary image of $[N, NZ_i]_{q^m}$. For each $i = 1, \ldots, t$, let $\underline{\gamma} = \{\gamma_0, \gamma_1, \ldots, \gamma_{\frac{m}{r_i}-1}\}$ be a basis of F_{q^m} over $F_{q^{r_i}}$, and let $\{g_0(z), \ldots, g_{|NZ_i|-1}(z)\}$ be a basis of C_i over $F_{q^{r_i}}$.

For $j = 0, \ldots, \frac{m}{r_i} - 1$, we define by $\gamma_j C_i$ the set $\{\gamma_j c(z)$ such that $c(z) \in C_i\}$. Clearly, for $j = 0, \ldots, \frac{m}{r_i} - 1$, $\gamma_j C_i$ is a subcode of C and $\{\gamma_j g_k(z)$ for $k = 0, \ldots, |NZ_i| - 1\}$ is a basis of $\gamma_j C_i$.

Then the $|NZ_i| \times \frac{m}{r_i}$ elements of $\cup_{j=0}^{\frac{m}{r_i}-1} \{\mathcal{D}_{\underline{\gamma}}(\gamma_j g_k(z)), k = 0, \ldots, |NZ_i|-1\}$ may be considered as the rows of a $F_{q^{r_i}}$-generator matrix of $\mathcal{D}_{\underline{\gamma}}([N, NZ_i]_{q^m})$. These rows form a block matrix :

$$\mathcal{T}_i = \begin{bmatrix} \mathcal{M}_i & 0 & \ldots & 0 \\ 0 & \mathcal{M}_i & \ldots & 0 \\ & \ldots & \ldots & \\ 0 & 0 & \ldots & \mathcal{M}_i \end{bmatrix},$$

where $\mathcal{M}_i$ is a generator matrix of C_i over $F_{q^{r_i}}$.

2.4. Construction of the F_q-generator matrix of $\mathcal{D}_{\underline{\alpha}}(C)$. Now, using the two previous parts, we can construct a F_q-generator matrix of $\mathcal{D}_{\underline{\alpha}}(C)$.

For that, the basis $\underline{\alpha}$ of F_{q^m} over F_q must be choosed such that $\underline{\alpha}$ is the direct product of a basis of F_{q^m} over $F_{q^{r_i}}$ with a basis of $F_{q^{r_i}}$ over F_q and this for every subfield $F_{q^{r_i}}$ of F_{q^m}. It is easy to verify that at least one such basis exists. So, for each i, we choose the bases used in parts 2.2 and 2.3 such that their direct product is equal to $\underline{\alpha}$.

Finally, in order to obtain a F_q-generator matrix of $\mathcal{D}_{\underline{\alpha}}([N, NZ_i]_{q^m})$ it is sufficient to replace $\mathcal{M}_i$ (part 2.3) by M_i (part 2.2) in $\mathcal{T}_i$. Let us call T_i the obtained matrix. If $r_1 = 1$ then $\mathcal{M}_1 = M_1$ and then $\mathcal{T}_1 = T_1$. If $r_t = m$ then $T_t = M_t$.

Since C is the direct sum of the codes $[N, NZ_i]_{q^m}$ (for $i = 1, ..., t$), a F_q-generator matrix of $\mathcal{D}_{\underline{\alpha}}(C)$ is :

$$\begin{bmatrix} T_1 \\ T_2 \\ \ldots \\ T_t \end{bmatrix}.$$

This matrix generates $\mathcal{D}_{\underline{\alpha}}(C)$ and it is compound of block matrices generating cyclic codes over F_q (see part 2.2).

3. Groups of permutations

Let us introduce the following sets of permutations.

DEFINITION 3.1. Let $(w_0, w_1, \ldots, w_{m-1})$ be some m-tuple, where each w_i is in $Z/(N)$. We define by (l, σ, a) the permutation of $\{0, 1, \ldots, m-1\} \times Z/(N)$ which send (i, j) onto $(\sigma(i), (j + s_i^{(l,\sigma)})q^l + a)$, where :

1- $\sigma \in S_m$ (the group of permutations of $\{0, 1, \ldots, m-1\}$)

2- $a \in Z/(N)$ and $l \in \{0, 1, \ldots, m-1\}$

3- $s_i^{(l,\sigma)} = q^{-l} w_{\sigma(i)} - w_i$, for $i = 0, 1, \ldots, m-1$.

Let us denote by $\mathcal{P}$ the set $\{(l, \sigma, a), l = 0, 1, \ldots, m-1, \sigma \in S_m$ and $a \in Z/(N)\}$.

PROPOSITION 3.2. *If $\circ$ is the law of composition, then*

1- $(\mathcal{P}, \circ)$ is a group.

2- The generators of this group are $(0, id, 1)$, $(1, id, 0)$, and the set of $(0, \sigma, 0)$ for σ in the set of the generators of S_m.

3- $|\mathcal{P}| = m \times m! \times N$.

PROOF. 1- Clearly $(l_1, \sigma_1, a_1) \circ (l_2, \sigma_2, a_2)$ is equal to $(l_1 + l_2, \sigma_1 \circ \sigma_2, a_1 + a_2 q^{l_1})$ which is also an element of $\mathcal{P}$. Moreover for all $(l, \sigma, a) \in \mathcal{P}$ we have the two following equalities :

- $(l, \sigma, a) \circ (0, id, 0) = (0, id, 0) \circ (l, \sigma, a) = (l, \sigma, a)$
- $(l, \sigma, a) \circ (-l, \sigma^{-1}, -q^{-l}a) = (0, id, 0)$

So, $\mathcal{P}$ is a group for the law of composition.

2- Direct.

3- It is sufficient to show that all these permutations are different. Let (l_1, σ_1, a_1) and (l_2, σ_2, a_2) be two permutations. Let us suppose that, for all pair (i, j), we have $(\sigma_1(i), (j + s_i^{(l_1, \sigma_1)})q^{l_1} + a_1) = (\sigma_2(i), (j + s_i^{(l_2, \sigma_2)})q^{l_2} + a_2)$. Then $\sigma_1 = \sigma_2$. Thus, for $\sigma_1 = \sigma_2 = \sigma$ and for all pair (i, j), we have :

$$(j + q^{m-l_1} w_{\sigma(i)} - w_i)q^{l_1} + a_1 \equiv (j + q^{m-l_2} w_{\sigma(i)} - w_i)q^{l_2} + a_2 \textit{ modulo } N.$$

So, for all pair (i, j), we have :

$$q^{l_1} j - w_i q^{l_1} + a_1 \equiv q^{l_2} j - w_i q^{l_2} + a_2 \textit{ modulo } N,$$

$$\textit{i.e. } (j - w_i)(q^{l_1} - q^{l_2}) + a_1 - a_2 \equiv 0 \textit{ modulo } N.$$

Since there exists a pair (i, j) such that $j - w_i \equiv 0$ modulo N, we have $a_1 \equiv a_2$ modulo N.

Moreover, there exists a pair (i, j) such that $(j - w_i, N) = 1$. Thus, $q^{l_1} - q^{l_2} \equiv 0$ modulo N and then $l_1 = l_2$. □

We define the action of $\mathcal{P}$ over an element of $(F_q[x]/(x^N - 1))^m$ as :

DEFINITION 3.3. Let $c(x)$ and $c'(x)$ be two elements of $(F_q[x]/(x^N - 1))^m$. Let us suppose that $c(x) = (c_0(x), c_1(x), \ldots, c_{m-1}(x))$ and $c'(x) = (c'_0(x), c'_1(x), \ldots, c'_{m-1}(x))$, where $c_i(x) = \sum_{j=0}^{N-1} c_{i,j} x^j$ and $c'_i(x) = \sum_{j=0}^{N-1} c'_{i,j} x^j$. Let (l, σ, a) be a permutation of $\mathcal{P}$.

The action of (l, σ, a) over $c(x)$ is defined by : $c'_{i,j} = c_{k,t}$, where $(k, t) = (l, \sigma, a)^{-1}(i, j)$, for $i = 0, 1, \ldots, m-1$ and $j \in Z/(N)$.

We call $c'(x)$ the permuted of $c(x)$.

Clearly, for a fixed permutation, the permuted of two different elements of $(F_q[x]/(x^N - 1))^m$ are different.

4. Invariant codes under the action of some groups of permutations

Let $\underline{\alpha} = \{\alpha_0, \alpha_1, \ldots, \alpha_{m-1}\}$ be a basis of F_{q^m} over F_q. Now, we consider the code C_1 equal to $[N, \{\beta\}]_{q^m}$, where β is a primitive element of F_{q^m}. Then the construction of the F_q-generator matrix of $\mathcal{D}_{\underline{\alpha}}(C_1)$ implies no condition on the basis $\underline{\alpha}$ because there is no subfield subcode (part 2.4). Moreover, a generator of C_1 is (see part 2.2):

$$\theta(z) \prod_{b \in C_q(\beta) \setminus C_{q^m}(\beta)} (z - b)$$

where $\theta(z)$ is the primitive idempotent of $[N, \mathcal{C}_q(\beta)]_q$. In the basis $\underline{\alpha}$, this polynomial may be expressed as :

$$\theta(z)(b_0(z)\alpha_0 + \ldots + b_{m-1}(z)\alpha_{m-1}),$$

where $b_i(z)$ is some polynomial over F_q $(i = 0, \ldots, m-1)$. Then the F_q-generator matrix of $\mathcal{D}_{\underline{\alpha}}(C_1)$ has the following form (proposition 2.2) :

$$\begin{bmatrix} \theta(x)b_0(x) & \theta(x)b_1(x) & \ldots & \theta(x)b_{m-1}(x) \\ x\theta(x)b_0(x) & x\theta(x)b_1(x) & \ldots & x\theta(x)b_{m-1}(x) \\ \ldots & \ldots & \ldots & \ldots \\ x^{m-1}\theta(x)b_0(x) & x^{m-1}\theta(x)b_1(x) & \ldots & x^{m-1}\theta(x)b_{m-1}(x) \end{bmatrix}.$$

Let us denote by $G_1^{\underline{\alpha}}(x)$ the first row of this matrix. As this matrix is entirely defined by its first row, then $G_1^{\underline{\alpha}}(x)$ may be considered as a generator of $\mathcal{D}_{\underline{\alpha}}(C_1)$. For this particular construction of the F_q-generator matrix of $\mathcal{D}_{\underline{\alpha}}(C_1)$ and for the fixed basis $\underline{\alpha}$, $G_1^{\underline{\alpha}}(x)$ is unique. Thus, for the end of this paper, $G_1^{\underline{\alpha}}(x)$ is called *the* generator of $\mathcal{D}_{\underline{\alpha}}(C_1)$.

In order to prove the different following propositions, we need to recall that the mapping ψ defined by :

$$(4.1) \qquad \begin{cases} F_{q^m} = F_q(\beta) & \longrightarrow \quad [N, \mathcal{C}_q(\beta)]_q \\ \sum_{i=0}^{m-1} e_i\beta^i & \longrightarrow \quad \theta(x)\sum_{i=0}^{m-1} e_i x^i \end{cases}$$

is an isomorphism of ring (see [**5**, chap. 8]).

PROPOSITION 4.1. *Let C_1 be equal to $[N, \{\beta\}]_{q^m}$, where β is a primitive element of F_{q^m}. Suppose that $G_1^{\underline{\alpha}}(x) = (\theta(x)b_0(x), \theta(x)b_1(x), \ldots, \theta(x)b_{m-1}(x))$. Then :*

1- $G_1^{\underline{\alpha}}(x)$ may be expressed as $(\theta(x)x^{u_0}, \theta(x)x^{u_1}, \ldots, \theta(x)x^{u_{m-1}})$.

2- $\mathcal{D}_{\underline{\alpha}}(C_1) = \{(\theta(x)x^{u_0+r}, \theta(x)x^{u_1+r}, \ldots, \theta(x)x^{u_{m-1}+r})$, for $r = 0, \ldots, q^m - 2\}$ $\cup\{(0, \ldots, 0)\}$.

PROOF. 1- Firstly, let us prove that $\theta(x)b_i(x) \neq 0$, for all $i = 0, \ldots, m-1$. If there exists some $\theta(x)b_{i_0}(x)$ equal to zero then all the codewords of C_1 have the form :

$$\sum_{j=0}^{N-1}\sum_{i=0}^{m-1} c_{i,j}\alpha_i z^j, \text{ with } c_{i_0,j} = 0, \forall j.$$

This is clearly impossible. Thus $\theta(x)b_i(x) \neq 0$, for all $i = 0, \ldots, m-1$.

Secondly, the nonzero β of C_1 is a primitive element of F_{q^m}, then $[N, \mathcal{C}_q(\beta)]_q$ is equal to $\{\theta(x)x^r, r = 0, \ldots, N-1\} \cup \{0\}$ (uses (4.1)). Thus all the $\theta(x)b_i(x)$ may be expressed as $\theta(x)x^{u_i}$.

2- Use the previous point and (4.1). □

Now, the expression of $G_1^{\underline{\alpha}}(x)$ leads us to define a group of permutations such that $\mathcal{D}_{\underline{\alpha}}(C_1)$ is invariant under the action of these permutations. All these permutations depend on the m-tuple $(u_0, \ldots, u_{m-1})$ defined by $G_1^{\underline{\alpha}}(x)$ (proposition 4.1), so they depend on the basis $\underline{\alpha}$ and on the code C_1.

DEFINITION 4.2. Let C_1 be equal to $[N, \{\beta\}]_{q^m}$, where β is a primitive element of F_{q^m}. Suppose that $G_1^{\underline{\alpha}}(x) = (\theta(x)x^{u_0}, \theta(x)x^{u_1}, \ldots, \theta(x)x^{u_{m-1}})$.

We define by $\mathcal{P}_1^{\underline{\alpha}}$ the group of permutations equal to $\mathcal{P}$ for which the m-tuple $(w_0, \ldots, w_{m-1})$ is equal to $(u_0, \ldots, u_{m-1})$.

PROPOSITION 4.3. *Let C_1 be equal to $[N, \{\beta\}]_{q^m}$, where β is a primitive element of F_{q^m}. Suppose that $G_1^{\underline{\alpha}}(x) = (\theta(x)x^{u_0}, \theta(x)x^{u_1}, \ldots, \theta(x)x^{u_{m-1}})$.*

Then $\mathcal{D}_{\underline{\alpha}}(C_1)$ is invariant under the action of each permutation of $\mathcal{P}_1{}^{\underline{\alpha}}$.

PROOF. In order to prove this proposition it is sufficient to show that the permuted of any codeword $(\theta(x)x^{r+u_0}, \ldots, \theta(x)x^{r+u_{m-1}})$ of $\mathcal{D}_{\underline{\alpha}}(C_1)$ is also a codeword of $\mathcal{D}_{\underline{\alpha}}(C_1)$. Let us express $\theta(x)$ as $\sum_{j=0}^{N-1} \theta_j x^j$. Then we have :

$$(\theta(x)x^{r+u_0}, \ldots, \theta(x)x^{r+u_{m-1}}) = (\sum_{j=0}^{N-1} \theta_{j-u_0-r}x^j, \ldots, \sum_{j=0}^{N-1} \theta_{j-u_{m-1}-r}x^j),$$

and using the definition 3.3 its permuted is equal to

$$(\sum_{j=0}^{N-1} \theta_{(j-a)q^{-l}-q^{-l}u_0-r}x^j, \ldots, \sum_{j=0}^{N-1} \theta_{(j-a)q^{-l}-q^{-l}u_{m-1}-r}x^j).$$

As $(\theta(x))^{q^l} = \theta(x)$ (it is because $\theta(x)$ is an idempotent), this element is also equal to $(\theta(x)x^{rq^l+a+u_0}, \ldots, \theta(x)x^{rq^l+a+u_{m-1}})$. □

Now, we prove that some other codes C (in $F_{q^m}[z]/(z^N - 1)$) are such that $\mathcal{D}_{\underline{\alpha}}(C)$ is also invariant under the action of any group $\mathcal{P}$ or under the action of the $\mathcal{P}_1{}^{\underline{\alpha}}$.

PROPOSITION 4.4. *Let C_0 be equal to $[N, V]_{q^m}$, where V is some union of full sets of conjugates with respect to F_q.*

Then $\mathcal{D}_{\underline{\alpha}}(C_0)$ is invariant under the action of all $\mathcal{P}$.

PROOF. Let us denote by C_0' the code $[N, V]_q$. The particular form of the F_q-generator matrix of $\mathcal{D}_{\underline{\alpha}}(C_0)$ (see part 2) implies that our code C_0 may be expressed as $\{(c_0(x), \ldots, c_{m-1}(x))$, for all $c_i(x)$ in $C_0'\}$.

The action of the permutations of $\mathcal{P}$ over $\mathcal{D}_{\underline{\alpha}}(C_0)$ may be analysed into two actions :

We have the permutations of the different polynomials $c_i(x)$ by the elements of S_m (the group of permutations of $\{0, 1, \ldots, m-1\}$). And $\mathcal{D}_{\underline{\alpha}}(C_0)$ is invariant under the action of these permutations.

We have some cyclic shifts and some exponentiations by q^l on the codewords of C_0'. And $\mathcal{D}_{\underline{\alpha}}(C_0)$ is also invariant under the action of these operations. □

PROPOSITION 4.5. *Let C be equal to $[N, \{\beta\} \cup V]_{q^m}$, where β is a primitive element of F_{q^m}, and V is some union of full sets of conjugates with respect to F_q. Let C_1 be equal to $[N, \{\beta\}]_{q^m}$, and suppose that $G_1^{\underline{\alpha}}(x) = (\theta(x)x^{u_0}, \theta(x)x^{u_1}, \ldots, \theta(x)x^{u_{m-1}})$.*

Then $\mathcal{D}_{\underline{\alpha}}(C)$ is invariant under the action of $\mathcal{P}_1{}^{\underline{\alpha}}$.

PROOF. Clearly, $C = C_0 \oplus C_1$, where $C_0 = [N, V]_{q^m}$. Propositions 4.3 and 4.4 prove this result. □

Another way to increase the number of codes which are invariant under the action of any group $\mathcal{P}$ is to consider the dual codes.

Let $\underline{\alpha}^\perp$ be the trace dual basis of $\underline{\alpha}$ and $C^\perp$ the dual code of C.

PROPOSITION 4.6. *Let C be a code in $F_{q^m}[z]/(z^N - 1)$ such that $\mathcal{D}_{\underline{\alpha}}(C)$ is invariant under the action of $\mathcal{P}$.*

Then $\mathcal{D}_{\underline{\alpha}^\perp}(C^\perp)$ is also invariant under the action of $\mathcal{P}$.

PROOF. Clearly $\mathcal{D}_{\underline{\alpha}}(C)^{\perp}$ is invariant under the action of $\mathcal{P}$. Moreover it is well known ([7, lemma 6]) that $\mathcal{D}_{\underline{\alpha}}(C)^{\perp} = \mathcal{D}_{\underline{\alpha}^{\perp}}(C^{\perp})$. Thus $\mathcal{D}_{\underline{\alpha}^{\perp}}(C^{\perp})$ is invariant under the action of $\mathcal{P}$. □

5. Consequences

A well known problem on the area of q-ary images of q^m-ary cyclic codes is to determine in what conditions the q-ary image is invariant under the action of the mapping which sends a codeword $(c_0(x), \ldots, c_{m-1}(x))$ onto the codeword $(xc_{m-1}(x), c_0(x), \ldots, c_{m-2}(x))$.

Clearly this mapping corresponds to the permutation :

$$\tau \; : \; \begin{cases} \{0,1,\ldots,m-1\} \times Z/(N) & \longrightarrow & \{0,1,\ldots,m-1\} \times Z/(N) \\ (i,j) & \longrightarrow & \begin{cases} (i+1,j) & \text{if} \quad i < m-1 \\ (0,j+1) & \text{else} \end{cases} \end{cases}$$

In order to prove some results on τ, let us give three lemmas. But before, let us first recall that if $\underline{\alpha}$ and $\underline{\gamma}$ are two bases of F_{q^m} over F_q, then we have $\mathcal{D}_{\underline{\alpha}}^{-1}(G_1^{\underline{\alpha}}(x)) = \mathcal{D}_{\underline{\gamma}}^{-1}(G_1^{\underline{\gamma}}(x))$, where $\mathcal{D}_{\underline{\alpha}}$ and $\mathcal{D}_{\underline{\gamma}}$ are defined in part 1.

LEMMA 5.1. *Let C_1 be equal to $[N, \{\beta\}]_m$, where β is a primitive element of F_{q^m}. Suppose that $G_1^{\underline{\alpha}}(x) = (\theta(x)x^{u_0}, \theta(x)x^{u_1}, \ldots, \theta(x)x^{u_{m-1}})$.*

Let us consider a m-tuple $(v_0, v_1, \ldots, v_{m-1})$. Then there exists a basis $\underline{\gamma}$ of F_{q^m} over F_q such that $G_1^{\underline{\gamma}}(x) = (\theta(x)x^{v_0}, \theta(x)x^{v_1}, \ldots, \theta(x)x^{v_{m-1}})$ if and only if $\{\beta^{v_0}, \ldots, \beta^{v_{m-1}}\}$ is a basis of F_{q^m} over F_q.

PROOF. In order to prove this lemma, let us give a preliminary result. Let $\underline{\alpha}$ and $\underline{\gamma}$ be two bases of F_{q^m} over F_q. Let P be the change of basis such that $\underline{\alpha}^t = P\underline{\gamma}^t$. Suppose that $G_1^{\underline{\alpha}}(x) = (\theta(x)x^{u_0}, \theta(x)x^{u_1}, \ldots, \theta(x)x^{u_{m-1}})$, and $G_1^{\underline{\gamma}}(x) = (\theta(x)x^{v_0}, \theta(x)x^{v_1}, \ldots, \theta(x)x^{v_{m-1}})$. By using the definition of $G_1^{\underline{\alpha}}(x)$ (and $G_1^{\underline{\gamma}}(x)$) given at the beginning of the part 4, it is clear that we have $G_1^{\underline{\gamma}}(x)^t = P^t G_1^{\underline{\alpha}}(x)^t$.

1- Suppose that there exists a basis $\underline{\gamma}$ of F_{q^m} over F_q such that $G_1^{\underline{\gamma}}(x) = (\theta(x)x^{v_0}, \theta(x)x^{v_1}, \ldots, \theta(x)x^{v_{m-1}})$. Suppose that $\underline{\gamma} = \{\gamma_0, \gamma_1, \ldots, \gamma_{m-1}\}$, and suppose that there exists some scalars a_i (not all equal to zero) such that $\sum_{i=0}^{m-1} a_i \beta^{v_i} = 0$. We take for example $a_0 \neq 0$. Then $\theta(x)\sum_{i=0}^{m-1} a_i x^{v_i} = 0$ (use (4.1)). Let us consider the basis $\underline{\delta}$ of F_{q^m} over F_q equal to $\{\gamma_0, \gamma_1 - \gamma_0 \frac{a_1}{a_0}, \ldots, \gamma_{m-1} - \gamma_0 \frac{a_{m-1}}{a_0}\}$. Then using the preliminary result, $G_1^{\underline{\delta}}(x) = (0, \theta(x)x^{v_1}, \ldots, \theta(x)x^{v_{m-1}})$ which is impossible (see the proof of proposition 4.1).

2- Now, suppose that $\{\beta^{v_0}, \beta^{v_1}, \ldots, \beta^{v_{m-1}}\}$ is a basis of F_{q^m} over F_q. Then $\{\theta(x)x^{v_0}, \theta(x)x^{v_1}, \ldots, \theta(x)x^{v_{m-1}}\}$ is a basis of $[N, \mathcal{C}_q(\beta)]_q$ (use (4.1)). On the other hand $\{\beta^{u_0}, \beta^{u_1}, \ldots, \beta^{u_{m-1}}\}$ is also a basis of F_{q^m} over F_q (point 1) and the same argument as above shows that $\{\theta(x)x^{u_0}, \theta(x)x^{u_1}, \ldots, \theta(x)x^{u_{m-1}}\}$ is also a basis of $[N, \mathcal{C}_q(\beta)]_q$. Then there exists an invertible matrix P' such that $(\theta(x)x^{v_0}, \theta(x)x^{v_1}, \ldots, \theta(x)x^{v_{m-1}})^t = P'(\theta(x)x^{u_0}, \theta(x)x^{u_1}, \ldots, \theta(x)x^{u_{m-1}})^t$. Now, let us consider the set $\underline{\gamma}$ such that $\underline{\alpha} = P'^t\underline{\gamma}^t$. Since the matrix P' is invertible, $\underline{\gamma}$ is also a basis of F_{q^m} over F_q and the preliminary result gives that $G_1^{\underline{\gamma}}(x) = (\theta(x)x^{v_0}, \theta(x)x^{v_1}, \ldots, \theta(x)x^{v_{m-1}})$. □

LEMMA 5.2. *Let C_1 be equal to $[N,\{\beta\}]_{q^m}$, where β is a primitive element of F_{q^m}. Suppose that $G_1^{\underline{\alpha}}(x) = (\theta(x)x^{u_0}, \theta(x)x^{u_1}, \dots, \theta(x)x^{u_{m-1}})$.*

Then for all integer t, there exists a basis $\underline{\gamma}$ of F_{q^m} over F_q such that $G_1^{\underline{\gamma}}(x) = (\theta(x)x^{u_0+t}, \dots, \theta(x)x^{u_{m-1}+t})$ and we have $\mathcal{D}_{\underline{\alpha}}(C_1) = \mathcal{D}_{\underline{\gamma}}(C_1)$.

PROOF. The lemma 5.1 proves that $\{\beta^{u_0}, \dots, \beta^{u_{m-1}}\}$ is a basis of F_{q^m} over F_q. Thus $\{\beta^{u_0+t}, \dots, \beta^{u_{m-1}+t}\}$ is also a basis of F_{q^m} over F_q. On the other hand it proves that there exists a basis $\underline{\gamma}$ of F_{q^m} over F_q such that $G_1^{\underline{\gamma}}(x) = (\theta(x)x^{u_0+t}, \dots, \theta(x)x^{u_{m-1}+t})$. The dimensions of $\mathcal{D}_{\underline{\alpha}}(C_1)$ and $\mathcal{D}_{\underline{\gamma}}(C_1)$ and the proposition 4.1 prove the last assertion. □

In proposition 4.3, we have proved that $\mathcal{D}_{\underline{\alpha}}(C_1)$ is invariant under the action of $\mathcal{P}_1^{\underline{\alpha}}$. The previous lemma proved that there exists other bases of F_{q^m} over F_q, called for example $\underline{\gamma}$, such that $\mathcal{D}_{\underline{\gamma}}(C_1)$ is also invariant under the action of $\mathcal{P}_1^{\underline{\alpha}}$.

LEMMA 5.3. *Let C_1 be equal to $[N,\{\beta\}]_{q^m}$, where β is a primitive element of F_{q^m}. Then for all integer t, there exists a basis $\underline{\gamma}$ such that $G_1^{\underline{\gamma}}(x) = (\theta(x)x^t, \theta(x)x^{-b+t}, \theta(x)x^{-2b+t}, \dots, \theta(x)x^{-(m-1)b+t})$, where b is invertible in $Z/(N)$.*

PROOF. Let us prove this lemma for $t = 0$. For $t \neq 0$, it is sufficient to apply the result of lemma 5.2.

Clearly $\{1, \beta^{-b}, \beta^{-2b}, \dots, \beta^{-(m-1)b}\}$ is a basis of F_{q^m} over F_q because β is a primitive element of F_{q^m} and b is invertible in $Z/(N)$. The lemma 5.1 gives the result. □

PROPOSITION 5.4. *Let C_1 be equal to $[N,\{\beta\}]_{q^m}$, where β is a primitive element of F_{q^m}.*

Then there exists a basis $\underline{\gamma}$ such that τ is in $\mathcal{P}_1^{\underline{\gamma}}$ if and only if $(N,m) = 1$.

When one of these two assertions is true, we have :

1- $G_1^{\underline{\gamma}}(x) = (\theta(x)x^{v_0}, \theta(x)x^{v_0-a}, \theta(x)x^{v_0-2a}, \dots, \theta(x)x^{v_0-(m-1)a})$, where a is the inverse of m in $Z/(N)$, and v_0 is some integer.

2- $\tau = (0, \sigma, a)$, where σ is the permutation of S_m defined by $\sigma(i) \equiv i+1$ modulo m and a is the inverse of m in $Z/(N)$.

PROOF. Suppose there exists a basis $\underline{\gamma}$ such that τ is in $\mathcal{P}_1^{\underline{\gamma}}$. Suppose that $G_1^{\underline{\gamma}}(x) = (\theta(x)x^{v_0}, \theta(x)x^{v_1}, \dots, \theta(x)x^{v_{m-1}})$. Then, for all j in $Z/(N)$, we have $(i+1, j) = (\sigma(i), jq^l + v_{\sigma(i)} - q^l v_i + a)$ if $i < m-1$, and $(0, j+1) = (\sigma(m-1), jq^l + v_{\sigma(m-1)} - q^l v_{m-1} + a)$ if $i = m-1$.

Then σ is the permutation of S_m defined by $\sigma(i) \equiv i+1$ modulo m, and for $j = 0$: $v_{i+1} - q^l v_i + a \equiv 0$ modulo N if $i < m-1$, and $v_0 - q^l v_{m-1} + a \equiv 1$ modulo N else.

Thus, for all j in $Z/(N)$, $q^l j \equiv j$ modulo N, and necessarily $l = 0$. Then we have : $v_{i+1} - v_i \equiv -a$ modulo N if $i < m-1$, and $v_0 - v_{m-1} \equiv 1 - a$ modulo N. Thus $1 - am \equiv 0$ modulo N, and $(N,m) = 1$.

Clearly, $\tau = (0, \sigma, a)$, where σ is the permutation of S_m defined by $\sigma(i) \equiv i+1$ modulo m and a is the inverse of m in $Z/(N)$. Moreover $v_i = v_0 - ia$, for all $i = 1, \dots, m-1$.

Conversely, suppose that $(N,m) = 1$. Let a be the inverse of m in $Z/(N)$. Then there exists a basis $\underline{\gamma}$ such that $G_1^{\underline{\gamma}}(x) = (\theta(x)x^{v_0}, \theta(x)x^{v_0-a}, \theta(x)x^{v_0-2a}, \dots, \theta(x)x^{v_0-(m-1)a})$, for some integer v_0 (lemma 5.3). Let us consider $\mathcal{P}_1^{\underline{\gamma}}$, and the

particular permutation $(0, \sigma, a)$, where σ is the permutation of S_m defined by $\sigma(i) \equiv i+1$ modulo m. Then this permutation is equal to τ, and it is in $\mathcal{P}_1^{\underline{\gamma}}$. □

COROLLARY 5.5. *Suppose that* $(N, m) = 1$. *Let* C_1 *be equal to* $[N, \{\beta\}]_{q^m}$, *where* β *is a primitive element of* F_{q^m}. *Let* C_0 *be equal to* $[N, V]_{q^m}$, *where* V *is some union of full sets of conjugates with respect to* F_q. *And let* C *be equal to* $C_0 \oplus C_1$.

Then there exists a basis $\underline{\gamma}$ *such that* $\mathcal{D}_{\underline{\gamma}}(C_1)$, $\mathcal{D}_{\underline{\gamma}}(C_0)$, *and* $\mathcal{D}_{\underline{\gamma}}(C)$ *are invariant under the action of* τ.

In the basis $\underline{\gamma}^{\perp}$, *their dual codes are invariant under the action of* τ.

PROOF. Use propositions 5.4, 4.3, 4.4, 4.5, and 4.6. □

This result is another proof of a part of the results given in [**7**].

In this paper G. E. Seguin presents an open problem which is "When does a q^m-ary cyclic code have a q-ary image which is equivalent to a cyclic code ?". Now, we give a part of the answer of this problem.

PROPOSITION 5.6. *Let* C *be a code in* $F_{q^m}[z]/(z^N - 1)$. *Suppose that there exists a* $\mathcal{P}$ *such that* $\mathcal{D}_{\underline{\alpha}}(C)$ *is invariant under its action. Then*

1- $\mathcal{D}_{\underline{\alpha}}(C)$ *is equivalent to a 2-D abelian code.*

2- if $(m, N) = 1$, *then* $\mathcal{D}_{\underline{\alpha}}(C)$ *is equivalent to a cyclic code.*

PROOF. 1- A set of matrices is a 2-D abelian code if it is a vector space invariant under the action of the shift of the rows and the columns. If it is possible to define a permutation P which sends the set of codewords of $\mathcal{D}_{\underline{\alpha}}(C)$ onto a set of $m \times N$-matrices which verifies the previous property then $\mathcal{D}_{\underline{\alpha}}(C)$ will be equivalent to a 2-D abelian code.

Let P be the permutation of $\{0, 1, \ldots, m-1\} \times Z/(N)$ which sends (i, j) onto $(i, w_0 - w_i + j)$ where $(w_0, w_1, \ldots, w_{m-1})$ is defined by $\mathcal{P}$ (see def. 3.1). Let $c(x)$ be an element of $\mathcal{D}_{\underline{\alpha}}(C)$ and suppose that $c(x) = (c_0(x), c_1(x), \ldots, c_{m-1}(x))$, where $c_i(x) = \sum_{j=0}^{N-1} c_{i,j} x^j$. Let $c'(x)$ be equal to $(c'_0(x), c'_1(x), \ldots, c'_{m-1}(x))$, where $c'_i(x) = \sum_{j=0}^{N-1} c'_{i,j} x^j$. The action of P over $c(x)$ is defined by : $c'_{i,j} = c_{k,t}$, where $(k, t) = P^{-1}(i, j)$ for $i = 0, 1, \ldots, m-1$, and $j \in Z/(N)$. We call $c'(x)$ the permuted of $c(x)$. Let us denote by $P(\mathcal{D}_{\underline{\alpha}}(C))$ the set of all permuted of $\mathcal{D}_{\underline{\alpha}}(C)$.

Now, let p be a permutation of $\mathcal{P}$. Since $\mathcal{D}_{\underline{\alpha}}(C)$ is invariant under the action of p, then $P(\mathcal{D}_{\underline{\alpha}}(C))$ is invariant under the action of $P \circ p \circ P^{-1}$.

Let σ be the permutation of S_m defined by $\sigma(i) \equiv i+1$ modulo m. Let us consider the action of $P \circ (0, \sigma, 0) \circ P^{-1}$ over $P(\mathcal{D}_{\underline{\alpha}}(C))$. Clearly we have : $P \circ (0, \sigma, 0) \circ P^{-1}(i, j) = (i+1, j)$. Thus this permutation acts on $P(\mathcal{D}_{\underline{\alpha}}(C))$ as the shift of each column and $P(\mathcal{D}_{\underline{\alpha}}(C))$ is invariant under the action of this permutation.

Finaly, let us consider the action of $P \circ (0, Id, 1) \circ P^{-1}$ over $P(\mathcal{D}_{\underline{\alpha}}(C))$. Then we have : $P \circ (0, Id, 1) \circ P^{-1}(i, j) = (i, j+1)$. So this permutation acts on $P(\mathcal{D}_{\underline{\alpha}}(C))$ as the shift of each row and $P(\mathcal{D}_{\underline{\alpha}}(C))$ is invariant under the action of this permutation. This proves the first point.

2- It is well known that a 2-D abelian code of length $n_1 \times n_2$ is equivalent to a cyclic code if $(n_1, n_2) = 1$, ([**6**, chap. 5]). □

References

[1] T. P. Berger and P. Charpin *The Permutation Group of Affine-Invariant Extended Cyclic Codes*, IEEE Trans. on Inform. Theory, vol. 42, no. 6, pp. 2194-2209, Nov. 1996.

[2] P. Delsarte *On Cyclic Codes that are Invariant under the General Linear Group*, IEEE Trans. on Inform. Theory, vol. IT-16, no. 6, pp. 760-769, Nov. 1970.

[3] T. Kasami, S. Lin abd W. W. Peterson *Polynomial Codes*, IEEE Trans. on Inform. Theory, vol. 14, no. 6, pp. 807-814, Nov. 1968.

[4] R.Lidl, H.Niederreiter *Finite Fields*, Reading, MA: Addison-Wesley, 1983.

[5] F.J.Mac Williams, N.J.A.Sloane *The Theory of Error-Correcting Codes*, North-Holland (1983, second reprint).

[6] A.Poli, Ll.Huguet 92 *Error Correcting Codes: theory and applications*, Prentice Hall, 1992.

[7] G. E. Seguin *The q-ary Image of q^m-ary Cyclic Code*, IEEE Trans. on Inform. Theory, vol.41, no. 2, pp. 387-399, March 1995.

[8] L. Tang, C. Boon Soh, and E. Gunawan *A Note on the q-ary Image of a q^m-ary Repeated-Root Cyclic Code*, IEEE Trans. on Inform. Theory, vol.43, no. 2, pp. 732-737, March 1997.

[9] A. Vardy and Y. Be'ery *Bit-Level Soft-Decision Decoding of Reed-Solomon Codes* IEEE Trans. on Inform. Theory, vol.39, no. 3, pp. 440-444, March 1991.

LABORATOIRE AAECC-IRIT, UNIVERSITY PAUL SABATIER, 118, ROUTE DE NARBONNE, 31062 TOULOUSE CEDEX, FRANCE AND LABORATOIRE GRID, IUT BELFORT-MONTBELIARD, BP 527, 90016 BELFORT, FRANCE

E-mail address: Jerome.Lacan@iut-bm.univ-fcomte.fr

LABORATOIRE AAECC-IRIT, UNIVERSITY PAUL SABATIER, 118, ROUTE DE NARBONNE, 31062 TOULOUSE CEDEX, FRANCE

E-mail address: delp@cict.fr

Contemporary Mathematics
Volume **225**, 1999

THE NUMBER OF SOLUTIONS TO A SYSTEM OF EQUATIONS AND SPECTRA OF CODES

OSNAT KEREN AND SIMON LITSYN

ABSTRACT. Consider a system of equations over a finite field of characteristic two corresponding to a parity check matrix of an extended BCH code. The number of solutions to this system with distinct values of the variables equals to the first component of the code's spectrum. We present a new bound on the error term of the binomial approximation to this number which is better than a bound from the Lang-Weil theorem due to Vladuts and Skorobogatov.

1. Introduction

Consider the following system of equations over the field $\mathbf{F}_{2^m}$:

$$\begin{cases} x_1^0 & +\cdots+ & x_i^0 & = & 0 \\ x_1^1 & +\ldots+ & x_i^1 & = & 0 \\ x_1^3 & +\ldots+ & x_i^3 & = & 0 \\ \vdots & & & \vdots & \vdots \\ x_1^{2t-1} & +\ldots+ & x_i^{2t-1} & = & 0 \end{cases} \tag{1.1}$$

Assume some order on the $q = 2^m$ elements of the field. We are interested in the number of solutions $(x_1, \ldots, x_i) \in (\mathbf{F}_{2^m})^i$, with $0 \leq x_1 < x_2 < \ldots < x_i$. This problem has an application in coding theory. Namely, every such solution corresponds to a codeword of weight i in an extended BCH code. So, the sought number is just the value of the i-th component of the weight (or distance) distribution of such code. Let B_i stand for the number of such solutions. Set $B_0 = 1$. Clearly, $B_i = 0$ for $i = 1, \ldots, 2t$, and for odd i's.

The standard approach to estimating the number of solutions to the system is based on use of the exponential sums method [3, 5] or the Lang-Weil estimates [6]. However, in this method the total number of solutions is estimated rather than the number of solutions with distinct values.

It is known (see, for example [4, §9.10]) that

$$B_i = \frac{\binom{2^m}{i}}{2^{mt}}(1 + E_i),$$

and for given i, E_i decreases with m. Moreover, the maximal (in i) E_i is of order 2^{-m} and occurs for $i = 2t + 2$. Therefore, we concentrate on improving known estimates for B_{2t+2}.

The best known estimates for E_i are due to Vladuts and Skorobogatov [6]:

$$E_V = \frac{(eq)^{2t+1}}{\binom{q}{2t+2}}. \tag{1.2}$$

1991 *Mathematics Subject Classification.* 11T71.

© 1999 American Mathematical Society

Here we suggest an alternative approach, which, along with an analysis of properties of Krawtchouk polynomials, allows us improving on (1.2).

2. Exponential sums and the MacWilliams transform

In this section we survey the coding theory background to the problem, and give a simple proof of the MacWilliams identities using exponential sums.

Let $\{y_1, \dots, y_q\}$ be the set of the field elements in the increasing order. The index vector of an ordered subset of i elements, $0 \le x_1 < x_2 < \cdots < x_i$, defines a binary vector v of weight i. All in all, there are $\binom{q}{i}$ such vectors, only B_i of them being solutions to the system.

Choose $\beta \in \mathbf{F}_{2^m}$ such that $Tr(\beta) = 1$. Define a set of polynomials, $f_{\underline{\alpha}}$, of degree $2t-1$,

$$f_{\underline{\alpha}} = \{\alpha_0 + \alpha_1 x + \alpha_2 x^3 + \cdots + \alpha_t x^{2t-1} | \alpha_i \in \mathbf{F}_{2^m}, \alpha_0 \in \{0, \beta\}\},$$

$|f_{\underline{\alpha}}| = 2q^t$. Let $f \in f_{\underline{\alpha}}$. Denote by u_f the trace vector of $f(y)$, i.e. $u_f = Tr(f(y)) = (Tr(f(y_1)), Tr(f(y_2)), \dots, Tr(f(y_q)))$, and let $wt(u_f)$ stand for the Hamming weight of u_f. Let $\Psi(x) = (-1)^{Tr(x)}$ be an additive character.

Lemma 1. *For $f \neq 0$,*

$$q/2 - (t-1)\sqrt{q} \le wt(u_f) \le q/2 + (t-1)\sqrt{q}.$$

Proof Let u_0 and u_1 stand for the number of zeroes and ones in u_f. Clearly $u_1 = wt(u_f)$ and $u_0 + u_1 = q$. The statement follows directly from the Weil inequality,

$$|\sum_{x \in F} \Psi(f(x))| = |u_0 - u_1| \le (\deg f - 1)\sqrt{q}.$$

□

Let B'_j stand for the number of polynomials f having $wt(u_f) = j$. Clearly $B'_0 = 1$ and

$$\sum_{j=0}^{q} B'_j = 2q^t.$$

By the lemma, $B'_j = 0$ for $1 \le j < q/2 - (t-1)\sqrt{q}$. Let d'_t stand for the minimal $j > 0$ such that $B'_j > 0$. Clearly

$$d'_t \ge q/2 - (t-1)\sqrt{q}.$$

There is a relation between B_i's and B'_j's. It employs Krawtchouk polynomials, $P_i^{(n)}(x)$, of degree i,

$$P_i(x) = P_i^{(n)}(x) = \sum_{k=0}^{i} (-1)^k \binom{x}{k} \binom{n-x}{i-k}.$$

The properties of Krawtchouk polynomials are described for example in [1, §2.3].

Lemma 2. *(MacWilliams transform)*

$$2q^t B_i = \sum_{j=0}^{q} B'_j P_i^q(j) \tag{2.3}$$

Proof Although there exist several proofs to (2.3), we give here another one for the sake of demonstrating how the exponential sums method can be used in this context. Consider the following sum

$$\begin{aligned} S = S(x_1, x_2, \ldots, x_i) \quad = \quad & \sum_{\alpha_0 \in \{0,\beta\}} \Psi(\alpha_0(x_1^0 + x_2^0 + \cdots + x_i^0)) \cdot \\ & \sum_{\alpha_1 \in \mathbf{F}_{2^m}} \Psi(\alpha_1(x_1 + x_2 + \cdots + x_i)) \cdot \\ & \sum_{\alpha_2 \in \mathbf{F}_{2^m}} \Psi(\alpha_2(x_1^3 + x_2^3 + \cdots + x_i^3)) \cdot \\ & \cdots \\ & \sum_{\alpha_t \in \mathbf{F}_{2^m}} \Psi(\alpha_t(x_1^{2t-1} + x_2^{2t-1} + \cdots + x_i^{2t-1})). \end{aligned}$$

Whenever i is even and $(x_1, x_2, \ldots x_i)$ is a solution to the system, $S = 2q^t$, otherwise it is 0. Therefore,

$$\sum_{0 \le x_1 < x_2 < \cdots < x_i} S(x_1, x_2 \ldots x_i) = 2q^t B_i.$$

By changing the order of summation we get

$$\begin{aligned} 2q^t B_i \quad &= \quad \sum_{f \in f_{\underline{\alpha}}} \sum_{0 \le x_1 < x_2 < \cdots < x_i} \Psi(f(x_1) + f(x_2) + \cdots + f(x_i)) \\ &= \quad \sum_{u_f, f \in f_{\underline{\alpha}}} \sum_{v, wt(v) = i} (-1)^{<u_f, v>}. \end{aligned}$$

Let $j = wt(u_f)$. The inner sum depends only on j,

$$\sum_{v, wt(v)=i} (-1)^{<u_f, v>} = \sum_{k=0}^{i} (-1)^k \binom{j}{k} \binom{q-j}{i-k} = P_i^{(q)}(j).$$

Since there are B'_j vectors u_f of weight $j = 0, 1, \ldots, q$, we have

$$2q^t B_i = \sum_{j=0}^{q} B'_j P_i^{(q)}(j).$$

□

Notice, that given B_i one can easily compute the number of solutions to the system

$$\begin{cases} z_1 & + \ldots + & z_i & = & 0 \\ z_1^3 & + \ldots + & z_i^3 & = & 0 \\ \vdots & & & \vdots & \vdots \\ z_1^{2t-1} & + \ldots + & z_i^{2t-1} & = & 0 \end{cases} \tag{2.4}$$

Here we consider the solutions over $\mathbf{F}^*_{2^m}$ satisfying $0 < z_1 < z_2 < \cdots < z_i$. Let b_i stand for the number of solutions to this system. Clearly, $B_{2m} = b_{2m-1} + b_{2m}$. Moreover,

Lemma 3.

$$b_{2m} = \frac{(n-2m)B_{2m}}{n}, \qquad b_{2m-1} = \frac{2mB_{2m}}{n}.$$

Proof If $z = (z_1, z_2, \ldots, z_{2m})$ is a solution to (1.1) then $\gamma z + \beta$, $\beta, \gamma \in \mathbf{F}_{2^m}$, is also a solution. Indeed, for $r = 1, 3, \ldots 2t-1$,

$$\begin{aligned}\sum_{i=1}^{2m}(\gamma z_i + \beta)^r &= \sum_{i=1}^{2m}\sum_{l=0}^{r}\binom{r}{l}\gamma^l\beta^{r-l}z_i^l \\ &= \sum_{l=0}^{r}\gamma^l\beta^{r-l}\sum_{i=1}^{2m}z_i^l \\ &= 2m\beta^r = 0. \qquad (2.5)\end{aligned}$$

This yields that the number of solutions containing a particular y_i does not depend on i, i.e. there are exactly $2mB_{2m}/q$ such solutions. Moreover b_{2m-1} is the number of z's with $z_1 = 0$, and

$$b_{2m-1} = B_{2m} - \frac{2mB_{2m}}{q} = \frac{(q-2m)B_{2m}}{q}.$$

□

3. Estimates for the number of solutions

In this section we estimate the number of solutions to system (1.1) for $i = 2t+2$. Let $h(x) = \sum_{i=0}^{q} h_i P_i(x)$, where $h_i = (1/2^q)\sum_{j=0}^{q} h(j)P_j(i)$, be a polynomial. The Krawtchouk polynomials constitute an orthogonal basis,

$$\sum_{i=0}^{q} P_k(i)P_i(l) = 2^q\delta_{k,l},$$

therefore the following relation holds

$$\sum_{i=0}^{q} B_i h_i = (1/2q^t)(1/2^q)\sum_{k=0}^{q}\sum_{j=0}^{q} B'_j h(k)\sum_{i=0}^{q} P_i(j)P_k(i) = (1/2q^t)\sum_{i=0}^{q} B'_i h(i).$$

The number of solutions can be estimated by choosing different h's.

Lemma 4. *Let $f(x) = \sum_{i=0}^{2t+2} f_i P_i(x)$ and $g(x) = \sum_{i=0}^{2t+2} g_i P_i(x)$ be functions even with respect to $q/2$, such that $f_{2t+2}, g_{2t+2} > 0$ and*

$$\begin{aligned} f(x) &\geq 0 \quad , \quad \forall x \\ g(x) &\leq 0 \quad , \quad d'_t \leq x \leq n - d'_t \end{aligned}$$

Then,

$$B_{2t+2} \geq \frac{\frac{f(0)}{q^t} - f_0}{f_{2t+2}},$$

$$B_{2t+2} \leq \frac{\frac{g(0)}{q^t} - g_0}{g_{2t+2}}.$$

Proof First notice that

$$\sum_{i=0}^{q} P_k(i)B_i = \frac{1}{2q^t}\sum_{j=0}^{q} B'_j\sum_{i=0}^{q} P_k(i)P_i(j) = \frac{2^q}{2q^t}B'_k,$$

and therefore $B'_k = B'_{n-k}$ since for the even values of i, $P_k(i) = P_{n-k}(i)$. Substituting $f(x)$ and $g(x)$ into (3) yields

$$f_0B_0 + f_{2t+2}B_{2t+2} = \frac{f(0)B'_0}{q^t} + (1/q^t)\sum_{i=d'}^{q/2} B'_i f(i) \geq \frac{f(0)}{q^t},$$

$$g_0B_0 + g_{2t+2}B_{2t+2} = \frac{g(0)B'_0}{q^t} + (1/q^t)\sum_{i=0}^{q/2} g(i)B'_i \leq \frac{g(0)}{q^t}.$$

□

In particular for **odd** t we choose $f(x) = (\sum_{i=0,i\,even}^{t+1} u_i P_i(x))^2$ and get the following lower bound on B_{2t+2}.

Theorem 5. *(Lower bound for odd t)*

$$B_{2t+2} \geq \frac{\binom{q}{t+1}^2}{\binom{2t+2}{t+1}q^t}\left(1 + \frac{V_{q-1}^{t-1}}{q^t - V_{q-1}^{t-1}}\right)(1 - \underline{E}), \tag{3.6}$$

where $V_q^k = \sum_{i=0}^{k}\binom{q}{k}$ *and the error term* $\underline{E} = \frac{q^t - V_{q-1}^{t-1}}{\binom{q}{t+1}}$.

Proof Let $f(x) = (\sum_{i=0,i\,even}^{t+1} u_i P_i(x))^2$, clearly $deg(f(x)) = 2t+2$ and $f(x) \geq 0$. Indeed,

$$f(0) = \left(\sum_{i=0,i even}^{t+1} u_i \binom{q}{i}\right)^2$$

$$f_0 = (1/2^q)\sum_{x=0}^{q} f(x)P_x(0) = (1/2^q)\sum_{i,j,even} u_i u_j \sum_{x=0}^{q}\binom{q}{x}P_i(x)P_j(x)$$

$$= \sum_{i,j} u_i u_j \delta_{ij}\binom{q}{i} = \sum_{i=0,i even}^{t+1} u_i^2\binom{q}{i},$$

and f_{2t+2} is the coefficient of $P_{2t+2}(x)$, which results from the multiplication of u_{t+1}^2 by $P_{t+1}^2(x)$, i.e.

$$P_{t+1}^2 = \sum_{k=0}^{t+1}\binom{2(t+1-k)}{t+1-k}\binom{q-2(t+1-k)}{k}P_{2(t+1-k)}(x),$$

and therefore,

$$f_{2t+2} = u_{t+1}^2\binom{2t+2}{t+1}.$$

Without loss of generality let $u_{t+1} = 1$. It is simple to see that the optimal u_i's which maximize the bound satisfy $u_i = u$ for $i = 0 \ldots t-1$, namely

$$u = \frac{\binom{q}{t+1}}{q^t - \sum_{i=0,i\,even}^{t-1}\binom{q}{i}}$$

Finally, after substituting the value of u we get

$$\begin{aligned} B_{2t+2} &\geq \frac{\binom{q}{t+1}^2}{\binom{2t+2}{t+1}q^t}\left(1+\frac{\sum_{i=0,i\,even}^{t-1}\binom{q}{i}}{q^t-\sum_{i=0,i\,even}^{t-1}\binom{q}{i}}\right)(1-\underline{E}) \\ &= \frac{\binom{q}{t+1}^2}{\binom{2t+2}{t+1}q^t}\left(1+\frac{V_{q-1}^{t-1}}{q^t-V_{q-1}^{t-1}}\right)(1-\underline{E}), \end{aligned}$$

where $V_q^k=\sum_{i=0}^{k}\binom{q}{k}$ and the error term $\underline{E}=\frac{q^t-V_{q-1}^{t-1}}{\binom{q}{t+1}}$. □

Notice that if $t<\sqrt{q}$ then,

$$\underline{E}\leq\frac{q^t}{\binom{q}{t+1}}<\frac{2(t+1)!}{q}.$$

The main term of equation the estimate can be written as

$$\begin{aligned} \frac{\binom{q}{t+1}^2}{\binom{t+2}{t+1}q^t} &= \frac{\binom{q}{2t+2}}{q^t}\left(\frac{q\cdot(q-1)\cdots(q-t)}{(q-(t+1))\cdot(q-(t+2))\cdots(q-(2t+1))}\right) \\ &\geq \frac{\binom{q}{2t+2}}{q^t}\left(1+\frac{t+1}{q-(t+1)}\right)^{t+1} \\ &\geq_{t<\sqrt{q}} \frac{\binom{q}{2t+2}}{q^t}\left(1+\frac{(t+1)^2}{q}\right), \end{aligned}$$

hence,

$$B_{2t+2}\geq\frac{\binom{q}{2t+2}}{q^t}\left(1+\frac{t+1}{q-(2t+1)}\right)^{t+1}\left(1+\frac{V_{q-1}^{t-1}}{q^t-V_{q-1}^{t-1}}\right)(1-\underline{E}).$$

For q large enough $B_{2t+2}\approx\frac{\binom{q}{2t+2}}{q^t}$. For comparison, the estimate (1.2) on the error term is

$$E_V=\frac{e^{2t+1}q^{2t+1}}{\binom{q}{2t+2}}>e^{2t+1}(2t+2)!/q>(2e)^{2t}t!\underline{E}.$$

Theorem 5 gives a lower bound for odd values of t. The next theorem provides a lower bound which is slightly weaker but applies for any t.

Theorem 6. *(Lower bound)*

$$B_{2t+2}\geq\frac{\binom{q}{t+1}^2}{\binom{2t+2}{t+1}q^t}\left(1-\frac{q^t}{\binom{q}{t+1}}\right).$$

Proof Let $f(x)=\sum_{i=0}^{t+1}u_iP_i^2(x)$. Clearly $f(x)$ is an even function of degree $2t+2$. For $u_i\geq 0, i=0\ldots t+1$ the function takes on nonnegative values. Moreover, for $u_{t+1}=1$ we get

$$\begin{aligned} f(0) &= \binom{q}{t+1}^2+\sum_{i=0}^{t}u_i\binom{q}{i}^2, \\ f_0 &= \binom{q}{t+1}+\sum_{i=0}^{t}u_i\binom{q}{i}, \\ f_{2t+2} &= \binom{2t+2}{t+1}. \end{aligned}$$

After substituting $f(0), f_0$ and f_{2t+2} into (4) we get

$$B_{2t+2} \geq \frac{\binom{q}{t+1}\left(\frac{\binom{q}{t+1}}{q^t} - 1\right)}{\binom{2t+2}{t+1}} + \frac{\sum_{i=0}^{t} u_i \binom{q}{i}\left(\frac{\binom{q}{i}}{q^t} - 1\right)}{\binom{2t+2}{t+1}}.$$

Clearly $\frac{\binom{q}{i}}{q^t} < 1$ and therefore we maximize the bound by setting $u_i = 0$ for $i = 0 \ldots t$, i.e.

$$B_{2t+2} \geq \frac{\binom{q}{t+1}^2}{\binom{2t+2}{t+1} q^t}\left(1 - \frac{q^t}{\binom{q}{t+1}}\right).$$

As before, this bound improves previous results. □

Theorem 7. *(Upper bound)*

$$B_{2t+2} \leq \frac{\binom{q}{t}^2 q^2}{q^t \binom{2t+2}{t+1}(t+1)^2}(1 + \overline{E}),$$

where the error term $\overline{E} \leq \frac{4(t-1)^2 t! e}{q}$.

Proof Let $g(x) = (P_2(x) + C)P_t^2(x)$, where $C = -P_2(d_t'')$ and $d_t'' = q/2 - (t-1)\sqrt{q} \leq d_t'$. The function $g(x)$ satisfies the restrictions of Lemma 4 since it is a product of two polynomials, a nonnegative polynomial of degree $2t$ and a quadratic function having roots at d_t'' and $q - d_t''$. Moreover,

$$\begin{aligned} g(0) &= \left(\binom{q}{2} + C\right)\binom{q}{t}^2, \\ g_0 &= \binom{q}{t}(C + t(q-t)), \\ g_{2t+2} &= \binom{2t+2}{t+1}\frac{(t+1)^2}{2}. \end{aligned}$$

By Lemma 4

$$\begin{aligned} B_{2t+2} &\leq \frac{\binom{q}{t}\left(\left(\binom{q}{2} + C\right)\binom{q}{t} - q^t(C + t(q-t))\right)}{q^t\binom{2t+2}{t+1}(t+1)^2} \\ &= \frac{\binom{q}{t}^2 q^2}{q^t\binom{2t+2}{t+1}(t+1)^2}(1 + \overline{E}), \end{aligned} \tag{3.7}$$

where

$$\begin{aligned} \overline{E} &= -\frac{4}{q}(t-1)^2 - \frac{2q^t\left((q/2)(1 - 4(t-1)^2) + t(q-t)\right)}{\binom{q}{t}q^2} \\ &\leq \frac{4(t-1)^2}{q}\left(\frac{q^t}{\binom{q}{t}} - 1\right) \\ &\leq \frac{4(t-1)^2 t! e}{q}. \end{aligned}$$

□

Asymptotically this upper bound converges to the binomial weight distribution. Indeed, the main term of (3.7) is

$$\begin{aligned}
\frac{\binom{q}{t}^2 q^2}{q^t \binom{2t+2}{t+1}(t+1)^2} &= \frac{(q\cdot(q-1)\cdots(q-t+1))^2 q^2 (t+1)!^2}{q^t t!^2 (2t+2)!(t+1)^2} \\
&\leq \frac{\binom{q}{2t+2}}{q^t}\left(1+\frac{t+2}{q-(2t+1)}\right)^{t+2} \\
&<_{t<\sqrt{q}} \frac{\binom{q}{2t+2}}{q^t}\left(1+\frac{(t+2)^2}{q-(t+2)^2-(2t+1)}\right).
\end{aligned}$$

Again, the upper bound is smaller than the one of [2, 6].

References

[1] G.Cohen, I.Honkala, S.Litsyn, A.Lobstein, *Covering Codes*, Elsevier, 1997.

[2] I.Krasikov and S. Litsyn, On spectra of BCH codes, *IEEE Trans. Inform. Theory*, vol 41, pp. 786-788, 1995.

[3] T. Helleseth, On the covering radius of cyclic linear codes and arithmetic codes, *Discrete Applied Mathematics*, vol. 11, pp. 157–173, 1985.

[4] F.J.MacWilliams and N.J.A.Sloane, *The Theory of Error-Correcting Codes*, North-Holland, 1977.

[5] A. Tietäväinen, On the covering radius of long binary BCH codes, *Discrete Applied Mathematics*, vol. 16, pp. 75–77, 1987.

[6] S. Vladuts and A. Skorobogatov, On spectra of binary cyclic codes, *Proceedings of the 9th All-Union Conference on Coding Theory and Information Transmission*, Odessa, pp.72–74, 1988 (in Russian)

Department of Electrical Engineering-Systems, Tel Aviv University 69978 Tel Aviv, Israel

E-mail address: osnatk@eng.tau.ac.il and litsyn@eng.tau.ac.il

Contemporary Mathematics
Volume **225**, 1999

The LD Probable Prime Test

Willi More

ABSTRACT. Modern applications of finite fields (e.g. public-key cryptography) need an algorithm to test whether a given large odd positive integer n is a prime number or not. In [**BaWa80**] Baillie & Wagstaff proposed to combine two probable prime tests for testing primality. Their suggestion was to check the integer if it is a strong pseudoprime to base 2 and a strong Lucas pseudoprime with parameters P and Q chosen properly. In [**Mo97**] it was shown how to avoid the parameter search for P and Q needed by Baillie & Wagstaff in 7 out of 8 cases of n mod 24. The result was called LD (Lucas discriminant) probable prime test and has been implemented in MapleV code. In this paper we will show that there is strong evidence that testing for Dickson pseudoprime (cf. [**MuOs93**]) instead of strong Lucas pseudoprime is not sufficient. If the proposed combination is sufficient or not is still an open problem.

Introduction

If an odd integer n satisfies Fermat's Little Theorem then n is called probable prime in base a (prp(a)), i.e. $\gcd(n,a) = 1$ and $a^{n-1} \equiv 1 \bmod n$. A pseudoprime (psp(a)) is a composite probable prime. There are infinitely many pseudoprimes for every base a. An odd integer n which is a pseudoprime for all non trivial bases is called Carmichael number. There exist infinitely many Carmichael numbers. Thus a probable prime test using prp(a) for different bases a simultaneously is not sufficient.

An odd integer n is called Euler probable prime in base a (eprp(a)) if $a^{\frac{n-1}{2}} \equiv (a/n) \bmod n$ and $\gcd(n,a) = 1$. An Euler pseudoprime in base a (epsp(a)) is a composite Euler probable prime. It is easy to see that every epsp(a) is a psp(a). There are infinitely many Euler pseudoprimes for every base a. An odd composite number n cannot be an Euler pseudoprime to all bases. It is an Euler pseudoprime simultaneously to no more than $\frac{1}{2}\phi(n)$ non trivial bases. An algorithm testing n to be eprp(a) for randomly chosen bases a was proposed in 1977 by Solovay & Strassen. This is a probabilistic test with probability $\leq 1/2$ to indicate a composite number as prime.

Let n be an odd integer, let $n - 1 = 2^s d$, with d odd and $s \geq 1$. Let a be an integer with $\gcd(n,a) = 1$ so n is called strong probable prime in base a (sprp(a)) if $a^d \equiv 1 \bmod n$, or $a^{2^r d} \equiv -1 \bmod n$ for some $r, 0 \leq r < s$. A strong pseudoprime

---

1991 *Mathematics Subject Classification.* Primary 11Y11, 11B39; Secondary 11A51, 11B50.

© 1999 American Mathematical Society

(spsp(a)) is a composite sprp(a). There exist infinitely many strong pseudoprimes for every base a. An odd composite number n cannot be a strong pseudoprime to all bases. It is a strong pseudoprime simultaneously to no more than $\frac{1}{4}(n-1)$ non trivial (i.e. $a \neq \pm 1$) bases. An algorithm testing n to be sprp(a) for randomly chosen bases a was proposed in 1976 by Miller & Rabin. This is a probabilistic test with probability $\leq 1/4$ to indicate an composite number as prime.

Let P, Q be integers. The polynomial $z^2 - Pz + Q$ with its discriminant $D = P^2 - 4Q$ has the two roots $\alpha = \frac{P+\sqrt{D}}{2}$ and $\beta = \frac{P-\sqrt{D}}{2}$. It is obvious that $\alpha+\beta = P$, $\alpha\beta = Q$ and $\alpha - \beta = \sqrt{D}$.

Let $D \neq 0$. Then the integer sequences

$$U_n(P,Q) = \frac{\alpha^n - \beta^n}{\alpha - \beta} \text{ and } V_n(P,Q) = \alpha^n + \beta^n, \text{ for } n \geq 0$$

are called Lucas sequences with parameters P, Q. An exhaustive listing of their algebraic properties and a lot of recent and historic remarks are given by Ribenboim [**Rib96**]. In particular, $U_0(P,Q) = 0, U_1(P,Q) = 1$ while $V_0(P,Q) = 2, V_1(P,Q) = P$. For $n \geq 2$ the linear recurrences of second order $U_n(P,Q) = PU_{n-1}(P,Q) - QU_{n-2}(P,Q)$ and $V_n(P,Q) = PV_{n-1}(P,Q) - QV_{n-2}(P,Q)$ give us a glimpse at the structure of the Lucas sequences. To simplify the notations we write $U_n = U_n(P,Q)$ and $V_n = V_n(P,Q)$.

Lucas sequences can be seen as power functions over a quadratic extension of the integers. The following congruences are generalizations of Fermat's Little Theorem. Let n be an odd prime, then

$$U_{n-(D/n)} \equiv 0 \bmod n, \text{ if } \gcd(n,D) = 1; \tag{1}$$

$$U_n \equiv (D/n) \bmod n; \tag{2}$$

$$V_n \equiv P \bmod n; \tag{3}$$

$$V_{n-(D/n)} \equiv 2Q^{(1-(D/n))/2} \bmod n, \text{ if } \gcd(n,D) = 1. \tag{4}$$

If n satisfies any two of the congruences (1) to (4) with $\gcd(n, 2PQD) = 1$, then n satisfies the other two.

An odd integer n for which congruence (1) holds is called a Lucas probable prime with parameters P, Q ($\mathcal{L}$prp(P,Q)). A Lucas pseudoprime ($\mathcal{L}$psp(P,Q)) is a composite Lucas probable prime. There exist infinitely many Lucas pseudoprimes for all parameters P, Q.

An odd integer n for which congruence (3) holds is called a Dickson probable prime with parameters P, Q ($\mathcal{D}$prp(P,Q)). A Dickson pseudoprime ($\mathcal{D}$psp(P,Q)) is a composite Dickson probable prime. For a list of references on Dickson pseudoprimes see [**MuOs93**]. Dickson pseudoprimes with fixed parameter $Q = -1$ are called Fibonacci pseudoprimes. There exist infinitely many Fibonacci pseudoprimes for every parameter P. An analogous result for Dickson pseudoprimes is not known. But there exist odd composite numbers (e.g. $N_1 = 443372888629441 = 17 \cdot 31 \cdot 41 \cdot 43 \cdot 89 \cdot 97 \cdot 167 \cdot 331$) which are Dickson pseudoprimes to all non trivial (i.e. $\gcd(n,Q) = 1$) parameters P, Q.

An odd integer n with $\gcd(n, QD) = 1$ and $U_{(n-(D/n))/2} \equiv 0 \bmod n$ if $(Q/n) = 1$, or $V_{(n-(D/n))/2} \equiv 0 \bmod n$ if $(Q/n) = -1$ is called Euler-Lucas probable prime with parameters P, Q (e$\mathcal{L}$prp(P,Q)). A Euler-Lucas pseudoprime (e$\mathcal{L}$psp(P,Q)) is a composite Euler-Lucas probable prime. Every e$\mathcal{L}$prp(P,Q) is a $\mathcal{L}$prp(P,Q). For nearly all parameters P, Q there exist infinitely many e$\mathcal{L}$prp(P,Q). An odd

composite number n cannot be an e$\mathcal{L}$prp(P,Q) simultaneously for all parameters P,Q with $\gcd(n,QD)=1$.

Let n be an odd integer n with $\gcd(n,D)=1$, $n-(D/n)=2^s d$, s.t. d odd and $s\geq 1$. If $U_d\equiv 0 \bmod n$, or $V_{2^r d}\equiv 0 \bmod n$ for some $r, 0\leq r<s$ then n is called a strong Lucas probable prime with parameters P,Q (s$\mathcal{L}$prp(P,Q)). A strong Lucas pseudoprime (s$\mathcal{L}$psp(P,Q)) is a composite s$\mathcal{L}$prp(P,Q). Every s$\mathcal{L}$prp$(P,Q)$is an e$\mathcal{L}$prp(P,Q). And therefore it is not possible for an odd composite number n to be a s$\mathcal{L}$prp(P,Q) simultaneously for all parameters P,Q with $\gcd(n,QD)=1$.

Note that it can be easily tested whether a large odd number n is a probable prime of one specific type, but it must be known somehow that n is composite to determine that n is a pseudoprime of the same type.

LD probable prime test

In 1980 Baillie & Wagstaff [**BaWa80**] proposed a probable prime test combining a strong probable prime test in base $a=2$ with a strong Lucas probable prime test, where the parameters P,Q are choosen by one of the two following algorithms:

A. Let D be the first element of the sequence $5,-7,9,-11,13,...$ for which $(D/n)=-1$. Let $P=1$ and $Q=(1-D)/4$.

B. Let D be the first element of the sequence $5,9,13,17,21,...$ for which $(D/n)=-1$. Let P the least odd integer exceeding $\sqrt{D}$, and $Q=(P^2-D)/4$.

A practical but not theoretical weakness of their test is the search for appropriate parameters P,Q.

The LD (Lucas Discriminant) probable prime test improves the probable prime test proposed by Baillie & Wagstaff in two ways:

1. Fixing the parameter $Q=\pm 2$ dependent only on n mod 24, so there is a dependency between the base $a=2$ and the parameter Q but *not* the parameter P.
2. Avoiding to search for an integer D with $(D/n)=-1$ in 7 out of 8 cases of n mod 24 (c.f. [**Mo97**]).

In the following we always assume $\gcd(n,2PQD)=1$. Otherwise the results can be given in a more complicated form to distinguish between necessary and sufficient conditions and their assumptions.

A relation between Dickson probable primes with parameters P,Q and Euler probable primes in base Q used by the LD probable prime test is given by

THEOREM 1. *Let n be an e$\mathcal{L}$prp(P,Q) with $\gcd(n,2PQD)=1$, then n is a $\mathcal{D}$prp(P,Q) if and only if n is an eprp(Q).*

PROOF. From the well known equations $V_{m+k}=V_mV_k-Q^kV_{m-k}=DU_mU_k+Q^kV_{m-k}$ we get with $m=(n+1)/2$, $k=(n-1)/2$

$$\begin{aligned} V_n-Q^{(n-1)/2}P &= DU_{(n+1)/2}U_{(n-1)/2} &&= DU_{(n+(D/n))/2}U_{(n-(D/n))/2} \\ V_n+Q^{(n-1)/2}P &= V_{(n+1)/2}V_{(n-1)/2} &&= V_{(n+(D/n))/2}V_{(n-(D/n))/2} \end{aligned}$$

and the result follows immediately. □

If n is a $\mathcal{D}$psp(P,Q) and an epsp(Q) then in general n is not an e$\mathcal{L}$psp(P,Q) as the following example illustrates.

EXAMPLE 1. Let $n = 7 \cdot 47 \cdot 89$ then n is a $\mathcal{D}\text{psp}(1,-1)$ and an epsp(-1) but from

$$U_{(n-(5/n))/2} \equiv 11515 \not\equiv 0 \bmod n \quad \text{and} \quad V_{(n-(5/n))/2} \equiv 233 \not\equiv 0 \bmod n$$

follows, that n is not an e$\mathcal{L}$psp$(1,-1)$.

The above theorem can be generalized using any two of the congruences (1) to (4).

THEOREM 2. *Let n be an eprp(Q) with $\gcd(n, 2PQD) = 1$, then n is an e$\mathcal{L}$prp(P,Q) if and only if n satisfies any two of the congruences (1) to (4).*

PROOF. Let n be an e$\mathcal{L}$prp(P,Q) then n is also a $\mathcal{L}\text{prp}(P,Q)$. Under the assumption that n is an eprp(Q) it follows from Theorem 1 that n is a $\mathcal{D}\text{prp}(P,Q)$. Hence n satisfies the congruences (1) and (3). The congruences (2) and (4) follow directly from the equations

$$\begin{aligned} U_n - Q^{(n-1)/2}(D/n) &= U_{(n-(D/n))/2} V_{(n+(D/n))/2} \\ U_n + Q^{(n-1)/2}(D/n) &= U_{(n+(D/n))/2} V_{(n-(D/n))/2} \\ V_{n-(D/n)} &= D U^2_{(n-(D/n))/2} + 2Q^{(n-(D/n))/2} \\ &= V^2_{(n-(D/n))/2} - 2Q^{(n-(D/n))/2}. \end{aligned}$$

Let n satisfy any two of the congrueneces (1) to (4) then n satisfies all congruences (1) to (4), i.e. congruence (1) and (2) hold always. From the congruence

$$U_{n+(D/n)} Q^{(1-(D/n))/2} \equiv (D/n) P \bmod n$$

and the equation $U_{n+(D/n)} = U_{(n+(D/n))/2} V_{(n+(D/n))/2}$ we get

$$\gcd(n, U_{(n+(D/n))/2}) = 1 \quad \text{and} \quad \gcd(n, V_{(n+(D/n))/2}) = 1.$$

That n is an e$\mathcal{L}$prp(P,Q) follows directly from

$$\begin{aligned} U_n - Q^{(n-1)/2}(D/n) &= U_{(n-(D/n))/2} V_{(n+(D/n))/2} \\ U_n + Q^{(n-1)/2}(D/n) &= U_{(n+(D/n))/2} V_{(n-(D/n))/2}. \end{aligned}$$

□

COROLLARY 2.1. *If n is a strong pseudoprime in base Q and a s$\mathcal{L}$psp(P,Q) then the congruences (1) to (4) hold for n.*

COROLLARY 2.2. *If n is an Euler-Lucas (or a strong Lucas) pseudoprime with parameters $P, Q = \pm 1$ then the congruences (1) to (4) hold for n.*

EXAMPLE 2. The smallest Euler-Lucas pseudoprimes 4181, 5777, 6721 and 10877 respectively the smallest strong Lucas pseudoprimes 4181, 5777 and 10877 with parameters $(1,-1)$ satisfy the congruences (1) to (4), i.e. they are also Lucas and Dickson probable primes with parameters $(1,-1)$.

COROLLARY 2.3. *Let n be an epsp(Q) with $\gcd(n, 2PQD) = 1$, then n is an e$\mathcal{L}$psp(P,Q) if and only if n is a $\mathcal{D}$psp(P,Q) and a $\mathcal{L}$psp(P,Q).*

That a *strong* version of the above corollary is not true is shown by

EXAMPLE 3. The odd composite number $n = 6721 = 11 \cdot 13 \cdot 47$ is a strong pseudoprime in base -1, a Dickson and Lucas pseudoprime with parameters $(1, -1)$ but not a strong Lucas pseudoprime with parameters $(1, -1)$.

To complete the considerations on fixing the parameter Q for the sprp($|Q|$) test and the s$\mathcal{L}$prp(P, Q) test the next lemma shows that it is possible to choose $a = 2 = |\pm 2| = |Q|$.

LEMMA 3. *An odd composite number n is a spsp(a) if and only if it is a spsp($-a$).*

PROOF. Let n be a spsp(a), i.e. for $n - 1 = 2^s d$ with d odd and $s \geq 1$ it follows that $a^d \equiv 1 \bmod n$, or $a^{2^r d} \equiv -1 \bmod n$ for some r with $0 \leq r < s$.

This implies

$$(-a)^d \equiv (-1)^d a^d \equiv (-1)a^{2^0 d} \equiv \mp 1 \bmod n$$

or if $r > 0$

$$(-a)^{2^r d} \equiv [(-1)^{2^r}]^d a^{2^r d} \equiv a^{2^r d} \equiv -1 \bmod n.$$

So if n is a spsp(a) then n is a spsp($-a$). If n is a spsp($-a$) then it is a spsp($-(-a)$)=spsp(a). □

We now complete our investigation of how strong probable primes in base Q interact with strong Lucas probable primes with parameters (P, Q). In [**Mo97**] it was shown that if $n \not\equiv 1 \bmod 24$, then the LD probable prime test has a worst case running time complexity of $O((\log n)^3)$. In the case of $n \equiv 1 \bmod 24$ the worst case complexity is $O(n^{\frac{1}{4}+\varepsilon})$ with $\varepsilon > 0$. If the extended form of Riemann's hypothesis is true, then the worst case complexity of the special case is also $O((\log n)^3)$. The running time can be reduced considerably if the implementation makes use of various dependencies among probable primes.

ALGORITHM LD (**L**ucas **D**iscriminant probable prime test) Let $n > 1$ be an integer. The LD probable prime test checks if n is a strong probable prime in base 2 and a strong Lucas probable prime with respect to parameters P, Q dependent only on n mod 24. If $n \not\equiv 1 \bmod 24$ then the given table, and otherwise the slightly modified method A proposed by Baillie & Wagstaff, results in a choice of parameters P, Q. The LD probable prime test certainly makes no mistakes for $n \leq 10^{13}$. If $n > 10^{13}$, no composite number passing the LD algorithm is known.

LD1. [Input.] $n > 1$.

LD2. [Initialize.] Let p_m some convenient prime number (e.g., $p_m = 1009$) and let $\mathcal{D}$ the set of all primes p with $5 \leq p < p_m$.
Set $\mathcal{S} \leftarrow \{2, 3, 1093, 3511\}$ and $N \leftarrow \prod_{p \in \mathcal{S} \cup \mathcal{D}} p$.

LD3. [Small prime?] If $\gcd(n, N) > 1$ and $n \in S \cup D$, then n is prime. If $\gcd(n, N) > 1$ and $n \notin S \cup D$, then n is composite. If $\gcd(n, N) = 1$ and $n < p_m^2$, then n is prime.

LD4. [sprp(2)?] If n is not a sprp(2), then n is composite.

LD5. [Choose P, Q.] If $n \not\equiv 1 \bmod 24$ then choose parameters P and Q according to

		P	Q
$n \equiv \pm 11 \bmod 24$		4	-2
$n \equiv \pm 5, -7 \bmod 24$		2	-2
$n \equiv -1, 7 \bmod 24$	$n \equiv 1, 2, 4 \bmod 7$	6	2
	$n \equiv 3, 5, 6 \bmod 7$	1	2

and continue with step LD8.

LD6. [n a square?] If n is a square then n is composite.

LD7. [Search $\mathcal{D}$.] Let $D \in \mathcal{D}$ the smallest element with $(D/n) < 1$. If there is no such $D \in \mathcal{D}$, then let $D \geq p_m$ the smallest odd number with $(D/n) < 1$. If $(D/n) = 0$, then n is composite, else set $P \leftarrow 1$ and $Q \leftarrow (1 - D)/4$ for $D \equiv 1 \bmod 4$; $Q \leftarrow (1 + D)/4$ otherwise.

LD8. [s$\mathcal{L}$prp(P, Q)?] If n is not a strong Lucas probable prime with parameters P and Q, then n is composite. Otherwise, n is almost certainly prime. ■

The parameters P, Q with $Q = \pm 2$ and $(D/n) = (P^2 - 4Q/n) = -1$ for $n \not\equiv 1 \bmod 24$ are given by a theorem in [**Mo97**]. In the case $n \equiv 1 \bmod 24$ the search for parameters P, Q cannot be avoided because then n might be a square.

Testing n to be a sprp(2) is only necessary if $n \equiv 1 \bmod 8$. In all other cases it is sufficient to test for eprp(2) but $(2/n)$ need not to be calculated, i.e. $2^{(n-1)/2} \equiv -1 \bmod n$ if $n \equiv \pm 3 \bmod 8$ and $2^{(n-1)/2} \equiv 1 \bmod n$ if $n \equiv 7 \bmod 8$. Also testing n to be a s$\mathcal{L}$prp(P, Q) is only necessary if $n \equiv 3 \bmod 4$. If $n \equiv 1 \bmod 4$ then it is sufficient to test for e$\mathcal{L}$prp(P, Q) but (Q/n) need not to be calculated, i.e. $U_{(n+1)/2} \equiv 0 \bmod n$ if $n \equiv 1 \bmod 8$ and $V_{(n+1)/2} \equiv 0 \bmod n$ if $n \equiv 5 \bmod 8$.

Testing n to be a Dickson probable prime instead of a strong Lucas probable prime in step LD8 is not sufficient. The following table lists all spsp(2) less than 10^{13} which will not be detected as composite using the Dickson probable prime test if the initial trial division is omitted.

			D
3581761	=	29·113·1093	-11
41217865921	=	23·89·2311·8713	13
551580094801	=	29·113·6301·26713	-11
756220537801	=	29·41·181·197·17837	-23
938986382881	=	29·757·5657·7561	-11
5203489730401	=	53·101·521·797·2341	-11

All the given numbers are congruent 1 modulo 24.

Conclusion

We have shown that the LD probable prime test makes extensive use of various dependencies between probable primes to ensure that composite numbers will be detected. There is strong evidence to combine a sprp(2) test with two different

Lucas congruences out of the congruences (1) to (4), i.e. a single Dickson test is not sufficient.

Finding a composite number bypassing the LD probable prime test seems to be a difficult task, but it may be possible. Whether the proposed combination of a sprp(2)- with a s$\mathcal{L}$prp$(P, \pm 2)$-test is sufficient is still an open problem. If it is not sufficient, further research on a probabilistic estimate with respect to the failure of the LD probable prime test will be necessary.

References

[BaWa80] R. Baillie and S. S. Wagstaff Jr., *Lucas pseudoprimes*, Math. Comp. **35** (1980), 1391–1417.

[Mo97] W. More, *Probable prime tests using Lucas sequences*, Applications of Fibonacci Numbers vol. 6, Kluwer, Dordrecht, 1997 (to appear).

[MuOs93] W. B. Müller and A. Oswald, *Generalized Fibonacci pseudoprimes and probable primes*, Applications of Fibonacci Numbers vol. 5, Kluwer, Dordrecht, 1993, pp. 459–464.

[Rib96] P. Ribenboim, *The New Book of Prime Number Records*, 3rd ed., Springer, New York, 1996.

INSTITUT FÜR MATHEMATIK, UNIVERSITÄT KLAGENFURT, A-9020 KLAGENFURT, AUSTRIA
E-mail address: willi.more@uni-klu.ac.at

This page intentionally left blank

Contemporary Mathematics
Volume **225**, 1999

Carmichael Numbers and Lucas Tests

Siguna M.S. Müller

ABSTRACT. Let $U_n(P,Q)$ and $V_n(P,Q)$ denote the Lucas sequences (cf. [**11, 16**]) of the first respectively second kind of degree n. For prime numbers n with $\gcd(n,QD)=1$ it is always true that

$$V_n(P,Q) \equiv P \pmod{n}, \text{ and} \tag{0.1}$$

$$U_{n-\epsilon(n)}(P,Q) \equiv 0 \pmod{n}, \tag{0.2}$$

where $D = P^2 - 4Q$ is the discriminant and $\epsilon(n) = \left(\frac{D}{n}\right)$ is the Legendre symbol. A composite integer n with $\gcd(n,2QD)=1$ fulfilling congruence (0.1) respectively (0.2) is called a Dickson- respectively Lucas pseudoprime (cf. [**1, 4, 7, 10**]) associated to the parameters P and Q. A major problem encountered with the test based on the V- sequences is the existence of super-strong Dickson pseudoprimes n, which although composite, fulfill congruence (0.1) for all integers P and Q (cf. [**6, 13, 14**]). These kinds of composites can be seen as counterparts of the Fermat Carmichael numbers in terms of the Lucas V- sequence. However, we will show that, if n is composite, congruence (0.2) cannot be fulfilled for all P and Q with $\gcd(n,DQ)=1$. This means that there are no Carmichael numbers for the Lucas test (0.2), or, equivalently, that there are no Lucas pseudoprimes with respect to all P and Q. Evenmore, we will also prove that there are no composite integers n that are Lucas pseudoprimes for a fixed value of $Q \in \mathbf{Z}_n^*$ and all varied values of P (or vice versa) with discriminants $D = P^2 - 4Q$ coprime to n.

INTRODUCTION

Let p and q denote odd prime factors of a composite integer n. It is known that the 'rank of apparition (appearance)', that is the smallest k (if it exists) with $U_k(P,Q) \equiv 0 \pmod{p}$, is always a divisor of $p - \left(\frac{D}{p}\right)$ provided DQ is coprime to p. We shall show that there exist parameters P and Q which give rise to the maximal rank, $k = p - \left(\frac{D}{p}\right)$ respectively $\frac{1}{2}\left(p - \left(\frac{D}{p}\right)\right)$.

As the rank is a function in two parameters P and Q, there are different ways of selecting those with the maximal rank. The ones considered will be, (1) keeping

---

1991 *Mathematics Subject Classification.* Primary: 11A51, 11B39; Secondary: 11Y11.
Research supported by the Forschungskommission der Universität Klagenfurt.

© 1999 American Mathematical Society

the discriminant D fixed, (2), (3) keeping either one of P or Q fixed and varying the other. In both of the latter cases the results obtained will establish the non-existence of Lucas pseudoprimes for varied parameters. The non-existence of Lucas pseudoprimes to all discriminants will be shown by using a theorem of [**22**] concerning Carmichael Lucas pseudoprimes.

The Lucas sequence with respect to a fixed discriminant

1. Carmichael Lucas pseudoprimes

H.C.Williams (cf. [**22**]) considered Lucas pseudoprimes with respect to all choices of integers (P,Q) having the same fixed discriminant D (say). More precisely, he called an odd composite integer n a Carmichael Lucas pseudoprime (associated to D), if $\gcd(n,D)=1$ and for all nonzero relatively prime integers P,Q with $P^2-4Q\equiv D \pmod n$ and $\gcd(n,Q)=1$ the number n is a Lucas pseudoprime. He has shown that if n is a Carmichael Lucas pseudoprime, then n is squarefree and each prime p dividing n fulfills $\left(p-\left(\frac{D}{p}\right)\right)\Big|\left(n-\left(\frac{D}{n}\right)\right)$. Further, it can easily be checked that those two conditions are also sufficient for n to be a Carmichael Lucas pseudoprime.

2. No absolute Carmichael Lucas pseudoprimes

Carmichael Lucas pseudoprimes can quite frequently be found using a modification of Chernick's universal forms algorithm (cf. [**3**]). Hence, one might try to introduce some kind of Lucas type pseudoprimes which don't occur with the high frequency as the Carmichael Lucas pseudoprimes.

We call a composite integer n an *absolute Carmichael Lucas pseudoprime*, if n is a Lucas pseudoprime for all parameters P and Q whose discriminants D are coprime to n. Thus, any absolute Carmichael Lucas pseudoprime has to be a Lucas pseudoprime to $\phi(n)$ distinct discriminants modulo n. We will show that numbers of that kind don't exist.

Lemma 2.1. *Suppose that n is a Carmichael Lucas pseudoprime associated to two distinct discriminants D_1 and D_2 with*

1. $\left(\frac{D_1}{p}\right)=\left(\frac{D_1}{n}\right)$ *for all prime divisors p of n, and*
2. $\left(\frac{D_2}{n}\right)=-\left(\frac{D_1}{n}\right)$,

then is n a Carmichael Lucas pseudoprime for all discriminants $D\in\mathbf{Z}_n^*$ for which $\left(\frac{D}{p}\right)=\left(\frac{D}{n}\right)$ for all p dividing n.

Proof. Without loss of generality let D_1 respectively D_2 denote any discriminant with Jacobi symbol $+1$ respectively -1 modulo n. Then by hypothesis, $\left(\frac{D_1}{p}\right)=\left(\frac{D_1}{n}\right)=1$ for all primes p dividing n. We claim that $\left(\frac{D_2}{p}\right)=-1$ for all $p|n$. For suppose there is a prime divisor q of n and $\left(\frac{D_2}{q}\right)=1$, then from the assumption that n is a Carmichael Lucas pseudoprime associated to D_2 it follows that $(q-1)|(n+1)$. But for D_1 we have $(q-1)|(n-1)$. These two results agree only when $q=3$. From $\left(\frac{D_2}{n}\right)=-1$ we conclude that there is a prime factor p of n so that $\left(\frac{D_2}{p}\right)=-1$. It likewise follows that $(p+1)|(n+1)$ and $(p-1)|(n-1)$.

This evidently is impossible if $3|n$ since $p \neq 3$. Therefore $\left(\frac{D_2}{n}\right) = \left(\frac{D_2}{p}\right) = -1$ for all primes p when $\left(\frac{D_2}{n}\right) = -1$. In the same manner it can be shown that any discriminant D_1 with $\left(\frac{D_1}{n}\right) = 1$ implies $\left(\frac{D_1}{p}\right) = 1$ for all prime factors p. For if $(p+1)|(n-1)$, then there is a quadratic nonresidue D_2, whence $(p+1)|(n+1)$, which will only be true for $p = 1$, a contradiction too. □

COROLLARY 2.2. *There are no absolute Carmichael Lucas pseudoprimes.*

PROOF. Let p be any prime dividing the absolute Carmichael Lucas pseudoprime n. Then $\left(\frac{D}{p}\right) = \left(\frac{D}{n}\right)$ for all $D \in \mathbf{Z}_n^*$. Thus there are precisely two classes of discriminants D, namely those for which $\left(\frac{D}{p}\right) = 1$ for all prime factors p of n, and those for which $\left(\frac{D}{p}\right) = -1$ for all p dividing n. This gives a number of $2\prod_{p|n}(p-1)/2$ discriminants. However, by definition, those have to comprise all $\phi(n)$ discriminants D in $\mathbf{Z}_n^*$, a contradiction. □

REMARK. As of today, no composite integers fulfilling the two conditions of Lemma 2.1 are known, although some heuristic arguments supporting their existence are stated in [**15**].

THE VARIATION OF PARAMETERS

The following considerations will be needed to prove our main results.

3. Squares and nonsquares among the discriminants

PROPOSITION 3.1. *Let $\epsilon \in \{-1, 1\}$ be a fixed integer and p an odd prime.*

1. *For $Q_0 \in \mathbf{Z}_p^*$ the number of elements $P \in \mathbf{Z}_p$ with $\left(\frac{P^2-4Q_0}{p}\right) = \epsilon$ is equal to*

$$\frac{p-\epsilon}{2} - \frac{1}{2}\left(1 + \left(\frac{Q_0}{p}\right)\right).$$

2. *For $P_0 \in \mathbf{Z}_p^*$ the number of elements $Q \in \mathbf{Z}_p^*$ with $\left(\frac{P_0^2-4Q}{p}\right) = \epsilon$ is equal to*

$$\frac{p-2-\epsilon}{2}.$$

PROOF. 1. This follows from [**7**].

2. By calculating the number of parameters Q in $\mathbf{Z}_p$ the desired number becomes

- for $\epsilon = 1$

$$\sum_{\substack{Q=0 \\ P_0^2 \not\equiv 4Q \mod p}}^{p-1} \frac{1}{2}\left(1 + \left(\frac{P_0^2-4Q}{p}\right)\right) = \frac{p}{2} - \frac{1}{2} + \frac{1}{2}\sum_{Q=0}^{p-1}\left(\frac{P_0^2-4Q}{p}\right) = \frac{p-1}{2}$$

- and thus for $\epsilon = -1$

$$\sum_{\substack{Q=0 \\ P_0^2 \not\equiv 4Q \mod p}}^{p-1} 1 - \frac{p-1}{2} = \frac{p-1}{2}.$$

Now, the number of parameters $Q \in \mathbf{Z}_p^*$ follows by observing that, for $Q = 0$ we have $\left(\frac{P_0^2}{p}\right) = 1$, so that for $\epsilon = 1$ we obtain the desired number as $\frac{p-1}{2} - 1 = \frac{p-3}{2}$.

□

COROLLARY 3.2. *Suppose p is an odd prime.*

1. *Let Q_0 be a fixed integer with $\gcd(p, Q_0) = 1$. Then the number of distinct discriminants $D(P) = P^2 - 4Q_0$ modulo p with $\left(\frac{D(Q)}{p}\right) = 1$ is*

$$\frac{r-1}{2} - \gamma, \text{ for } \gamma = \begin{cases} 1, & \text{if } 2 \nmid r \\ 0, & \text{else} \end{cases}$$

and $r = \frac{p - \left(\frac{D(P)}{p}\right)}{2} - \frac{1}{2}\left(1 + \left(\frac{Q_0}{p}\right)\right)$.

2. *Let P_0 be a fixed integer with $\gcd(p, P_0) = 1$. Then the number of distinct discriminants $D(Q) = P_0^2 - 4Q$ modulo p with $\left(\frac{D(Q)}{p}\right) = 1$ is $\frac{p-3}{2}$ and the number of those with $\left(\frac{D(Q)}{p}\right) = -1$ is $\frac{p-1}{2}$.*

4. Squarefreeness of Lucas pseudoprimes to distinct parameters

Given the Lucas sequence $U(P, Q)$ and an integer $m > 0$, let $\rho(m) = \rho(m, P, Q)$ be the least positive integer k, if it exists, such that $m | U_k(P, Q)$. Then $\rho(m)$ is called the rank of apparition (modulo m of the Lucas sequence $U(P, Q)$). It can be shown that $\rho(m)$ exists if $p \nmid Q$ for all prime divisors p of m (cf. [**16, 18**]).

For our purpose it suffices to consider integers m, m_i respectively odd primes p with $\gcd(mm_i, QD) = 1$ respectively $\gcd(p, QD) = 1$. Then the rank of apparition is known to have the following properties (cf. [**2**],[**16**]).

(4.1) $m | U_k(P, Q)$ if and only if $\rho(m, P, Q) | k$,

(4.2) $\rho(p, P, Q) \Big| \left(p - \left(\frac{D}{p}\right)\right)$,

(4.3) $\rho(p, P', Q') = \rho(p, Q, P)$ when $P' \equiv P,\ Q' \equiv Q \pmod{p}$,

(4.4) $\rho(p, P, Q) \Big| \frac{p - (D/p)}{2}$ if and only if $\left(\frac{Q}{p}\right) = 1$,

(4.5) $\rho(\operatorname{lcm}(m_1, \ldots, m_k)) = \operatorname{lcm}(\rho(m_1), \ldots, \rho(m_k))$,

(4.6) $\rho(p^t, P, Q) = p^c \rho(p, P, Q)$ for a $c \in \{0, \ldots, t-1\}$.

REMARK. For a generalization of the concept of the rank of apparition we refer to [**19**], [**20**], and [**21**], where L. Somer deals with the (restricted) period of k-th order linear recurrence sequences.

PROPOSITION 4.1. *Let p be an odd prime, $P \in \mathbf{Z}$, $Q \in \mathbf{Z}_p^*$. There exists an integer P' such that $\left(\frac{P^2-4Q}{p}\right) = \left(\frac{P'^2-4Q}{p}\right)$, and $\rho(p^2, P', Q) = p \cdot d$, where $d \Big| \left(p - \left(\frac{P^2-4Q}{p}\right)\right)$.*

REMARK. In dealing with Carmichael Lucas pseudoprimes, a property similar to this was proved in [22]. We restrict ourselves to the case that $Q = Q_0$ is kept fixed whence $U_k(x, Q_0)$ becomes a polynomial in $x = P$. If $U_k = U_k(P, Q)$ is considered to be a polynomial in two indeterminates P and Q, or $U_k = U_k(P_0, y)$, when P_0 is fixed, the proof runs along the same line.

PROOF. Let $\epsilon(p)$ denote the Legendre symbol $\left(\frac{P^2-4Q}{p}\right)$. Now, if $p^2|U_{p-\epsilon(p)}(P)$ then put $P' = P+Kp$ with $\gcd(K, p) = 1$, whereas $U_k(P+Kp) \equiv U_k(P)+U'_k(P)Kp \pmod{p^2}$ by Taylor's Expansion. As $\epsilon(p) = \left(\frac{P^2-4Q_0}{p}\right) = \left(\frac{P'^2-4Q_0}{p}\right)$ this yields $U_{p-\epsilon(p)}(P+Kp, Q) \equiv U_{p-\epsilon(p)}(P, Q)+U'_{p-\epsilon(p)}(P, Q)Kp \pmod{p^2}$. Using fundamental properties of the U-sequences it can be shown that $p \nmid U'_{p-\epsilon(p)}(P)$, which gives $U_{p-\epsilon(p)}(P') \not\equiv 0 \pmod{p^2}$, so that $\rho(p^2, P', Q_0) > \rho(p, P', Q_0) = \rho(p, P, Q_0) = p - \epsilon(p)$ and thus necessarily $p|\rho(p^2, P', Q_0)$. □

COROLLARY 4.2. 1. *Any Carmichael Lucas pseudoprime n is squarefree.*
2. *Suppose there is an integer n that is a Lucas pseudoprime to a fixed Q_0 and all parameters P for which $\gcd(P^2 - 4Q_0, n) = 1$. Then n has to be squarefree.*
3. *Suppose n that is a Lucas pseudoprime to a fixed P_0 and all parameters Q for which $\gcd(P_0^2 - 4Q, n) = 1$. Then n has to be squarefree.*

PROOF. The case for Carmichael Lucas pseudoprimes has been dealt with in [22]. If $Q = Q_0$ is assumed to be fixed and $U_{n-(D/n)}(x, Q_0) \equiv 0 \pmod{n}$ with $n = p^2R$ then choose P' as above to obtain $p|\rho(p, P', Q_0)$. On the other hand, $U_{n-\left(\frac{D}{n}\right)}(P', Q_0) \equiv 0 \pmod{p^2}$ yields $\rho(p^2, P, Q)\left|\left(n - \left(\frac{D}{n}\right)\right)\right.$ for $D = P'^2 - 4Q_0$. Combining these two conditions we obtain $p|(n-\epsilon)$ with $\epsilon = \left(\frac{D}{n}\right) \neq 0$ and $p|n$, which cannot occur. Now the case for a fixed P_0 can be treated in a similar fashion. □

THE ONEDIMENSIONAL LUCAS TEST

5. Parameters with the maximal rank

5.1. Motivation. In [22] H. C. Williams defined, for a fixed discriminant D and a fixed odd prime p, the function $\psi(d, D)$, where $d|(p - (D/p))$, to be the number of distinct values of P modulo p such that there exists a Q with $P^2 - 4Q \equiv D \pmod{p}$ and $\rho(p, P, Q) = d$. Analogously, we introduce similar functions for keeping, instead of the discriminant, either P_0 or Q_0 fixed.

In particular, we shall deal with the case $d = p - \left(\frac{D}{p}\right)$.

5.2. Keeping $P = P_0$ fixed and varying Q.

DEFINITION 5.1. Let $P_0 \in \mathbf{Z}_p^*$, $\epsilon \in \{-1, 1\}$ be fixed integers and $d > 1$ be any divisor of $p - \epsilon$. Denote by $\underline{\psi}(d, P_0, \epsilon)$ the number of distinct values of $Q \in \mathbf{Z}_p^*$ for which $\rho(p, P_0, Q) = d$.

REMARK. The function $\underline{\psi}(d, P_0, \epsilon)$ counts the number of $Q's$ such that both $\left(\frac{P_0^2-4Q}{p}\right) = \epsilon$ and $\rho(p) = d|(p - \epsilon)$.

LEMMA 5.2. *If $\epsilon \in \{-1,1\}$ is fixed, then there exist $\frac{\phi(p-\epsilon)}{2}$ parameters $Q \in \mathbf{Z}_p^*$ for which $\rho(P_0,Q,p) = p-\epsilon$.*

PROOF. The number of solutions $Q \in \mathbf{Z}_p^*$ with $\left(\frac{D(Q)}{p}\right) = \epsilon$ of $U_{p-\epsilon}(P_0,Q) \equiv 0 \pmod p$ is according to Proposition 3.1 exactly $\frac{p-\epsilon-2}{2}$. Now put

$$\begin{cases} \chi(h) = \underline{\psi}(h,P_0,\epsilon) & \text{for } h \neq 1,2 \\ \chi(h) = \begin{cases} 1 & \text{for } h = 1 \\ 0 & \text{for } h = 2 \end{cases} \end{cases}$$

Then from the definition of $\underline{\psi}(h,P_0,\epsilon)$ this gives

$$\sum_{h|(p-\epsilon)} \chi(h) = \frac{p-\epsilon-2}{2} + 1 = \frac{p-\epsilon}{2}$$

and by Möbius' inversion

$$\underline{\psi}(p-\epsilon) = \sum_{h|(p-\epsilon)} \mu(h)\frac{p-\epsilon}{2h} = \frac{\phi(p-\epsilon)}{2}.$$

□

5.3. Keeping $Q = Q_0$ fixed and varying P. Similar to the above case we define

DEFINITION 5.3. Let $Q_0 \in \mathbf{Z}_p^*$, $\epsilon \in \{-1,1\}$ be fixed, and $d > 1$ be any divisor of $p-\epsilon$. The function $\bar{\psi}(d,Q_0,\epsilon)$ is defined to be the number of distinct values of P modulo p for which $\rho(p,P,Q_0) = d$.

REMARK. Now, obviously $\bar{\psi}(d,Q_0,\epsilon)$ counts the values of P with $\left(\frac{P^2-4Q_0}{p}\right) = \epsilon$ and $\rho(p) = d|(p-\epsilon)$.

LEMMA 5.4. *If $\epsilon \in \{-1,1\}$ is fixed, then there exist $\phi(\frac{p-\epsilon}{t})$ parameters $P \in \mathbf{Z}_p^*$ for which $\rho(P,Q_0,p) = \frac{p-\epsilon}{t}$ with $t = 1$ if $\left(\frac{Q_0}{p}\right) = -1$, and $t = 2$ if $\left(\frac{Q_0}{p}\right) = 1$.*

PROOF. (a) Let $\left(\frac{Q_0}{p}\right) = -1$.

Again, from Proposition 3.1 there are $\frac{p-\epsilon}{2}$ solutions P of $U_{p-\epsilon}(P,Q_0) \equiv 0 \pmod p$ with $\left(\frac{D(P)}{p}\right) = \epsilon$. Moreover, $U_{(p-\epsilon)/2}(P,Q_0) \not\equiv 0 \pmod p$ for all those P. In putting

$$\begin{cases} \chi(h) = \overline{\psi}(h,P_0,\epsilon) & \text{for } \nu_2(h) = \nu_2(p-\epsilon) \\ \chi(h) = \phi(h) & \text{otherwise} \end{cases}$$

we find

$$\sum_{h|(p-\epsilon)} \chi(h) = \sum_{\substack{h|(p-\epsilon) \\ \nu_2(h)=\nu_2(p-\epsilon)}} \overline{\psi}(h,P_0,\epsilon) + \sum_{h|\frac{p-\epsilon}{2}} \phi(h) =$$

$$= \frac{p-\epsilon}{2} + \frac{p-\epsilon}{2} = p-\epsilon.$$

By applying Möbius' inversion formula we get

$$\chi(p-\epsilon) = \sum_{h|(p-\epsilon)} \mu(h)\frac{p-\epsilon}{h} = \phi(p-\epsilon).$$

(b) Let $\left(\frac{Q_0}{p}\right) = 1$.

By observing that, for all P, $U_{(p-\epsilon)/2}(P, Q_0) \equiv 0 \pmod{p}$ and arguing as above, we obtain

$$\sum_{h \mid \frac{p-\epsilon}{2}} \chi(h) = \sum_{h \neq 1} \overline{\psi}(h, P_0, \epsilon) + 1 = \frac{p-\epsilon}{2}$$

where

$$\begin{cases} \chi(h) = \overline{\psi}(h, P_0, \epsilon) & \text{for } h \mid \frac{p-\epsilon}{2} \text{ and } h \neq 1 \\ \chi(h) = 1 & \text{for } h = 1. \end{cases}$$

Similarly, Möbius' formula gives

$$\chi(\frac{p-\epsilon}{2}) = \phi(\frac{p-\epsilon}{2}).$$

□

6. No Carmichael numbers for the Lucas test in the first indeterminate

THEOREM 6.1. *There are no composite integers n with $5 \nmid n$ such that the congruence $U_{n-(\frac{D(P)}{n})}(P, Q_0) \equiv 0 \pmod{n}$ holds for all P with $\gcd(Q_0 D(P), n) = 1$, when $Q = Q_0$ is kept fixed.*

PROOF. Assume that there is a number n fulfilling the properties of the theorem. Then Corollary 4.2 asserts then n is the product of different primes p. For each of these p we can choose $P_1 \pmod{p}$ with $\rho(p, P_1) = \frac{p-1}{t}$, where t is chosen as in Lemma 5.4. Thus, by Property (i) we obtain $\frac{p-1}{t} \Big| (n-1)$. Further, if for all p we select $P_2 \pmod{p}$ with $\rho(p, P_2) = \frac{p-\left(\frac{D(P_2)}{p}\right)}{t}$ and $\prod_{p \mid n} \left(\frac{D(P_2)}{p}\right) = \left(\frac{D(P_2)}{n}\right) = -1$, then we obtain $\frac{p-(D(P_2)/p)}{t} \Big| (n+1)$.

We show that this implies $\left(\frac{D(P_2)}{p}\right) = \left(\frac{D(P_2)}{n}\right)$ for any prime $p \mid n$. In like manner as in Lemma 2.1 the contrary yields

$$\frac{p-1}{t} \Big| (n+1), \ \frac{p-1}{t} \Big| (n-1),$$

so that necessarily $\frac{p-1}{t} = 2$. However, $t = 1$ is eliminated by the arguments used for Corollary 2.1, while $t = 2$ yields $p = 5$, which has been excluded by assumption. Similarly, for any arbitrary $P \pmod{p}$ with $\left(\frac{D(P)}{p}\right) = 1$ we obtain $\rho(p, P) \mid \frac{p-1}{t} \Big| (n-1)$ and therefore, because of $\rho(p, P) > 2$, $\left(\frac{D(P)}{n}\right) = 1$. Analogously, for $\left(\frac{D(P)}{p}\right) = -1$ it follows that $\left(\frac{D(P)}{n}\right) = -1$. We thus have two types of discriminants $D(P)$, those for which $\left(\frac{D(P)}{p}\right) = 1$ respectively -1 for all primes p dividing n.

We remember that the number of distinct $P \in \mathbf{Z}_p$ with $\left(\frac{D(P)}{p}\right) = \epsilon(p) \in \{\pm 1\}$ is by Corollary 3.1 given as

$$\frac{p - \left(\frac{D(P)}{p}\right)}{2} - \frac{1}{2}\left(1 + \left(\frac{Q_0}{p}\right)\right).$$

Put $\gamma(Q_0) = \frac{1}{2}\left(1 + \left(\frac{Q_0}{p}\right)\right)$. Then we obtain the number of $P \in \mathbf{Z}_p$ with $\gcd(D(P), p) = 1$ as

$$\frac{p-1}{2} - \gamma(Q_0) + \frac{p+1}{2} - \gamma(Q_0) = p - 2\gamma(Q_0),$$

and the number of $P \in \mathbf{Z}_n$ with $\gcd(D(P), n) = 1$ as

$$\prod_{p|n}(p - 2\gamma(Q_0)).$$

This number is equal to the number of P's $\in \mathbf{Z}_n$ with $\left(\frac{D(P)}{n}\right) = 1$ plus the number of those with $\left(\frac{D(P)}{n}\right) = -1$. Using the fact that $\left(\frac{D(P)}{p}\right) = \left(\frac{D(P)}{n}\right)$ for all $p|n$ this therefore implies

$$\sum_{\substack{P \in \mathbf{Z}_n \\ (\frac{D(P)}{n})=\pm 1}} 1 = \sum_{\substack{P \in \mathbf{Z}_n \\ (\frac{D(P)}{n})=1}} 1 + \sum_{\substack{P \in \mathbf{Z}_n \\ (\frac{D(P)}{n})=-1}} 1 = \prod_{p|n} \sum_{\substack{P \in \mathbf{Z}_p \\ (\frac{D(P)}{p})=1}} 1 + \prod_{p|n} \sum_{\substack{P \in \mathbf{Z}_p \\ (\frac{D(P)}{p})=-1}} 1,$$

so that

$$\prod_{p|n}(p - 2\gamma(Q_0)) = \prod_{p|n}\left(\frac{p-1}{2} - \gamma(Q_0)\right) + \prod_{p|n}\left(\frac{p+1}{2} - \gamma(Q_0)\right),$$

which always holds for $n = p$ prime. For composite integers n the right hand side is always $\leq \prod_{p|n} \frac{p-1}{2} + \prod_{p|n} \frac{p+1}{2}$, while the left hand side is always $\geq \prod_{p|n}(p-2)$. This is a contradiction. □

7. No Carmichael numbers for the Lucas test in the second indeterminate

THEOREM 7.1. *There are no composite integers n such that $U_{n-(\frac{D(Q)}{n})}(P_0, Q) \equiv 0 \pmod{n}$ holds for all discriminants $D(Q) = P_0^2 - 4Q$ that are relatively prime to n, when $P = P_0$ is fixed.*

PROOF. Analogously to the proof of Theorem 6.1 we conclude that $p^2 \nmid n$ for all primes p dividing n and we can find parameters Q with $\rho(p, Q) = p - \left(\frac{D(Q)}{p}\right)$. It follows that $\left(p - (\frac{D(Q)}{p})\right) \mid \left(n - (\frac{D(Q)}{n})\right)$. In the same manner as above this yields $(p-1)|(n-1)$ and $(p+1)|(n+1)$, which again implies $\left(\frac{D(Q)}{p}\right) = \left(\frac{D(Q)}{n}\right)$ for all $p|n$. Therefore the number of $D(Q)'s$ modulo n is the number of those that are squares plus the number of the nonsquares, which gives, using Corollary 3.2,

$$\prod_{p|n} \frac{p-3}{2} + \prod_{p|n} \frac{p-1}{2} = \prod_{p|n}(p-2).$$

However, this is impossible when n is not a prime. □

COROLLARY 7.2. *There are no composite integers n such that the congruence $U_{n-(\frac{D(Q)}{n})}(P_0, Q) \equiv 0 \pmod{n}$ holds for a fixed parameter $P = P_0$ and all Q with $\gcd(QD(Q), n) = 1$.*

8. Concluding Remarks

It has been shown that using the Lucas test $U_{n-(D/n)}(P,Q) \equiv 0 \pmod{n}$ as a compositeness test is more preferable than using the Lucas test $V_n(P,Q) \equiv P \pmod{n}$. Whereas the latter congruence gives rise to the existence of pseudoprimes with respect to any parameters P and Q, the former congruence cannot be fulfilled for all those parameters. The actual number of parameters to the Lucas test and related questions will be investigated in a future paper.

ACKNOWLEDGMENT. I am deeply grateful to Professor W. B. Müller for numerous helpful discussions, his valuable comments and his patience in being my teacher and supervisor. Also, I am very thankful to Professor J. Schoißengeier for his qualifying advice, and Professor C. Pomerance for providing [**15**] and his interest in my work. Many thanks go to Professor L. Somer for providing [**18**], [**19**], [**20**], and [**21**], and making me aware of those articles.

References

1. Baillie R. and Wagstaff S., Jr., *Lucas pseudoprimes,* Math. Comp. **35** (1980), 1391 - 1417.
2. Carmichael R. D., *On the numerical factors of the arithmetic forms* $a^n \pm b^n$, Ann. of Math. **15** (1913), 30 - 70.
3. Chernick J., *On fermat's simple theorem,* Bull. Amer. Math. Soc. **45** (1939), 269 -274.
4. Di Porto A. and Filipponi P., *A probabilistic primality test based on the properties of certain generalized Lucas numbers,* Advances in Cryptology – Eurocrypt '88, Springer, Berlin, (1988), 211 - 223.
5. ———, *Generating M-strong Fibonacci pseudoprimes,* Fibonacci Quart. **30** (1992), 339 - 343.
6. Guillaume D. and Morain F., *Building pseudoprimes with a large number of prime factors,* AAECC, **7**, no. 4, (1996), 263 - 277.
7. Kowol G., *On strong dickson pseudoprimes,* AAECC **3** (1992), 129 - 138.
8. Lidl R. and Müller W. B., *A note on strong Fibonacci pseudoprimes,* Advances in Cryptology. - Auscrypt'90, Springer, New York (1990), 311 - 317.
9. ———, *Generalization of the Fibonacci pseudoprimes test,* Discrete Mathematics **92** (1991), 211 - 220.
10. Lidl R., Müller W. B., and Oswald A., *Some remarks on strong Fibonacci pseudoprimes,* AAECC **1** (1990), 59 - 65.
11. Lidl R., Mullen G. L., Turnwald G., *Dickson Polynomials,* Pitman Monographs and Surveys in Pure ans Applied Mathematics, vol 65. Longman, London (1993).
12. Müller W. B. and Oswald A., *Dickson pseudoprimes and primality testing,* Advances in Cryptology. - Eurocrypt'91, Springer, Berlin (1991), 512 -516.
13. ———, *Generalized Fibonacci pseudoprimes and probable primes,* Application of Fibonacci Numbers, **5** (1993), 459 - 464.
14. Pinch R. G. E., *The Carmichael numbers up to* 10^{15}, Math. Comp. **61** (1993), 381 - 391.
15. Pomerance C., *Are there counter-examples to the Baillie-PSW primality test?* In: Dopo le parole, (A. K. Lenstra, ed.), Amsterdam (1984).
16. Ribenboim P., *The Book of Prime Number Records,* Springer Verlag, Berlin (1988).
17. Riesel H., *Prime Numbers and Computer Methods for Factorization,* Birkhäuser, Boston, Basel, Stuttgart (1985).
18. Somer L., *Divisibility of Terms in Lucas Sequences by their Subscripts,* Applications of Fibonacci Numbers **5** (1993), 515-525.
19. ———, *Periodicity Properties of kth Order Linear Recurrences Whose Characteristic Polynomial Splits Completely Over a Finite Field, I,* Contemporary Mathematics **168** (1994), 327-339.
20. ———, *Periodicity Properties of kth Order Linear Recurrences Whose Characteristic Polynomial Splits Completely Over a Finite Field, II,* In: Finite Fields and their Applications, S. Cohen, H. Niederreiter (eds.), Cambridge University Press (1996), 333-347.

21. ———, *Periodicity Properties of kth Order Linear Recurrences with Irreducible Characteristic Polynomial Over a Finite Field,* In: Finite Fields, Coding Theory and Advances in Communications and Computing, Gary L. Mullen and Peter Jau-Shyong Shiue (eds.), Marcel Dekker Inc., (1993), 515-525.
22. Williams H. C., *On numbers analogous to the Carmichael - numbers,* Canad. Math. Bull. **20** (1977), 133 - 143.

Department of Mathematics, University of Klagenfurt, 9020 Klagenfurt, Austria, Europe
E-mail address: siguna.mueller@uni-klu.ac.at

Contemporary Mathematics
Volume 225, 1999

On the state complexity of some long codes

Tim Blackmore and Graham Norton

ABSTRACT. We determine the state complexities of three families of codes that generalise the Reed–Muller codes. Our approach would seem to be new and in particular would seem to provide simplified proofs of known results on trellises for Reed–Muller codes. One of the families is new and its classical code parameters, which compare well with those of the other codes considered, are given. We conclude with a comparison of the asymptotic performance of the codes' parameters.

1. Introduction

1.1. Background. The state complexity (SC) of a code provides a measure of the complexity of the Viterbi decoding algorithm for that code. (We consider linear block codes only.) As such, it is often regarded as the fourth code parameter (the three classical parameters being the length, dimension and minimum distance of the code). Unlike the other three parameters it is dependent on the bit–ordering of the code—i.e. equivalent codes can have different SCs.

It is well–known that cyclic (here we include shortened cyclic and extended cyclic) codes have worst possible SC, [**7**], reaching an upper–bound given by Wolf, [**12**]. There has been considerable work on finding the SCs of short (lengths of up to about 128) $\mathcal{BCH}$–codes under various (non–cyclic) bit–orderings. However, it seems that the only long codes for which SCs under non–cyclic bit–orderings have been considered are the family of binary Reed–Muller ($\mathcal{RM}$–)codes.

In fact, since Forney's defining work, [**5**], in which the SC of a 4–section uniform trellis of a $\mathcal{RM}$–code is determined, there has been considerable interest in the SCs of $\mathcal{RM}$–codes. Most notably, it has been shown that the standard bit–ordering of an $\mathcal{RM}$–code is always optimum with respect to its SC, [**6**], and the SC under this bit–ordering has been determined, [**1**].

Here we determine and compare the SCs of three distinct families of (not necessarily binary) codes, each of which contains the $\mathcal{RM}$–codes as a special case. We show that one of these families of codes can be considered as generalising the $\mathcal{RM}$–codes with respect to SC—a family of codes defined a long time before SCs were first considered but of little interest otherwise. We believe our consideration of the SCs of these codes gives a simplified approach to the determination of the SCs (and other trellis characteristics) of $\mathcal{RM}$–codes.

1991 *Mathematics Subject Classification.* 11T71, 94B99.

Research supported by the U. K. Engineering and Physical Sciences Research Council under grant K27728.

© 1999 American Mathematical Society

1.2. State complexities. In [12] the Viterbi decoding algorithm was applied to block codes. The algorithm takes place along a trellis for a code. A trellis is a directed graph whose vertices are placed at depths. A trellis for a length n code has $n+1$ depths, usually labelled from 0 to n, but here labelled from -1 to $n-1$. The initial and final depth each have only one vertex. Paths through the trellis, passing through a single vertex at each depth, are in one–to–one correspondence with the codewords. It is advantageous for Viterbi decoding that many paths pass through each vertex and hence that there are as few vertices as possible at each depth. A code has a trellis which simultaneously minimises the number of vertices at each depth, called its minimal trellis (e. g. [8]). We consider only minimal trellises.

The set of vertices at each depth of a (minimal) trellis forms a vector space. For a length n code C, we write $s_i(C)$ for the dimension of the vertex space at depth i (where $-1 \leq i \leq n-1$). The state complexity (SC) of C is given by

$$s(C) = \max_{-1 \leq i \leq n-1} \{s_i(C)\}.$$

In [11] the SC of a code was described as a 'fundamental descriptive characteristic, comparable to the length, size and minimum distance'. A list of more recent publications in which SC plays a central role is given in [10].

Calculating the $s_i(C)$ is possible without full knowledge of the trellis, [5]. For $-1 \leq i \leq n-1$, the i^{th} past subcode of C, denoted by C_i^-, is the set of codewords of the form $(c_0, c_1, \ldots, c_i, 0, \ldots, 0)$. Similarly the i^{th} future subcode of C, denoted by C_i^+, is the set of codewords of the form $(0, \ldots, 0, c_{i+1}, c_{i+2}, \ldots, c_{n-1})$. If we write $k(D)$ for the dimension of a code D then

$$s_i(C) = k(C) - k(C_i^-) - k(C_i^+). \tag{1.1}$$

Now $k(C_i^-)$ increases in unit steps from 0 to $k(C)$, and $k(C_i^+)$ decreases in unit steps from $k(C)$ to 0. An increase in $k(C_i^-)$ leads to a (possible) decrease in $s_i(C)$ and so we refer to an i where this happens as a point of fall (PofF). Similarly a decrease in $k(C_i^+)$ leads to a (possible) increase in $s_i(C)$ and so we refer to an i where this happens as a point of gain (PofG). It is possible that i is both a PofF and PofG, in which case $s_i(C) = s_{i-1}(C)$. (Such an i can affect other 'trellis complexities', such as branch complexity and edge complexity, not considered here.) We note that if $\gamma_i(C)$ and $\delta_i(C)$ are respectively the number of PsofG and PsofF before and including i then $\gamma_i(C) = k(C) - k(C_i^+)$ and $\delta_i(C) = k(C_i^-)$, so that

$$s_i(C) = \gamma_i(C) - \delta_i(C).$$

It is well–known that the state complexity of a code and its dual are equal—in fact the dimensions of their vertex spaces at each depth are equal, [5].

1.3. Outline. In Section 2 we consider a family of binary codes defined by Berman in [2]. These codes have defining parameters p, r and m, where p is an odd prime, m and r integers with $m \geq 1$ and $0 \leq r \leq m-1$—we denote such a code $\mathcal{B}(p, r, m)$. Berman used these codes to demonstrate the existence of semisimple abelian codes with better asymptotic performance than any semisimple cyclic codes. Towards this end, he determined their classical code parameters. We show how these codes together with their duals can be considered as a generalisation of $\mathcal{RM}$–codes ($\mathcal{RM}$–codes are the case $p = 2$ and so do not, strictly speaking, belong to the family of $\mathcal{B}$–codes and their duals). We determine the minimum distance of

the dual codes. We also determine the SC of the dual codes and hence the SC of the 'Berman codes'. This SC is greater than might have been expected.

In Section 3 we consider a less well–known family of codes defined in [**4**]. This family generalises $\mathcal{RM}$–codes (this time including them as a special case). These codes are defined over any finite field, $GF(q)$, and have defining parameters n, r and m, where n, m and r are integers with $n \geq 2$, $m \geq 1$ and $0 \leq r \leq m-1$—we denote such a code $\mathcal{DH}_q(n,r,m)$. Thus $\mathcal{DH}$–codes are more numerous than $\mathcal{B}$–codes or their duals. However when both are defined, the $\mathcal{DH}$–codes have poorer classical code parameters than either $\mathcal{B}$–codes or their duals—their poor parameters explaining why $\mathcal{DH}$–codes are less well–known. We determine the SC of $\mathcal{DH}$–codes and hence show that it is these codes that generalise $\mathcal{RM}$–codes with respect to SC.

In Section 4 we introduce a new family codes, defined over any finite field, $GF(q)$, with defining parameters $n \geq 2$, $m \geq 1$, and $0 \leq r \leq m-1$ (as for $\mathcal{DH}$–codes). We denote such a code by $\mathcal{C}_q(n,r,m)$. Their code parameters (including SC) are comparable to those of $\mathcal{B}$–codes, and coincide when both are defined.

When considering the SC of $\mathcal{DH}$– and $\mathcal{C}$–codes, we give a local description of their trellis behaviour, which coincides (and as far as we know was previously unknown) in the case that these codes are $\mathcal{RM}$–codes. From this, we determine recurrence relations for their SCs which generalise those given in [**9**] for $\mathcal{RM}$–codes. From the recurrence relations we determine the SCs. In the case of $\mathcal{RM}$–codes, we believe our derivations to be simpler than those of [**1**] and [**9**].

We summarise the code parameters in Section 5 and in Section 6 we compare the asymptotic performances of the parameters.

2. Berman codes

Berman codes are defined as certain ideals in the ring

$$R_{p,m} = \frac{GF(2)[X_1, \ldots, X_m]}{(X_1^p - 1, \ldots, X_m^p - 1)},$$

where p is an odd prime and m an integer, $m \geq 1$. All such ideals are semisimple, the codes being examples of semisimple abelian codes. For $m = 1$, Berman codes are semisimple cyclic codes. Of course to say that an ideal is a code is to identify a polynomial in the ideal with the codeword of coefficients of monomials in the polynomial (zero coefficients included). Thus Berman codes are binary codes of length p^m. Certainly when considering SC, we need a definite bit–ordering for our code. We take the bit–ordering inherited from the lexicographical ordering of monomials (with $X_1 < \ldots < X_m$) in $R_{p,m}$.

We fix m and for $1 \leq j \leq m$ we put

$$P_p(X_j) = 1 + X_j + X_j^2 + \cdots + X_j^{p-1} \quad \text{and} \quad Q_p(X_j) = X_j + X_j^2 + \cdots + X_j^{p-1}.$$

For $0 \leq r \leq m-1$ we put $G(p,r,m)$ equal to the set of polynomials in $R_{p,m}$ of the form

$$\left(Q_p(X_{j_1}) \cdots Q_p(X_{j_s})\right) \cdot \left(P_p(X_{j_{s+1}}) \cdots P_p(X_{j_m})\right),$$

for some $0 \leq s \leq r$ and arrangement, $(j_1, \ldots, j_n)$, of $(1, \ldots, n)$. Berman shows, [**2**, Theorem 2.2], that for each odd prime p, the code (ideal) generated by $G(p,r,m)$

has dimension,

$$K_1(p,r,m) = \sum_{i=0}^{r} \binom{m}{i} (p-1)^i,$$

and that the check code, which then has dimension,

$$K_2(p,r,m) = p^m - K_1(p,r,m) = \sum_{i=r+1}^{m} \binom{m}{i} (p-1)^i,$$

has minimum distance 2^{r+1}. It is this code that we denote by $\mathcal{B}(p,r,m)$.

The code generated by $G(p,r,m)$—the check code of $\mathcal{B}(p,r,m)$—is also the dual code of $\mathcal{B}(p,r,m)$, since the permutation $\pi(i) = p^m - i$ is in its automorphism group. We denote this code by $\mathcal{B}^\perp(p,r,m)$.

Our initial interest in $\mathcal{B}^\perp(p,r,m)$ was that it has the same SC as $\mathcal{B}(p,r,m)$ (this being true of any code and its dual) and that, unlike $\mathcal{B}(p,r,m)$, we have an explicit description of the codewords of $\mathcal{B}^\perp(p,r,m)$.

For completeness we have also shown,

PROPOSITION 2.1. *The minimum distance of* $\mathcal{B}^\perp(p,r,m)$ *is* p^{m-r}.

Proposition 2.1 can be proved by induction using the fact that $\mathcal{B}^\perp(p,r,m)$ is the direct sum of

$$B_1 = \left\{ \sum_{l=0}^{p-1} f_l(X_1,\ldots,X_{m-1}) \cdot X_m^l : f_0,\ldots,f_{p-1} \in \mathcal{B}^\perp(p,r-1,m-1) \right\}$$

and

$$B_2 = \{ g(X_1,\ldots,X_{m-1}) \cdot P_p(X_m) : g \in \mathcal{B}^\perp(p,r,m-1) \setminus \mathcal{B}^\perp(p,r-1,m-1)^* \}$$

where $\mathcal{B}^\perp(p,r-1,m-1)^* = \mathcal{B}^\perp(p,r-1,m-1) \setminus \{0\}$. (We adopt the convention that $\mathcal{B}^\perp(p,-1,m-1) = \{0\}$ and $\mathcal{B}^\perp(p,m-1,m-1) = GF(2)^{p^{m-1}}$.) That $B_1 \oplus B_2 \subseteq \mathcal{B}^\perp(p,r,m)$ follows from $X_m^l = P_p(X_m) + Q_p(X_m) \cdot X_m^l$ in $R_{p,m}$ and that $B_1 \oplus B_2$ and $\mathcal{B}^\perp(p,r,m)$ have the same dimension is a straightforward counting argument.

2.1. Berman codes and Reed–Muller codes. There is then a strong connection between the classical code parameters of $\mathcal{B}$–codes and their duals (for p an odd prime) and $\mathcal{RM}$–codes (for $p = 2$). We look at another way in which $\mathcal{B}$–, $\mathcal{B}^\perp$– and $\mathcal{RM}$–codes can be thought of as being part of the same family.

In [3] it is noted that $\mathcal{RM}(r,m)$ is equal to the $(m-r)^{th}$ power of the radical of $R_{2,m}$ (which is not a semisimple ring, unlike $R_{p,m}$ for odd p). It is not hard to see that,

PROPOSITION 2.2. *For* $0 \le r \le m-1$, *the* $(m-r)^{th}$ *power of the radical of* $R_{2,m}$ *is generated by* $G(2,r,m)$.

Thus $\mathcal{RM}(r,m)$ and $\mathcal{B}^\perp(p,r,m)$ belong to the same family of codes: those generated by $G(p,r,m)$ for all primes p. (Amongst these codes, the $\mathcal{RM}$–codes are modular abelian codes and the $\mathcal{B}^\perp$–codes are semisimple abelian codes.) A code in this family has dimension $K_1(p,r,m)$ and minimum distance p^{m-r} and its dual has dimension $K_2(p,r,m)$ and minimum distance 2^{r+1}.

2.2. State complexity. The ordering implicit in the ideal description of $\mathcal{RM}$–codes is the (non–cyclic) standard bit–ordering, which has been shown to be optimal with respect their SC in [**6**]. Under this bit ordering it is shown in [**1**] that the SC of $\mathcal{RM}(r,m)$ is $S_1(2,r,m)$ where,

$$S_1(p,r,m) = \sum_{i=0}^{\min\{r,m-r-1\}} \binom{m-2i-1}{r-i} (p-1)^{r-i}.$$

Thus, in view of the close connection between $\mathcal{B}^\perp$–codes and their duals and $\mathcal{RM}$–codes and their duals, it may have been hoped that the SC of $\mathcal{B}^\perp$–codes, and hence the SC of $\mathcal{B}$–codes, would be $S_1(p,r,m)$. However,

PROPOSITION 2.3. *The SC of* $\mathcal{B}(p,r,m)$ *is,*

$$S_2(p,r,m) = \sum_{i=0}^{r} \binom{m-i-1}{r-i} (p-1)^{r-i}.$$

It would seem significant that whilst the dual of an $\mathcal{RM}$–code is an $\mathcal{RM}$–code, the dual of a $\mathcal{B}^\perp$–code is not a $\mathcal{B}^\perp$–code.

The proof of Proposition 2.3 uses an alternative version of Equation (1.1). The i^{th} past *truncated* code of C is $C_-^i = \{(c_0,\dots,c_i) : (c_0,\dots,c_n) \in C\}$ and the i^{th} future *truncated* code of C is $C_+^i = \{(c_{i+1},\dots,c_n) : (c_0,\dots,c_n) \in C\}$. Then $k(C_-^i) = k(C) - k(C_i^+)$ and $k(C_+^i) = k(C) - k(C_i^-)$ so that

$$s_i(C) = k(C_-^i) + k(C_+^i) - k(C). \tag{2.1}$$

For codes C_1 and C_2 with $C_1 \cap C_2 = \{0\}$ it is then straightforward to see that

$$s_i(C_1 \oplus C_2) \le s_i(C_1) + s_i(C_2), \tag{2.2}$$

with equality if $k((C_1)_-^i \cap (C_2)_-^i) = k((C_1)_+^i \cap (C_2)_+^i) = 0$.

Now we take B_1 and B_2 as above and $i = Qp + R$, where $0 \le Q \le p-1$ and $0 \le R \le p^m - 1$. Then

$$k((B_1)_-^i) = Q \cdot k(\mathcal{B}^\perp(p,r-1,m-1)) + k(\mathcal{B}^\perp(p,r-1,m-1)_-^R)$$

and

$$k((B_1)_+^i) = (p-1-Q) \cdot k(\mathcal{B}^\perp(p,r-1,m-1)) + k(\mathcal{B}^\perp(p,r-1,m-1)_+^R)$$

so that from (2.1), $s_i(B_1) = s_R(\mathcal{B}^\perp(p,r-1,m-1))$. Also, with $B = \mathcal{B}^\perp(p,r,m-1) \setminus \mathcal{B}^\perp(p,r-1,m-1)^*$,

$$k((B_2)_-^i) = \begin{cases} k(B_-^R) & \text{if } Q = 0 \\ k(B) & \text{if } Q \ge 1 \end{cases} \quad \text{and} \quad k((B_2)_+^i) = \begin{cases} k(B_+^R) & \text{if } Q = p-1 \\ k(B) & \text{if } Q \le p-2 \end{cases}$$

so that from (2.1), $s_i(B_2) \le k(B)$ with equality if $1 \le Q \le p-2$. Thus noting that if $1 \le Q \le p-2$ then $k((B_1)_-^i \cap (B_2)_-^i) = k((B_1)_+^i \cap (B_2)_+^i) = 0$, we have from (2.2) that

$$s_i(\mathcal{B}^\perp(p,r,m)) \le s_R(\mathcal{B}^\perp(p,r-1,m-1)) + k(B),$$

with equality if $1 \le Q \le p-2$. Thus

LEMMA 2.4. $s(\mathcal{B}^\perp(p,r,m)) = s(\mathcal{B}^\perp(p,r-1,m-1)) + \binom{m-1}{r}(p-1)^r$.

Proposition 2.3 follows from Lemma 2.4 by induction.

Apart from trivial cases, when equality holds, it is straightforward to see that $S_2(p,r,m) > S_1(p,r,m)$. Thus the SC of $\mathcal{B}$–codes would seem disappointing, although in Section 6.2 we see that asymptotically S_2 and S_1 coincide.

The parameters of $\mathcal{B}$– and $\mathcal{B}^\perp$–codes are in Table 1 of Section 5.

3. Dwork–Heller codes

Let n be an integer, $n \geq 1$, $M_{q,n,m}$ the set of monomials in

$$\frac{GF(q)[X_1,\ldots,X_m]}{(X_1^n-1,\ldots,X_m^n-1)}$$

and $R_{q,n,m} = \langle M_{q,n,m} \rangle$, the linear span of $M_{q,n,m}$. For $M \in M_{q,n,m}$, we set

$$P_M = \sum_{M|M',M' \in M_{q,n,m}} M'.$$

If $D_{q,n,m}$ is the set of all such polynomials, then $|D_{q,n,m}| = n^m$ and $\langle D_{q,n,m} \rangle = R_{q,n,m}$. For $0 \leq r \leq m-1$, put

$$H_{q,n,m} = \langle M \in M_{q,n,m} : M \text{ is divisible by at most } r \text{ variables} \rangle.$$

Each polynomial in $H_q(n,r,m)$ is a linear combination of elements of $D_q(n,m)$. The coefficients of each such linear combinations (somehow ordered) are the codewords of $\mathcal{DH}_q(n,r,m)$. Thus $\mathcal{DH}_q(n,r,m)$ is a code of length n^m over $GF(q)$.

For example $H_2(3,0,2) = \{0,1\}$. Now $1 = P_1 + P_{X_1} + P_{X_2} + P_{X_1X_2}$, so $\mathcal{DH}_q(3,0,2)$ is $\{(000000000),(110110000)\}$ (not the repetition code we would want).

These codes were defined in [4], where it was shown that $\mathcal{DH}_q(n,r,m)$, has dimension $K_1(n,r,m)$ and minimum distance 2^{m-r}, and stated that $\mathcal{DH}_2(2,r,m) = \mathcal{RM}(r,m)$. We note that for p an odd prime, $\mathcal{DH}_2(p,r,m)$ has the same number of codewords as $\mathcal{B}^\perp(p,r,m)$ but inferior minimum distance by Proposition 2.1, and that $\mathcal{DH}_2(p,r,m)$ has the same minimum distance as $\mathcal{B}(p,m-r-1,m)$, but fewer codewords.

3.1. Local behaviour of trellis complexities. To consider the SC of $\mathcal{DH}$–codes we need a bit–ordering. Since $\mathcal{DH}_q(n,m)$ is a length n^m code we label our bit positions from 0 to n^m-1 and our trellis depths from -1 to n^m-1. For $0 \leq i \leq n^m-1$ we have the n–expansion of i, $(a_1,\ldots,a_m)$, where $i = \sum_{j=1}^m a_j n^{j-1}$ and $0 \leq a_j \leq n-1$. A codeword is the vector of coefficients of an element of $\langle D_q(n,m) \rangle$. The i^{th} symbol of this codeword is the coefficient of $P_M \in D_q(n,m)$, where $M = X_1^{a_1}\ldots X_m^{a_m}$ and $(a_1,\ldots,a_m)$ is the n–expansion of i. In the case of $\mathcal{RM}$–codes this ordering is the standard bit–ordering.

For $0 \leq a \leq n-1$ we write $|i|_a$ for the number of the a_j in the n–expansion of i equal to a. The following result gives a comprehensive local description of the behaviour of the state (or any of the other usual types of trellis) complexity, which as far as we know was previously unknown for $\mathcal{RM}$–codes.

LEMMA 3.1. *For $0 \leq i \leq n^m-1$,*

1. *i is a PofG of $\mathcal{DH}_q(n,r,m)$ if and only if $|i|_0 \geq m-r$ and*
2. *i is a PofF of $\mathcal{DH}_q(n,r,m)$ if and only if $|i|_1 \geq m-r$.*

We note that for $r \leq m-r-1$ no i is a PofG and PofF (since e. g. if $|i|_0 \geq m-r \geq m-(m-r-1) = r+1$ then $|i|_1 \leq m-r-1$). Also for $n=2$, for $r \geq m-r$, i is a PofG of $\mathcal{DH}_q(2,r,m)$ which is not a PofG of $\mathcal{DH}_q(2,m-r-1,m)$ if and only if $m-(m-r-1)-1 = r \geq |i|_0 \geq m-r$ if and only if $m-r \leq |i|_1 \leq r$ if and only if i is a PofF of $\mathcal{DH}_q(2,r,m)$ which is not a PofF of $\mathcal{DH}_q(2,m-r-1,m)$. This of course ties in with fact that the vertex dimension at each depth of an $\mathcal{RM}(r,m)$ is the same as for its dual, $\mathcal{RM}(m-r-1,m)$. It also shows that the edge complexity of a low–rate $\mathcal{RM}$–code will be less than that of its high–rate dual.

REMARK 3.2. The bit–ordering of $\mathcal{DH}_q(n,r,m)$ described corresponds to the lexicographic ordering of $D_q(n,m)$—in the sense that the coefficient of P_{M_1} comes before that of P_{M_2} in a codeword if and only if $M_1 < M_2$ where $<$ is the lexicographic ordering of monomials. In fact Lemma 3.1 holds for any monomial ordering of $D_q(n,m)$. This is not true of the results in the rest of the section.

Lemma 3.1 makes calculating the dimension of a vertex space at a given depth quite straightforward—we just have to count the i with $|i|_0 \geq m-r$ and $|i|_1 \geq m-r$ that occur before our given depth and subtract the latter from the former. For example, the results of [**5**] and [**7**] on the 4–section and 8–section uniform trellises of $\mathcal{RM}$–codes follow quite easily. However to determine at which depth the difference between these counts is maximised requires some more work.

3.2. Recurrence relations. We derive recurrence relations that generalise those for $\mathcal{RM}$–codes given in [**9**]. In the case of $\mathcal{RM}$–codes our approach would seem to simplify that of [**9**]. For $\mathcal{RM}$–codes we have that

$$s_i(\mathcal{RM}(r,m)) = s_{2^m-2-i}(\mathcal{RM}(r,m))$$

for $-1 \leq i \leq 2^m-1$, (a known fact that is easily deducible from Lemma 3.1) so that it is only necessary to calculate recurrence relations for $-1 \leq i \leq 2^{m-1}-1$. No such identity holds for $\mathcal{DH}$–codes in general. It is the recurrence relations for $n^{m-1} \leq i \leq 2n^{m-1}-1$ that cause difficulty. The cases $i=-1,0$ are trivial. For $i \geq 1$ not in the range $n^{m-1} \leq i \leq 2n^{m-1}-1$ either

1. there is a j, $1 \leq j \leq m-1$, such that $n^{j-1} \leq i \leq 2n^{j-1}-1$ (this being the only case for $\mathcal{RM}$–codes), in which case we get the recurrence relation

$$s_i\left(\mathcal{DH}_q(n,r,m)\right) = s_{i-n^{j-1}}\left(\mathcal{DH}_q(n,r-1,m-2)\right) + s_{n^{j-1}-1}\left(\mathcal{DH}_q(n,r,m)\right),$$

   or

2. there is a j, $1 \leq j \leq m$ and an a, $2 \leq a \leq n-1$, such that $an^{j-1} \leq i \leq (a+1)n^{j-1}-1$, in which case we get the recurrence relation

$$s_i\left(\mathcal{DH}_q(n,r,m)\right) = s_{i-an^{j-1}}\left(\mathcal{DH}_q(n,r-1,m-1)\right) + s_{an^{j-1}-1}\left(\mathcal{DH}_q(n,r,m)\right).$$

(We note that calculating the second terms in the right–hand sides of the recurrence relations is straightforward from Lemma 3.1.)

For $n^{m-1} \leq i \leq 2n^{m-1}-1$ we need some notation. We write $u(l) = \sum_{j=l+1}^{m} n^{j-1}$ and $v(l) = u(m-2) - n^{l-1}$ and $u(l,a) = u(l) + an^{l-1}$ and $v(l,a) = u(m-1) + (a-1)n^{l-1}$ $(v(l,0) \neq v(l))$. Then for i in this range, except $i = \sum_{j=1}^{m} q^{j-1}$ which is always a PofF (and so cannot be a depth at which SC is attained), either

1. there is an l, $1 \leq l \leq m-1$, such that $u(l) \leq i \leq u(l) + n^{l-1}$, in which case

$$s_i\left(\mathcal{DH}_q(n,r,m)\right) - s_{u(l)-1}\left(\mathcal{DH}_q(n,r,m)\right) =$$
$$s_{i-v(l)}\left(\mathcal{DH}_q(n,r-1,m-2)\right) - s_{u(l)-v(l)-1}\left(\mathcal{DH}_q(n,r-1,m-2)\right),$$

or

2. there is an l, $1 \leq l \leq m-1$, and an a, $2 \leq a \leq n-1$, such that $u(l,a) \leq i \leq u(l,a) + n^{l-1}$, in which case

$$s_i\left(\mathcal{D}H_q(n,r,m)\right) - s_{u(l,a)-1}\left(\mathcal{D}H_q(n,r,m)\right) =$$
$$s_{i-v(l,a)}\left(\mathcal{D}H_q(n,r-1,m-1)\right) - s_{u(l,a)-v(l,a)-1}\left(\mathcal{D}H_q(n,r-1,m-1)\right).$$

(Again the terms not dependent on i are quite straightforward to calculate.)

3.3. State complexity. It is possible to inductively determine from the recurrence relations at which depth the SC is attained and the value of the SC. For some $\mathcal{D}H$–codes the depth where the SC is attained is unique and in this case will be in the problem area, $n^{m-1} \leq i \leq 2n^{m-1} - 1$.

We put $[r,m] = m - 2\min\{r, m-r-1\} - 1$. Then,

PROPOSITION 3.3. *The state complexity of $\mathcal{D}H_q(n,r,m)$ is attained at depth with n–expansion,*

$$(\underbrace{n-1,\ldots,n-1}_{[r,m]},\underbrace{0,0,1,0,1,0,1,\ldots,0,1}_{m-[r,m]}).$$

Its value is $S_1(n,r,m)$.

Thus $\mathcal{D}H$–codes can be considered to generalise $\mathcal{R}M$–codes with respect to state complexity.

Again the parameters of $\mathcal{D}H$–codes are in Table 1 of Section 5.

4. A new family of codes

These codes are defined similarly to $\mathcal{D}H$–codes. Again we work in the vector space $R_{q,n,m}$, but with the basis $E_q(n,m)$ of polynomials of the form

$$Q_M = \sum_{M'|M, M' \in M_{q,n,m}} M',$$

and for $0 \leq r \leq m-1$ we put $I_q(n,r,m)$ equal to the linear span of all monomials divisible by at least $r+1$ variables. Then again each polynomial in $I_q(n,r,m)$ is a linear combination of elements of $E_q(n,m)$ and the codewords of the code which we denote $\mathcal{C}_q(n,r,m)$, are the coefficients of such linear combinations.

PROPOSITION 4.1. *$\mathcal{C}_q(n,r,m)$ is an $[n^m, K_2(n,r,m), 2^{r+1}]$ code.*

Thus $\mathcal{C}$–codes are defined as often as $\mathcal{D}H$–codes but have classical code parameters comparable to the superior, but less often defined, $\mathcal{B}$–codes. For $q = n = 2$ we again get the $\mathcal{R}M$–codes, but here $\mathcal{C}_2(2,r,m) = \mathcal{R}M(m-r-1,m)$, the dual of $\mathcal{R}M(r,m)$.

4.1. Local behaviour of trellis complexities. For $\mathcal{C}$–codes, the i^{th} symbol position is the coefficient of Q_M, where $M = X_1^{a_1} \ldots X_m^{a_m}$ and $(a_1,\ldots,a_m)$ is the n–expansion of i $(0 \leq i \leq n^m - 1)$. Again when $\mathcal{C}$–codes are $\mathcal{R}M$–codes we have their standard bit–ordering. We have the following analogue of Lemma 3.1,

LEMMA 4.2. *For $0 \leq i \leq n^m - 1$,*

1. *i is a PofG of $\mathcal{C}_q(n,r,m)$ if and only if $|i|_{n-1} \leq m-r-1$ and*
2. *i is a PofF of $\mathcal{C}_q(n,r,m)$ if and only if $|i|_0 \leq m-r-1$.*

We note that for $\mathcal{RM}(r,m) = \mathcal{C}_2(2, m-r-1, m)$, Lemma 4.2 implies that i is a PofG if and only if $|i|_1 \leq r$ if and only if $|i|_0 \geq m-r$, and that i is a PofG if and only if $|i|_0 \leq r$ if and only if $|i|_1 \geq m-r$, both of which are in agreement with Lemma 3.1. We note also that Lemma 4.2 holds for any monomial ordering of $E_q(n,m)$—c.f. Lemma 3.1 and Remark 3.2.

4.2. Recurrence relations. We quickly get from Lemma 4.2 that, for $-1 \leq i \leq n^m - 1$,

$$s_i\left(\mathcal{C}_q(n,r,m)\right) = s_{n^m-2-i}\left(\mathcal{C}_q(n,r,m)\right),$$

a property of $\mathcal{RM}$–codes not shared in general by $\mathcal{DH}$–codes, as noted in the previous section.

Thus for $\mathcal{C}$–codes, as for $\mathcal{RM}$–codes, we do not need to find recurrence relations for $(n-1)n^{m-1} \leq i \leq n^m - 1$ (the vertex dimensions for these depths being deducible from those for $-1 \leq i \leq n^{m-1} - 2$). We do need to divide all other $i \geq 1$ into two sets though.

For $1 \leq i \leq (n-1)n^{m-1} - 1$ either,

1. there is a j, $1 \leq j \leq m$, and an a, $1 \leq a \leq n-2$, such that $an^{j-1} \leq i \leq (a+1)n^{j-1} - 1$, in which case

$$s_i\left(\mathcal{C}_q(n,r,m)\right) = s_{i-an^{j-1}}\left(\mathcal{C}_q(n,r-1,m-1)\right) + s_{an^{j-1}-1}\left(\mathcal{C}_q(n,r,m)\right),$$

   or

2. there is a j, $1 \leq j \leq m-1$, such that $(n-1)n^{j-1} \leq i \leq n^j - 1$ (this being the only case for $\mathcal{RM}$–codes), in which case

$$s_i\left(\mathcal{C}_q(n,r,m)\right) = s_{i-(n-1)n^{j-1}}\left(\mathcal{C}_q(n,r-1,m-2)\right) + s_{(n-1)n^{j-1}-1}\left(\mathcal{C}_q(n,r,m)\right).$$

(Again the second terms on the right–hand side of these recurrences can be easily calculated from Lemma 4.2.)

4.3. State complexity. It follows quickly by induction from the recurrence relations that

PROPOSITION 4.3. *For $n = 2$ the state complexity of $\mathcal{C}_q(n,r,m)$ is attained at depth with n–expansion*

$$(\underbrace{1,\ldots,1}_{[r,m]},\underbrace{0,0,1,0,1,0,1,\ldots,0,1}_{m-[r,m]}).$$

Its value is $S_1(n,r,m)$.

For $n \geq 3$, the state complexity of $\mathcal{C}_q(n,r,m)$ is attained at all depths with n–expansion $(a_1,\ldots,a_m)$, where $1 \leq a_1,\ldots,a_m \leq n-2$. Its value is $S_2(n,r,m)$.

The parameters of $\mathcal{C}$–codes are in Table 1 of Section 5.

5. Code Parameters

The parameters of the codes discussed are summarised in Table 1. A defining parameter for each code is $m \geq 1$. For the other defining parameters (DPs) we have n, r integers, $n \geq 2$, and $0 \leq r \leq m-1$, p an odd prime and q a power of a prime. The codes are of length p^m, n^m or 2^m according to whether p, n or neither appear as a defining parameter; K_1, K_2, S_1 and S_2 are defined in Section 2.

TABLE 1. Code parameters

Code	DPs	Field	Dimension	Minimum Distance	State Complexity
$\mathcal{RM}$	r	$GF(2)$	$K_1(2,r,m)$	2^{m-r}	$S_1(2,r,m)$
	$m-r-1$	$GF(2)$	$K_2(2,r,m)$	2^{r+1}	$S_1(2,r,m)$
$\mathcal{B}^\perp$	p,r	$GF(2)$	$K_1(p,r,m)$	p^{m-r}	$S_2(p,r,m)$
$\mathcal{B}$	p,r	$GF(2)$	$K_2(p,r,m)$	2^{r+1}	$S_2(p,r,m)$
$\mathcal{DH}$	q,n,r	$GF(q)$	$K_1(n,r,m)$	2^{m-r}	$S_1(n,r,m)$
$\mathcal{C}$	q,n,r	$GF(q)$	$K_2(n,r,m)$	2^{r+1}	$S_1(2,r,m)$ if $n=2$ $S_2(n,r,m)$ if $n\geq 3$

6. Asymptotic analysis

The general theory of asymptotic behaviour of SCs has received some attention (e. g. [**10**] and references given there). However the SCs of few long codes are known and hence little is known about the asymptotic behaviour of SCs for specific families of codes. Here we look at the behaviour of $S_1(n,r,m)$ and $S_2(n,r,m)$ as $m\to\infty$. For r fixed the behaviour is trivial so we want r to increase with m. We fix λ, $0<\lambda<1$, and put $r=\lfloor\lambda m\rfloor$. Our results of course apply to $\mathcal{RM}(\lfloor\lambda m\rfloor,m)$ as a special case.

6.1. Asymptotic comparison of classical code parameters. We know that, for an odd prime p, $\mathcal{B}^\perp(p,\lfloor\lambda m\rfloor,m)$ and $\mathcal{DH}_2(p,\lfloor\lambda m\rfloor,m)$ both have the same number of codewords, but that the former has minimum distance $p^{m-\lfloor\lambda m\rfloor}$, compared with the latter's $2^{m-\lfloor\lambda m\rfloor}$. A non–trivial asymptotic comparison of these minimum distances (one for which both do not either tend to 0 or ∞) is given by

$$\lim_{m\to\infty}\frac{\log_p p^{m-\lfloor\lambda m\rfloor}}{m}=(1-\lambda)>(1-\lambda)\log_p 2=\lim_{m\to\infty}\frac{\log_p 2^{m-\lfloor\lambda m\rfloor}}{m}. \tag{6.1}$$

Thus asymptotically the minimum distance of $\mathcal{B}^\perp$–codes remains superior.

For convenience we introduce the following notation,

$$\begin{aligned}
&\mathcal{DH}_q^\lambda(n,m)=\mathcal{DH}_q(n,\lfloor\lambda m\rfloor,m) && \mathcal{C}_q^\lambda(n,m)=\mathcal{C}_q(n,m-\lfloor\lambda m\rfloor-1,m)\\
&K_1^\lambda(n,m)=K_1(n,\lfloor\lambda m\rfloor,m) && K_2^\lambda(n,m)=K_2(n,m-\lfloor\lambda m\rfloor-1,m)\\
&R_1^\lambda(n,m)=K_1^\lambda(n,m)/q^m && R_2^\lambda(n,m)=K_2^\lambda(n,m)/q^m.
\end{aligned}$$

Thus $\mathcal{DH}_q^\lambda(n,m)$ and $\mathcal{C}_q^\lambda(n,m)$ both have minimum distance $2^{m-\lfloor\lambda m\rfloor}$.

We also put

$$R_i^\lambda(n,\infty)=\lim_{m\to\infty}R_i^\lambda(n,m)$$

for $i=1,2$.

PROPOSITION 6.1. *With the above notation, we have*

$$R_1^\lambda(n,\infty)=\begin{cases}0 & \text{for } 0<\lambda<(n-1)/n\\ 1 & \text{for } (n-1)/n<\lambda<1\end{cases}$$

and

$$R_2^\lambda(n,\infty)=\begin{cases}0 & \text{for } 0<\lambda<1/n\\ 1 & \text{for } 1/n<\lambda<1.\end{cases}$$

Thus for $1/n<\lambda<(n-1)/n$, $\mathcal{C}_q^\lambda(n,m)$ has asymptotic rate 1 whereas $\mathcal{DH}_q^\lambda(n,m)$ has asymptotic rate 0.

CONJECTURE 6.2. *Both* $R_1^{(n-1)/n}(n,\infty)$ *and* $R_2^{1/n}(n,\infty)$ *are equal to* $1/2$.

In fact, for $n \geq 3$, we can also distinguish between the asymptotic performance of $K_1^\lambda(n,m)$ and $K_2^\lambda(n,m)$ for $0 < \lambda < 1/n$ using a $\frac{\log_n}{m}$ comparison similar to Equation (6.1). Explicitly, using the entropy function $H_n(\lambda) = \lambda \log_n(n-1) - \lambda \log_n \lambda - (1-\lambda)\log_n(1-\lambda)$, we have

PROPOSITION 6.3. *For* $0 < \lambda < 1/n < 1/2$,

$$\lim_{m\to\infty} \frac{\log_n K_1^\lambda(n,m)}{m} = H_n(\lambda) < H_n(1-\lambda) = \lim_{m\to\infty} \frac{\log_n K_2^\lambda(n,m)}{m},$$

6.2. Asymptotic SC performance. It is quite straightforward to see that

$$\frac{S_2(n,\lfloor\lambda m\rfloor,m)}{m} \geq \frac{S_1(n,\lfloor\lambda m\rfloor,m)}{m} \longrightarrow \infty \text{ as } m \longrightarrow \infty$$

and that

$$0 \leq \frac{S_1(n,\lfloor\lambda m\rfloor,m)}{n^m} \leq \frac{S_2(n,\lfloor\lambda m\rfloor,m)}{n^m} \longrightarrow 0 \text{ as } m \longrightarrow \infty.$$

Thus neither of these provides a substantial comparison of the asymptotic performance of the SCs and so we look at the more subtle $\frac{\log_n}{m}$ comparison, used above.

PROPOSITION 6.4. *For* $0 < \lambda < 1$,

$$\lim_{m\to\infty} \frac{\log_n S_1(n,\lfloor\lambda m\rfloor,m)}{m} = H_n(\lambda) = \lim_{m\to\infty} \frac{\log_n S_2(n,\lfloor\lambda m\rfloor,m)}{m}.$$

Thus the $\frac{\log_n}{m}$ comparison fails to distinguish between the asymptotic performances of the SCs of $\mathcal{D}H_2(p,r,m)$ and the superior $\mathcal{B}^\perp(p,r,m)$.

Writing $S_1^\lambda(n,m)$ and $S_2^\lambda(n,m)$ for the SCs of $\mathcal{D}H_q^\lambda(n,m)$ and $\mathcal{C}_q^\lambda(n,m)$ respectively, we have

COROLLARY 6.5. *For* $0 < \lambda < 1$,

$$\lim_{m\to\infty} \frac{\log_n S_1^\lambda(n,m)}{m} = H_n(\lambda) \quad \textit{and} \quad \lim_{m\to\infty} \frac{\log_n S_2^\lambda(n,m)}{m} = H_n(1-\lambda).$$

Thus for $n \geq 3$, $\mathcal{D}H_q^\lambda(n,m)$ has asymptotically lower SC for $\lambda < 1/2$ but the superior $\mathcal{C}_q^\lambda(n,m)$ has asymptotically lower SC for $\lambda > 1/2$.

Acknowledgements. The authors gratefully acknowledge financial support from the U. K. Engineering and Physical Sciences Research Council. The first author was supported by the EPSRC.

References

[1] Y. Berger, Y. Be'ery, *Bounds on the trellis size of linear block codes,* IEEE Trans. Information Theory **39**, 203–209.

[2] S. D. Berman, *Semisimple cyclic and abelian codes II,* Kibernetika **3**, 21–30.

[3] ———, *On the theory of group codes,* Kibernetika **3**, 31–39.

[4] B. M. Dwork, R. M. Heller, *Results of a geometric approach to the theory and construction of non-binary multiple error and failure correcting codes,* IRE Nat. Conv. Rec., 123–129.

[5] G. D. Forney, *Coset codes—Part II: Binary lattices and related codes,* IEEE Trans. Information Theory **34** (1988), 1152–1187.

[6] T. Kasami, T. Takata, T. Fujiwara, S. Lin, *On the optimum bit orders with respect to state complexity of trellis diagrams for binary linear codes,* IEEE Trans. Information Theory **39** (1993), 242–245.

[7] ———, *On complexity of trellis structure of linear block codes,* IEEE Trans. Information Theory **39** (1993), 1057–1064.

[8] A. B. Kiely, S. J. Dolinar, R. J. McEliece, L. L. Ekroot, W. Lin, *Trellis decoding complexity of linear block codes,* IEEE Trans. Information Theory **42** (1996), 1687–1697.

[9] C. Lu, S. Huang, *On bit-level trellis complexity of Reed-Muller codes,* IEEE Trans. Information Theory **41** (1995), 2061–2064.

[10] A. Lafourcade, A. Vardy, *Lower bounds on trellis complexity of block codes,* IEEE Trans. Information Theory **41** (1995), 1938–1954.

[11] D. J. Muder, *Minimal trellises for block codes,* IEEE Trans. Information Theory **34** (1988), 1049–1053.

[12] J. K. Wolf, *Efficient maximum likelihood decoding of linear block codes using a trellis,* IEEE Trans. Information Theory **24**(1978), 76–80.

ALGEBRAIC CODING RESEARCH GROUP, CENTRE FOR COMMUNICATIONS RESEARCH, UNIVERSITY OF BRISTOL, ENGLAND

E-mail address: Tim.Blackmore@Bristol.ac.uk

ALGEBRAIC CODING RESEARCH GROUP, CENTRE FOR COMMUNICATIONS RESEARCH, UNIVERSITY OF BRISTOL, ENGLAND

E-mail address: Graham.Norton@Bristol.ac.uk

Contemporary Mathematics
Volume **225**, 1999

ID-Based Key Distribution System over an Elliptic Curve

Hisao Sakazaki Eiji Okamoto Masahiro Mambo

Japan Advanced Institute of Science and Technology
1-1 Asahidai, Tatsunokuchi, Nomi, Ishikawa, 923-12, Japan

Abstract

A key distribution system is a system in which users securely generate a common key. One kind of identity-based key distribution system was proposed by E. Okamoto[1]. Its security depends on the difficulty of factoring a composite number of two large primes like RSA public-key cryptosystem.

On the other hand, Koblitz and Miller described how the group of points on an elliptic curve over a finite field can be used to construct a public key cryptosystem.

In this paper, we propose an ID-based key distribution system over an elliptic curve, as well as over the ring Z/nZ. We show that the system over an elliptic curve is more suitable for the implementation than that over the ring Z/nZ.

1 Introduction

A key distribution system is a system in which users securely generate a common key. The ID-based key distribution system called ID-KDS, is a key distribution system such that public keys used for key distribution are generated from ID information. It is a promising key distribution system since the ID-KDS can be used not only for key distribution but also for authentication. There are a lot of reports about ID-KDS constructed on the ring Z/nZ.

1991 *Mathematics Subject Classifications.* Primary 94A60; Secondary 14H52.

© 1999 American Mathematical Society

In 1986, E. Okamoto proposed an ID-based key distribution system whose security depends on the difficulty of factoring a composite number of two large primes like RSA public-key cryptosystem.

On the other hand, Koblitz and Miller found how a group of points on an elliptic curve over a finite field could be used to construct public key cryptosystems. Compared with ID-KDS constructed on the ring Z/nZ, little is known on ID-KDS constructed on elliptic curves.

In this paper we study whether the ID-KDS proposed by E. Okamoto can be constructed on an elliptic curve or not. The original ID-KDS cannot be constructed on the elliptic curve in a straightforward way. This is because the point corresponding to the user's identity ID cannot be defined on the elliptic curve. As a solution to this problem, we propose a new ID-KDS on an elliptic curve.

The new scheme can be also constructed on the ring Z/nZ. We compare the new scheme on the elliptic curve with that on the ring Z/nZ. The order of the optimal basepoint in the former scheme is almost four times as much as the order of the optimal basepoint in the latter scheme. Thus, the proposed scheme over an elliptic curve is more suitable for implementation than that over the ring Z/nZ.

This paper is organized as follows. Section 2 summarizes original ID-KDS[1]. Section 3 discusses original ID-KDS over an elliptic curve. Section 4 summarizes a new ID-KDS over an elliptic curve. Section 5 compares the new scheme over $E_n(a, b)$ with that over Z/nZ.

2 Original ID-based Key Distribution System

This section summarizes the original ID-KDS[1]. This system consists of three phases. The first phase is called generation phase of information. The second one is called participation phase. The last one is called generation phase of common key.

Generation phase of information

Let n be a product of primes p and q. Let $e \in Z_n^*$ be a public key of the center satisfying $gcd(e, \varphi(n)) = 1$, where $\varphi(n) = (p-1)(q-1)$. Let $d \in Z_n^*$ be a secret key of the center satisfying $ed \equiv 1 \ mod \ \varphi(n)$. Let $g \in Z_n^*$ be a basepoint.(An alternative notation for Z_n used in the literature is Z/nZ.)

Then the key center publishes n, e and g, and secrets d.

Participation phase

Let ID_i be the identity of user i. For the sake of brevity, we will write ID_A, which is the abbreviation for $h(ID_A)$, where h is a cryptographically secure one-way hash function. Let s_i be a secret key of user i satisfying

$$s_i^e \cdot ID_i \equiv 1 \ mod \ n.$$

The key center sends (ID_i, s_i) to user i, when user i participates in the network.

Generation phase of a common key

We assume here that both Alice and Bob wish to obtain their common key.

First, Alice chooses a random number $r_A \in Z_n^*$, and then she computes

$$c_A \equiv s_A \cdot g^{r_A} \ \ mod \ \ n,$$

and sends c_A to Bob. Similarly Bob chooses a random number $r_B \in Z_n^*$, and then he computes

$$c_B \equiv s_B \cdot g^{r_B} \ \ mod \ \ n,$$

and sends c_B to Alice.

Next, she computes

$$K_{AB} \equiv (ID_B \cdot {c_B}^e)^{r_A} \ \ mod \ \ n.$$

Similarly he computes

$$K_{BA} \equiv (ID_A \cdot {c_A}^e)^{r_B} \ \ mod \ \ n.$$

Then $K_{AB} = K_{BA}$, since

$$\begin{aligned} K_{AB} &\equiv (ID_B \cdot {c_B}^e)^{r_A} \\ &\equiv (ID_B \cdot {s_B}^e \cdot g^{r_B \cdot e})^{r_A} \\ &\equiv g^{e \cdot r_A \cdot r_B} \\ &\equiv K_{BA} \qquad\qquad (mod \ \ n). \end{aligned}$$

3 Original ID-KDS over an Elliptic Curve

In 1993 Menezes, Okamoto and Vanstone[6] presented a new cryptanalysis for a set of elliptic curves named supersingular. Their idea is due to Weil pairing, by which elliptic curve discrete logarithm problems can be reduced to discrete logarithm problems over some extension field of

underlying field. Thus elliptic curve discrete logarithm problems over supersingular curves can be solved in sub-exponential-time algorithm.

On the other hand, Smart[9] as well as Satoh and Araki[10] announced independently another type of cryptanalysis in 1997, which is effective only for anomalous elliptic curves. Their algorithm terminates within a polynomial-time.

Thus supersingular elliptic curves and anomalous elliptic curves should not be chosen for implementation.

In this section, we discuss the original ID-KDS over an elliptic curve.

Generation phase of information

Let n be a product of primes p and q. Let $a, b \in Z_n$ be two parameters satisfying $4a^3 + 27b^2 \neq 0 \ mod\ n$. An elliptic curve over Z/nZ with parameters a and b is defined as a set of points (x, y) with $x, y \in Z_n$ satisfying $y^2 \equiv x^3 + ax + b \ mod \ n$ together with a special element, called the point at infinity. Such a curve is denoted $E_n(a, b)$. Let $\mathbf{G} \in E_n(a, b)$ be a basepoint, and $e \in Z_n$ be a public key of the Center satisfying $gcd(e, k) = 1$, where $k = lcm(\#E_p(a, b)\ ,\ \#E_q(a, b))$. Let $d \in Z_n$ be a secret key of the Center satisfying $ed \equiv 1 \ mod\ k$. The key center publishes $E_n(a, b), e$ and $\mathbf{G}$.

Participation phase

In this phase, we need a user's secret key corresponding to the antecedent secret key: $s \equiv ID^{-d} \ mod\ n$. To sum up, we wish to define a point $\mathbf{P}_{ID} \in E_n(a, b)$ corresponding to the user's identity ID. The simplest correspondence is the following one.

$$ID_i \Leftrightarrow \mathbf{P}_{ID_i} = (x, y) = (ID_i, ?)$$

So let the x-coordinate of $\mathbf{P}_{ID_i}$ correspond to ID_i. However a problem will occur. The problem is whether its point $\mathbf{P}_{ID_i}$ is a point on the elliptic curve or not. The probability that $ID_i^3 + aID_i + b$ is a quadratic residue $(mod\ n)$, is about $\frac{1}{4}$. For simplicity, assume that $\mathbf{P}_{ID_i} = (ID_i, Y_i)$ is on the elliptic curve, and we shall call it the ID-point in this paper. Then let $\mathbf{S}_i$ be a secret key of user i satisfying $\mathbf{S}_i = -d \cdot \mathbf{P}_{ID_i}\ over\ E_n(a, b)$. The key center sends $((ID_i, Y_i), \mathbf{S}_i)$ to user i.

Generation phase of a common key

We assume here that both Alice and Bob wish to obtain their common key.

First, Alice chooses a random number $r_A \in Z_n^*$, and then she computes

$$\mathbf{C}_A = \mathbf{S}_A + r_A \cdot \mathbf{G} \quad over \quad E_n(a, b),$$

and she sends $(\mathbf{C}_A, Y_A)$ to Bob. Similarly Bob chooses a random number $r_B \in Z_n^*$, and then he computes

$$\mathbf{C}_B = \mathbf{S}_B + r_B \cdot \mathbf{G} \quad over \quad E_n(a, b),$$

and he sends $(\mathbf{C}_B, Y_B)$ to Alice.

Next, Alice finds the Bob's ID-point $\mathbf{P}_{ID_B}$, and computes

$$\mathbf{K}_{AB} = r_A \cdot (e \cdot \mathbf{C}_B + \mathbf{P}_{ID_B}) \quad over \quad E_n(a, b).$$

Similarly Bob finds the Alice's ID-point $\mathbf{P}_{ID_A}$, and computes

$$\mathbf{K}_{BA} = r_B \cdot (e \cdot \mathbf{C}_A + \mathbf{P}_{ID_B}) \quad over \quad E_n(a, b).$$

Then $\mathbf{K}_{AB} = \mathbf{K}_{BA}$, since

$$\begin{aligned} \mathbf{K}_{AB} &= r_A \cdot (e \cdot \mathbf{C}_B + \mathbf{P}_{ID_B}) \\ &= r_A \cdot (e \cdot (-d \cdot \mathbf{P}_{ID_B} + r_B \cdot \mathbf{G}) + \mathbf{P}_{ID_B}) \\ &= r_A \cdot (-\mathbf{P}_{ID_B} + e \cdot r_B \cdot \mathbf{G} + \mathbf{P}_{ID_B}) \\ &= e \cdot r_A \cdot r_B \cdot \mathbf{G} \\ &= \mathbf{K}_{BA} \qquad over \quad E_n(a, b). \end{aligned}$$

However Bob cannot find the Alice's ID-point $\mathbf{P}_{ID_A}$ without Y_A. So she has to send Y_A to Bob. It is not preferable to transfer large data. We realize it is difficult to construct the original ID-KDS on an elliptic curve in a straightforward way. Therefore we propose a new scheme suitable for implementation on an elliptic curve.

4 The New ID-KDS over an Elliptic Curve

This section summarizes a new ID-KDS over an elliptic curve.

Generation phase of information

Similarly, the key center publishes $E_n(a, b)$ and $\mathbf{G}$ as in the previous section. This scheme need not generate, both the center's public key e and the center's secret key d. The center's secret information is p, q and k, where $k = lcm(\#E_p(a, b), \#E_q(a, b))$.

Participation phase

Let $\mathbf{S}_i$ be a secret key of user i satisfying

$$\mathbf{S}_i = -ID_i^{-1} \cdot \mathbf{G} \quad over \quad E_n(a, b),$$

where $ID_i \cdot ID_i^{-1} \equiv 1 \ mod \ k$. The key center sends $(ID_i, \mathbf{S}_i)$ to user i.

Generation phase of a common key

We assume here that both Alice and Bob wish to obtain their common key.

First, Alice chooses a random number $r_A \in Z_n^*$, and then she computes

$$\mathbf{C}_A = \mathbf{S}_A + r_A \cdot ID_B \cdot \mathbf{G} \quad over \quad E_n(a, b),$$

and sends $\mathbf{C}_A$ to Bob. Similarly Bob chooses a random number $r_B \in Z_n^*$, and then he computes

$$\mathbf{C}_B = \mathbf{S}_B + r_B \cdot ID_A \cdot \mathbf{G} \quad over \quad E_n(a, b),$$

sends $\mathbf{C}_B$ to Alice.

Next, Alice computes

$$\mathbf{K}_{AB} = r_A \cdot (ID_B \cdot \mathbf{C}_B + \mathbf{G}) \quad over \quad E_n(a, b).$$

Similarly Bob computes

$$\mathbf{K}_{BA} = r_B \cdot (ID_A \cdot \mathbf{C}_A + \mathbf{G}) \quad over \quad E_n(a, b).$$

Then $\mathbf{K}_{AB} = \mathbf{K}_{BA}$, since

$$\begin{aligned}
\mathbf{K}_{AB} &= r_A \cdot (ID_B \cdot \mathbf{C}_B + \mathbf{G}) \\
&= r_A \cdot (ID_B \cdot (\mathbf{S}_B + r_B \cdot ID_A \cdot \mathbf{G}) + \mathbf{G}) \\
&= r_A \cdot (ID_B \cdot (-ID_B^{-1} \cdot \mathbf{G} + r_B \cdot ID_A \cdot \mathbf{G}) + \mathbf{G}) \\
&= r_A \cdot (-\mathbf{G} + r_B \cdot ID_A \cdot ID_B \cdot \mathbf{G} + \mathbf{G}) \\
&= r_A \cdot r_B \cdot ID_A \cdot ID_B \cdot \mathbf{G} \\
&= \mathbf{K}_{BA} \qquad over \quad E_n(a, b).
\end{aligned}$$

This scheme is preferable, because we don't require the ID-point $\mathbf{P}_{ID}$.

5 The Comparison between the New Scheme over $E_n(a, b)$ and over Z/nZ

5.1 The new scheme over Z/nZ

This section summarize the new scheme over Z/nZ. Let n be product of primes p and q, and let $g \in Z_n^*$ be a basepoint.

In the generation phase of information, the key center publishes n and g.

In the participation phase, let s_i be a secret key of user i satisfying $s_i \equiv g^{-ID_i^{-1}} \ mod\ n$, where $ID_i \cdot ID_i^{-1} \equiv 1 \ mod\ \varphi(n)$. The key center sends (ID_i, s_i) to user i.

In the generation phase of a common key, first, Alice chooses a random number $r_A \in Z_n^*$, and then she computes $c_A \equiv s_A \cdot g^{r_A \cdot ID_B} \ mod\ n$, and sends c_A to Bob. Similarly Bob chooses a random number $r_B \in Z_n^*$, and then he computes $c_B \equiv s_B \cdot g^{r_B \cdot ID_A} \ mod\ n$, and sends c_B to Alice.

So, Alice and Bob can compute

$$\begin{aligned} K_{AB} &\equiv (c_B{}^{ID_B} \cdot g)^{r_A} \\ &\equiv ((s_B \cdot g^{r_B \cdot ID_A})^{\cdot ID_B} \cdot g)^{r_A} \\ &\equiv ((g^{-ID_B^{-1}} \cdot g^{r_B \cdot ID_A})^{\cdot ID_B} \cdot g)^{r_A} \\ &\equiv ((g^{(-ID_B^{-1} + r_B \cdot ID_A)})^{\cdot ID_B} \cdot g)^{r_A} \\ &\equiv (g^{(-1 + r_B \cdot ID_A \cdot ID_B)} \cdot g)^{r_A} \\ &\equiv g^{r_A \cdot r_B \cdot ID_A \cdot ID_B} \\ &\equiv K_{BA} \qquad (mod\ \ n). \end{aligned}$$

5.2 Difficulty of Breaking

In this section, we study the relationship between the new-ID-KDS over Z/nZ and the Diffie-Hellman key exchange scheme constructed on the ring Z/nZ with respect to the security.

Definition 1

Define by $NEW(n,\ g,\ ID_A,\ ID_B,\ c_A,\ c_B)$ a function that on input $n \in N_{>1}$, $g \in Z_n^*$, $ID_A \in Z_{\phi(n)}^*$, $ID_B \in Z_{\phi(n)}^*$, $c_A \in Z_n^*$, $c_B \in Z_n^*$, outputs $C \in Z_n^*$ such that $C \equiv (c_B^{ID_B} \cdot g)^{r_A} \equiv (c_A^{ID_A} \cdot g)^{r_B} \equiv g^{r_A \cdot r_B \cdot ID_A \cdot ID_B} \ mod\ n$, where $c_A \equiv g^{-ID_A^{-1}} \cdot g^{r_A \cdot ID_B} \ mod\ n$, where $c_B \equiv g^{-ID_B^{-1}} \cdot g^{r_B \cdot ID_A} \ mod\ n$, and if such a C exists.

Definition 2

Define by $DH(n,\ g,\ A,\ B)$ a function that on input $n \in N_{>1}$, $g \in Z_n^*$, $A \in Z_n^*$, $B \in Z_n^*$, outputs $C \in Z_p^*$ such that $C \equiv g^{r_A \cdot r_B} \ mod\ n$, where $A \equiv g^{r_A} \ mod\ n$, $B \equiv g^{r_B} \ mod\ n$, if such a C exists.

Definition 3

For functions F and G, if there exists a polynomial-time computable function h such that $F(x) = G(h(x))$, then we say that F reduces to G

with respect to the polynomial-time many-one reducibility, and write $F \leq_m^p G$. If the converse reduction also holds, we write $F \equiv_m^p G$.

Theorem

Suppose Alice and Bob generate a common key using either the new scheme or the Diffie-Hellman scheme, and a forger tries to masquerade as Alice.

If the forger can obtain the common key of Alice and Bob in time polynomial without knowledge of the secret keys of Alice in the new scheme, then so he can in the Diffie-Hellman scheme.

The converse is also true. Therefore,

$$NEW \equiv_m^p DH.$$

Proof

$NEW \leq_m^p DH$:

$$NEW(n,\ g,\ ID_A,\ ID_B,\ c_A,\ c_B) = DH(n,\ g^{ID_A \cdot ID_B},\ c_A^{ID_A} \cdot g,\ c_B^{ID_B} \cdot g).$$

$DH \leq_m^p NEW$:

$$DH(n,\ g,\ A,\ B) = NEW(n,\ g,\ 1,\ 1,\ A \cdot g^{-1},\ B \cdot g^{-1}).$$

q.e.d.

5.3 The comparison between the new scheme over $E_n(a, b)$ and over Z/nZ

In this section, we compare the new scheme over $E_n(a, b)$ with one over Z/nZ

In the latter scheme, the user's secret key is

$$s_i \equiv g^{-ID_i^{-1}} \ mod\ n.$$

Therefore, the necessary condition for the secret key is

$$gcd(ID_i, \varphi(n)) = 1.$$

However, since $\varphi(n) = (p-1)(q-1)$, if ID_i is even, we cannot generate the secret key. Hence, the order of the optimal basepoint is $\frac{\varphi(n)}{4} =$

$\frac{(p-1)(q-1)}{4} = p'q' < pq$, where $p-1 = 2p', q-1 = 2q'$ ($p, q, p', q'$are primes).

On the other hand, in former scheme, the key center can choose an elliptic curve E_p (E_q) which has prime elements. Namely, the order of the optimal basepoint can be $\#E_p \cdot \#E_q > n = pq$. To sum up, the order of the optimal basepoint has increased by 4 times.

In this point, the new scheme over an elliptic curve is more suitable for implementation than that over the ring Z/nZ.

6 Conclusion

In this paper, we have proposed the new schemes and have shown the following results.

It is difficult to construct the original ID-KDS over an elliptic curve in a straightforward way.

The new scheme over an elliptic curve is more suitable for implementation than that on the ring Z/nZ.

7 Acknowledgments

I would like to thank Dr. T.Uyematsu for his helpful advice.

References

[1] E. Okamoto, "An Introduction to the Theory of Cryptography", Kyoritsu Shuppan, 1993.

[2] J.H. Silverman, J. Tate, "Rational Points on Elliptic Curves", Springer-Verlag, 1994.

[3] K. Koyama, U.M. Maurer, T. Okamoto and S. Vanstone, "New public-keyschemes based on elliptic curves over the ring Z_n", *Advances in Cryptology-Crypto*'91, LNCS 576, Springer-Verlag, pp.252-266, 1991.

[4] H. Tanaka, "Identity-Based Non-Interactive Key Sharing Scheme and Its Application to Some Cryptographic Systems", SCIS'94-3D, 1994.

[5] T. Matsumoto, H. Imai, "Key Predistribution System", *The transactions of the institute of electronics information and communication engineers,* Vol.J71-A, No.11, pp2046-2053, 1988.

[6] A. Menezes, T. Okamoto and S. Vaston, "Reducing elliptic curve logarithms to logarithms in a finite field", *Proceedings of 22nd Annual ACM Symposium on the Theory of Computing,* ACM Press, pp.80-89, 1991.

[7] N. Koblitz, "A Course in number theory and cryptocraphy", Springer-Verlag, 1987.

[8] W. Jonge, D. Chaum, "Some Variations on RSA Signatures & their Security", *Advances in Cryptology-Crypto'86,* LNCS 263, Springer-Verlag, pp.49-59, 1986.

[9] N.P. Smart, "The discrete logarithm problem on elliptic curves of trace one", preprint, 1997.

[10] T. Satoh, K. Araki, "Fermat quotients and the polynomial time discrete log algorithm for anomalous elliptic curves", preprint,

Contemporary Mathematics
Volume **225**, 1999

Symmetric Sets of Curves and Combinatorial Arrays

Ryoh Fuji-Hara and Satoshi Shinohara

ABSTRACT. Let V be an algebraic curve. Let $\mathcal{P}$ be a set of points on V. Let $\mathcal{C}$ be a set of curves each of which intersects V at some points of $\mathcal{P}$. We denote $I_P(C,V)$ as the intersection multiplicity of $C \in \mathcal{C}$ with V at the point $P \in \mathcal{P}$. If $(V,\mathcal{P},\mathcal{C})$ satisfies the following conditions, we call it a *symmetric set of curves*:
(1) for any point $p \in \mathcal{P}$, the number of $\mathcal{C}$ having intersection multiplicity a is a constant λ_a independent of p,
(2) for any ordered pair (p,q) points of $\mathcal{P}$, the number of curves $C \in \mathcal{C}$ is equal to a constant $\lambda_{a,b}$ independent of (p,q) satisfying $I_p(C,V) = a$ and $I_q(C,V) = b$.

When we arrange the multiplicities in an array of size $|\mathcal{C}| \times |\mathcal{P}|$, we have a combinatorial array called a *balanced array.*

We show a general construction of a symmetric set of curves using the Riemann-Roch theorem. We also consider a case that V is an elliptic curve and $\mathcal{C}$ is a set of conics. We show, in this case, the problem is reduced to finding a set $\mathcal{P}$ of points which is the intersection of V and a curve of degree 4 derived from V.

1. Introduction

Let K be a field and V a curve defined by an equation $v(\boldsymbol{x}) = 0$. If $v \in K[\boldsymbol{x}]$ then V is said to be *defined over* K, and denoted by V/K. We denote the intersection multiplicity of V with a curve C at p by $I_p(C,V)$. Let $\mathcal{P}$ be a finite set of points on V and $\mathcal{C}$ a finite set of curves.

DEFINITION 1.1. A *symmetric set of curves* is a triple $(V,\mathcal{P},\mathcal{C})$ which satisfies the following two conditions:

- for any point $p \in \mathcal{P}$, the number of curves of $\mathcal{C}$ having intersection multiplicity a at p is exactly λ_a, and
- for any ordered pair (p,q) of distinct points of $\mathcal{P}$, the number of curves $C \in \mathcal{C}$ satisfying $I_p(C,V) = a$ and $I_q(C,V) = b$ is equal to $\lambda_{a,b}$.

Note that $\lambda_{a,b} = \lambda_{b,a}$. We call V the *base curve.*

Let $\mathcal{P} = \{p_1, \cdots, p_n\}$ and $\mathcal{C} = \{C_1, \cdots, C_m\}$. If $(V,\mathcal{P},\mathcal{C})$ is a symmetric set of curves, an $m \times n$ combinatorial array $[a_{ij}]$, $a_{ij} = I_{p_j}(V, C_i)$ is called a *balanced array* [**1, 2, 4, 8**]. A Balanced array may be called a *partial* or *generalized orthogonal array.* An *orthogonal array* is a balanced array with $\lambda_{a,b} = \lambda$.

1991 *Mathematics Subject Classification.* 05B99,11G20,11G05.

© 1999 American Mathematical Society

To construct a symmetric set of curves, we apply a vector space of rational functions over a finite field. We suppose in this paper that the base curve V is defined over a finite field.

Notation and definitions in this paper are due to [**5, 6**]. Let F_q be a finite field of order q and $\bar{F}_q$ the algebraic closure of F_q. A point whose coordinates lie in F_q is called a F_q-*rational* point. A *divisor* D on a curve V is a formal sum of $\bar{F}_q$-rational points

$$D = \sum_{p \in V} n_p p,$$

where $n_p \in \mathbf{Z}$ and $n_p = 0$ for all but finitely many $p \in V$. The addition of two divisors is $\sum n_p p + \sum m_p p = \sum (n_p + m_p)p$. The support of D, denoted by Supp D, is the set of points with $n_p \neq 0$. If $n_p \geq 0$ for all $p \in V$ then the divisor is said to be *effective*. The *degree* of D is the integer $\deg D = \sum n_p$.

Let $v \in F_q[\boldsymbol{x}]$ and suppose V is defined by an equation $v(\boldsymbol{x}) = 0$. The *function field* $F_q(V)$ of V over F_q is the field of fractions of the integral domain $F_q[\boldsymbol{x}]/(v)$, where (v) denotes the ideal in $F_q[\boldsymbol{x}]$ generated by v. Similarly, $\bar{F}_q(V)$ is the field of fractions of $\bar{F}_q[\boldsymbol{x}]/(v)$. The elements of $\bar{F}_q(V)$ are called *rational functions*. A non-zero rational function f is said to be *defined at* a point $p \in V$ if there exists a representation $f = g/h, g, h \in \bar{F}_q(V)$ such that $h(p) \neq 0$. If f is not defined at p then we write $f(p) = \infty$. For any $f \in \bar{F}_q(V)$ and $p \in V$, f can be written by $f = u^d s$, where $u, s \in \bar{F}_q(V)$ such that $u(p) = 0$ and $s(p) \neq 0, \infty$. The integer d is said to be the *order of* f *at* p, and denoted by $\mathrm{ord}_p(f)$. The divisor $\mathrm{div}(f)$ of a rational function f is $\sum_p \mathrm{ord}_p(f) \cdot p$.

Let $\mathrm{Aut}(\bar{F}_q/F_q)$ be the Galois group of $\bar{F}_q$ over F_q. We define $p^\sigma = (\sigma(a_0) : \sigma(a_1) : \cdots : \sigma(a_n))$ and $D^\sigma = \sum n_p \sigma(p)$, where $\sigma \in \mathrm{Aut}(\bar{F}_q/F_q)$ and $p = (a_0 : a_1 : \cdots : a_n)$. If a divisor $D = n_1 p_1 + \cdots + n_s p_s$ satisfies: (1) there exists a finite extension F_{q^m} of F_q such that each p_i is a F_{q^m}-rational point, and (2) $D^\sigma = D$ for any $\sigma \in \mathrm{Aut}(\bar{F}_q/F_q)$, then D is called a *rational divisor over* F_q.

Let $F_q(V)$ be the function field of V over F_q and $L(D) = \{f \in F_q(V) : \mathrm{div}(f) + D \geq 0 \text{ or } f \equiv 0\}$. If D is a rational divisor over F_q then $L(D)$ is a vector space over F_q. The next result is well-known.

RESULT 1.2. If $\deg D < 0$ then $L(D) = \{0\}$.

From the Riemann-Roch theorem, we have the following result.

RESULT 1.3. Let V be a curve of the genus g defined over a finite field F_q. Let D be a rational divisor over F_q on a curve V. If $\deg D > 2g - 2$ then $l(D) = \deg D + 1 - g$, where $l(D)$ is the dimension of $L(D)$.

In the next section, we show a general construction of symmetric sets of curves using the Riemann-Roch theorem.

2. Symmetric sets of curves

We suppose in this section that V is defined over F_q and D is a rational divisor over F_{q^m}. Let $L(D)^* = L(D) \setminus \{0\}$.

THEOREM 2.1. *Let V be a non-singular curve with the genus $g = 0$. Let D be an effective divisor on V and W a curve such that* $\mathrm{div}(W) \geq D$. *If* $\mathcal{P} = \bigcup(\mathrm{Supp}\ (\mathrm{div}(f)) \setminus \mathrm{Supp}\ (\mathrm{div}(W)))$ *for all* $f \in L(D)^*$ *then* $(V, \mathcal{P}, \mathcal{C})$ *is a symmetric set of curves, where* $\mathcal{C} = \{f \cdot W : f \in L(D)^*\}$.

PROOF. For any $f \in L(D)$, $f \cdot W$ is a curve since

$$\operatorname{div}(f \cdot W) = \operatorname{div}(f) + \operatorname{div}(W) = \operatorname{div}(f) + D + \operatorname{div}(W) - D \geq 0.$$

Suppose $\operatorname{div}(f) = \alpha p + \beta q + R_1$ for any distinct two points $p, q \in \mathcal{P}$ such that $p, q \notin \operatorname{Supp} R_1$. Then we have

$$\operatorname{div}(f \cdot W) = \operatorname{div}(f) + \operatorname{div}(W) = \alpha p + \beta q + R_2 \ , \ p, q \notin \operatorname{Supp} R_2$$

since $p, q \notin \operatorname{Supp}(\operatorname{div}(W))$. Therefore the intersection multiplicity $I_p(f \cdot W)$ is equal to the order $\operatorname{ord}_p(f)$, moreover we have

$$|\{f \cdot W : I_p(f \cdot W, V) = \alpha, f \in L(D)^*\}| = |\{f \in L(D)^* : \operatorname{ord}_p(f) = \alpha\}|$$

and

$$\begin{aligned} & |\{f \cdot W : I_p(f \cdot W, V) = \alpha, I_q(f \cdot W, V) = \beta, f \in L(D)^*\}| \\ = \ & |\{f \in L(D)^* : \operatorname{ord}_p(f) = \alpha, \operatorname{ord}_q(f) = \beta\}|. \end{aligned}$$

Let $D_p(\alpha) = D - \alpha p$ and $D_{p,q}(\alpha, \beta) = D - (\alpha p + \beta q)$, where $p, q \in \mathcal{P}$. We can easily see that

$$|\{f \in L(D)^* : \operatorname{ord}_p(f) = \alpha\}| = |L(D_p(\alpha))| - |L(D_p(\alpha + 1))| \tag{2.1}$$

and

$$\begin{aligned} & |\{f \in L(D)^* : \operatorname{ord}_p(f) = \alpha, \operatorname{ord}_q(f) = \beta\}| \\ = \ & |L(D_{p,q}(\alpha, \beta))| - |L(D_{p,q}(\alpha + 1, \beta))| - |L(D_{p,q}(\alpha, \beta + 1))| \\ & + |L(D_{p,q}(\alpha + 1, \beta + 1))|. \end{aligned} \tag{2.2}$$

When the genus $g = 0$, we can evaluate all dimensions of $L(D_{p,q}(\alpha, \beta))$ from the Riemann-Roch theorem for any pair (p, q) of distinct points and any pair (α, β) of integers. Since the all cardinalities of (2.1) and (2.2) are not depend on points p, q chosen, $(V, \mathcal{P}, \mathcal{C})$ is a symmetric set of curves. □

Next we consider the case of the genus $g \geq 1$. For a divisor D such that $0 \leq \deg D \leq 2g - 2$, the dimension of $L(D)$ can not be obtained from the Riemann-Roch theorem.

Let $M(p, q; \alpha, \beta) = \{f \in L(D) : \operatorname{ord}_p(f) = \alpha, \operatorname{ord}_q(f) = \beta\}$. In the same manner as the proof of Theorem 2.1, we can say that if $M(p, q; \alpha, \beta) = M(p', q'; \alpha, \beta)$ for any distinct pairs (p, q) and (p', q') then $(V, \mathcal{P}, \mathcal{C})$ is a symmetric set of curves. $M(p, q; \alpha, \beta)$ is said to be *independent of points* if the cardinality of $M(p, q; \alpha, \beta)$ is a constant value $\lambda_{\alpha,\beta}$ for any pair (p, q) of distinct points of $\mathcal{P}$.

THEOREM 2.2. *Let V be a non-singular curve with the genus $g \geq 1$, let D be an effective divisor on V and W a curve such that* $\operatorname{div}(W) \geq D$. *Suppose* $\mathcal{P} = \bigcup(\operatorname{Supp}(\operatorname{div}(f)) \setminus \operatorname{Supp}(\operatorname{div}(W)))$ *for all* $f \in L(D)^*$. *If $M(p, q; \alpha, \beta)$ is independent of points for any pair (α, β) then $(V, \mathcal{P}, \mathcal{C})$ is a symmetric set of curves, where $\mathcal{C} = \{f \cdot W : f \in L(D)^*\}$.*

The necessity of the above theorem requires to prove for all pairs (α, β) whether $M(p, q; \alpha, \beta)$ is independent of points. We show that the number of checks is reducible in the next corollary.

COROLLARY 2.3. *If $M(p, q; \alpha, \beta)$ is independent of points for (α, β) satisfying* $\deg D - 2g + 2 \leq \alpha + \beta \leq \deg D$, *then $(V, \mathcal{P}, \mathcal{C})$ is a symmetric set of curves.*

PROOF. Let $D_{p,q}(\alpha,\beta) = D-(\alpha p+\beta q)$. If $\deg D-2g+2 \leq \alpha+\beta \leq \deg D$ then $0 \leq \deg D_{p,q}(\alpha,\beta) \leq 2g-2$ and the dimension of $L(D_{p,q}(\alpha,\beta))$ cannot be obtained from Riemann-Roch theorem. Let $N(\alpha,\beta) = \{(\alpha',\beta') : \alpha' \geq \alpha, \beta' \geq \beta, \alpha'+\beta' < \deg D\}$. The cardinality of $L(D_{p,q}(\alpha,\beta))$ is

$$|L(D_{p,q}(\alpha,\beta))| = 1 + \sum_{(\alpha',\beta')\in N(\alpha,\beta)} |M(p,q;\alpha',\beta')|.$$

If $M(p,q;\alpha',\beta')$ is independent of points for any (α',β') such that $\deg D-2g+2 \leq \alpha'+\beta' \leq \deg D$, then $|L(D_{p,q}(\alpha,\beta))|$ is also independent of points p and q chosen. Hence, from (2.2) in the proof of Theorem 2.1, we can conclude that $M(p,q;\alpha,\beta)$ is independent of points for any pair $(\alpha.\beta)$. □

Let V be a curve defined by an equation $v(x,y) = 0$, and let $P = (x_0, y_0)$ be a non-singular point on V such that $\frac{\partial v}{\partial y}(P) \neq 0$. Suppose that the following power series

$$\begin{cases} x = x_0 + t \\ y = y_0 + h(t), \end{cases} \tag{2.3}$$

where

$$h(t) = \sum_{i=1}^{\infty} y_i t^i,$$

satisfies the equation $f(x,y) = 0$. Let C be a curve defined by an equation $c(x,y) = 0$. The intersection multiplicity $I_P(C,V)$ at P of V with C is the integer l such that

$$c(x_0+t, y_0+h(t)) = \alpha t^l + \sum_{i\geq l+1} \alpha_i t^i \ , \ \alpha \neq 0.$$

In general case of the genus $g \geq 1$, it is not easy to find a point set $\mathcal{P}$ and a curve set $\mathcal{C}$ satisfying the necessary condition of the above theorem 2.2 or its corollary 2.3. We next consider a case that V is an elliptic curve, say $g = 1$.

3. Construction on an elliptic curve

Suppose, in this section, F_q is a finite field with odd characteristic and F_{q^m} is an extension of F_q. Let E be a non-singular elliptic curve defined over F_q given by an equation

$$e(x,y) = x^3 + a_2x^2 + a_4x + a_6 - y^2 = 0.$$

We denote an elliptic curve defined over F_q by E/F_q and its point at infinity by $\mathcal{O}$.

THEOREM 3.1. *Let $\mathcal{C}$ be the set of all conics over F_{q^m}. Let $\mathcal{P}$ be the set of all F_{q^m}-rational intersection points of E and a curve W which excludes the point $\mathcal{O}$ and p such that $\frac{\partial F}{\partial y}(p) = 0$ and $y_2 = 0$. If W is a curve defined by an equation*

$$9x^4 + 12a_2x^3 + (4a_2^2 + 6a_4)x^2 + 4a_2a_4x + a_4^2 - 4(a_2+3x)y^2 = 0, \tag{3.1}$$

where a_2, a_4 and a_6 are coefficients of e, then $(E,\mathcal{P},\mathcal{C})$ is a symmetric set of curves.

PROOF. Let r be a point not in the set of intersections of E and W. Let $D = 6r$ and F_0 a curve with $\operatorname{div}(F_0) = D$. Then the set $\mathcal{C}$ of conics is $\mathcal{C} = \{f \cdot F_0 : f \in L(D)^*\}$. We will show that $M(p, q; \alpha, \beta)$ is independent of points for any pair (α, β) satisfying $\alpha + \beta = 6$ for any distinct points $p, q \in \mathcal{P}$.

Let C be a conic defined by $c(x, y) = c_1x^2 + c_2y^2 + c_3xy + c_4x + c_5y + c_6 = 0$. By substituting (2.3) into c, we have

$$c(x_0 + t, y_0 + h(t)) = \mathbf{c}A\mathbf{t}, \tag{3.2}$$

where $\mathbf{c} = (c_1, c_2, c_3, c_4, c_5, c_6)$, $\mathbf{t}^t = (1, t, t^2, t^3, t^4, t^5)$ and

$$A^t = \begin{pmatrix} x_0^2 & y_0^2 & x_0y_0 & x_0 & y_0 & 1 \\ 2x_0 & 2y_0y_1 & y_0 + x_0y_1 & 1 & y_1 & 0 \\ 1 & y_1^2 + 2y_0y_2 & y_1 + x_0y_2 & 0 & y_2 & 0 \\ 0 & 2y_1y_2 + 2y_0y_3 & y_2 + x_0y_3 & 0 & y_3 & 0 \\ 0 & y_2^2 + 2y_1y_3 + 2y_0y_4 & y_3 + x_0y_4 & 0 & y_4 & 0 \\ 0 & 2y_2y_3 + 2y_1y_4 + 2y_0y_5 & y_4 + x_0y_5 & 0 & y_5 & 0 \end{pmatrix}.$$

(B^t is the transpose of a matrix B.) Let $L(p, q; \alpha, \beta) = \{C \in \mathcal{C} : I_p(C, E) \geq \alpha, I_q(C, E) \geq \beta\}$. $L(p, q; \alpha, \beta)$ is a linear space of curves. Let $A(p; \alpha)$ be the submatrix of the first α columns of A^t obtained by substituting p into (3.2). $\dim L(p, q; \alpha, \beta)$ is the dimension of the null space of $\mathbf{g}[A(p; \alpha), A(q; \beta)] = \mathbf{0}$. If $\det A(p; 6)$ is equal to 0 then $\dim L(p, q; 6, 0) = 1$ since the dimension is 0 or 1. Suppose now that the coefficients y_2 of (2.3) corresponding to both p and q are 0. Then $\dim L(p, q; 6, 0) = \dim L(p, q; 0, 6) = 1$ since $\det A(p; 6)$ is

$$\det A(p; 6) = y_2(-2y_3^3 + 3y_2y_3y_4 - y_2^2y_5).$$

Moreover we have $\dim L(p, q; 3, 3) = 1$ because the determinant of the matrix $[A(p; 3), A(q; 3)]$ is 0. From the result 1.2, $L(p, q; \alpha, \beta) = \{0\}$ for any pair (α, β) satisfying $\alpha + \beta \geq 7$. From the result 1.3, $\dim L(p, q; \alpha, \beta) = 1$ for $\alpha + \beta = 5$. Since $\dim L(p, q; \alpha, \beta) = \dim L(p, q; \alpha+1, \beta) + \dim L(p, q; \alpha, \beta+1) - \dim L(p, q; \alpha+1, \beta+1)$, we have

$$\dim L(p, q; 6, 0) = \dim L(p, q; 3, 3) = \dim L(p, q; 0, 6) = 1$$

and

$$\dim L(p, q; 5, 1) = \dim L(p, q; 4, 2) = \dim L(p, q; 2, 4) = \dim L(p, q; 1, 5) = 0.$$

Hence, $M(p, q; \alpha, \beta)$ is independent of points for any pairs (α, β) satisfying $\alpha+\beta = 6$.

The elliptic curve E is given by

$$e(x, y) = x^3 + a_2x^2 + a_4x + a_6 - y^2 = 0.$$

From $e(x_0 + t, y_0 + h(t)) = 0$, we have

$$\begin{aligned} & (a_6 + a_4x_0 + a_2x_0^2 + x_0^3 - y_0^2) \\ + \; & (a_4 + 2a_2x_0 + 3x_0^2 - 2y_0y_1)t + (a_2 + 3x_0 - y_1^2)t^2 \\ + \; & (1 - 2y_0y_3)t^3 + (-2y_1y_3 - 2y_0y_4)t^4 + (-2y_1y_4 - 2y_0y_5)t^5 \\ + \; & (-y_3^2 - 2y_1y_5 - 2y_0y_6)t^6 + \cdots \\ = \; & 0. \end{aligned}$$

Since all coefficients of t must be equal to 0, we have

$$\begin{cases} a_4 + 2a_2x_0 + 3x_0^2 - 2y_0y_1 = 0 \\ a_2 + 3x_0 - y_1^2 = 0 \end{cases}$$

which is equivalent to the equation (3.1). Therefore the point (x_0, y_0) is on the curve W defined by the equation (3.1). □

We show here an example which constructs a symmetric set of curves obtained from the Theorem 3.1. Let E be an elliptic curve defined over F_5 given by

$$y^2 = x^3 + x^2 + 2x + 1.$$

Then points $(0,1)$, $(0,4)$, $(3,\omega)$ and $(3,4\omega)$, where ω is a root of x^2+2 in F_{5^2}, are intersection points of E and a curve given by

$$4x^4 + 2x^3 + x^2 + 3x + 4 + y + 3xy^2 = 0.$$

Let $\mathcal{P}$ be the set of these four points and $\mathcal{C}$ the set of conics defined over F_{5^2}. The power series corresponding to each points of $\mathcal{P}$ are

$$\begin{cases} x &= t \\ y &= 1 + t + 3t^3 + 3t^4 + 3t^5 + \cdots, \end{cases} \quad \begin{cases} x &= t \\ y &= 1 + t + 3t^3 + 3t^4 + 3t^5 + \cdots, \end{cases}$$

$$\begin{cases} x &= 3 + t \\ y &= \omega + \omega t^3 + 3\omega t^6 + \cdots, \end{cases} \quad \begin{cases} x &= 3 + t \\ y &= 4\omega + 4\omega t^3 + 2\omega t^6 + \cdots. \end{cases}$$

Let $L(p,q;\alpha,\beta) = \{C \in \mathcal{C} : I_p(C,E) \geq \alpha, I_q(C,E) \geq \beta\}$. We can say that $\dim L(p,q;6,0) = \dim L(p,q;3,3) = \dim L(p,q;0,6) = 1$ and $\dim L(p,q;5,1) = \dim L(p,q;4,2) = \dim L(p,q;2,4) = \dim L(p,q;1,5) = 0$ for any pair (p,q) of points of $\mathcal{P}$. Hence $(E,\mathcal{P},\mathcal{C})$ is a symmetric set of curves with $\lambda_{6,0} = \lambda_{3,3} = \lambda_{0,6} = 24$ and $\lambda_{5,1} = \lambda_{4,2} = \lambda_{2,4} = \lambda_{1,5} = 0$, where $|\mathcal{C}| = (5^2)^6$.

References

1. I. M. Chakravarti, *Fractional replication in asymmetrical factorial designs and partially balanced arrays*, Sankhyā **17** (1956), 143–164.
2. R. Fuji-Hara and S. Kuriki, *Mutually balanced nested designs*, Discrete Math. **97** (1991), 167–176.
3. William Fulton, *Algebraic curves : an introduction to algebraic geometry*, Mathematics lecture note series, Benjamin, 1969.
4. S. Kuriki and R. Fuji-Hara, *Balanced arrays of strength two and nested (r,λ)-designs*, J. Combin. Designs **2** (1994), 407–414.
5. Alfred Menezes, *Elliptic curve public key cryptosystems*, Kluwer Academic Publishers, 1993.
6. Carlos Moreno, *Algebraic curves over finite fields*, Cambridge University Press, New York, 1991.
7. Joseph H. Silverman and John Tate, *Rational points on elliptic curves*, Undergraduate texts in mathematics, Springer-Verlag, New York, 1992.
8. J. N. Srivastava, *Some general existence conditions for balanced arrays of strength t and 2 symbols*, J. Combinatorial Theory (A) **13** (1972), 198–206.

SYSTEM, INFORMATION AND MATHEMATICAL SCIENCES, UNIVERSITY OF TSUKUBA, TSUKUBA, IBARAKI, 305 JAPAN

E-mail address: fujihara@sk.tsukuba.ac.jp

DOCTORAL PROGRAM IN POLICY AND PLANNING SCIENCES, UNIVERSITY OF TSUKUBA, TSUKUBA, IBARAKI, 305 JAPAN

E-mail address: sshinoha@sk.tsukuba.ac.jp

Contemporary Mathematics
Volume **225**, 1999

Weight Functions and the Extension Theorem for Linear Codes over Finite Rings

Jay A. Wood

In memory of Ed Assmus

ABSTRACT. An extension theorem for general weight functions is proved over finite chain rings. The structure of the complex semigroup ring associated to the multiplicative semigroup of the ring plays a prominent role in the proof.

1. Background

In her doctoral dissertation, MacWilliams [**7**], [**8**] proved an equivalence theorem: two linear codes $C_1, C_2 \subset \mathbb{F}^n$ defined over a finite field $\mathbb{F}$ are equivalent up to monomial transformations if and only if there is a linear isomorphism $f : C_1 \to C_2$ which preserves Hamming weight. Bogart, Goldberg, and Gordon [**2**] gave another proof of this theorem, and a character theoretic proof was provided by Ward and the author [**13**].

Following up on the ideas in [**13**], the author has extended the character theoretic techniques to linear codes defined over finite Frobenius rings, first for the Hamming weight [**15**] and then for symmetrized weight compositions [**16**]. In this paper, the author treats general weight functions defined over finite chain rings, i.e., finite commutative local principal ideal rings. Goldberg proved the extension theorem for symmetrized weight compositions over finite fields, [**5**], and Constantinescu, Heise, and Honold have proved an extension theorem for homogeneous weight functions over $\mathbb{Z}/m$, [**4**].

A word on the name of the theorem. MacWilliams' result above is sometimes referred to as "the equivalence theorem of MacWilliams." I have come to prefer

1991 *Mathematics Subject Classification.* Primary 94B05; Secondary 13M05, 16P10, 16S36, 20M25.

Key words and phrases. Semigroup rings, finite Fourier transform, extension theorem.

Partially supported by NSA grants MDA904-94-H-2025 and MDA904-96-1-0067, and by Purdue University Calumet Scholarly Research Awards.

Expanded version of results presented at the Fourth International Conference on Finite Fields and Applications and at the Thirty-Fifth Allerton Conference on Communication, Control, and Computing [**17**]. This paper is in final form and no version of it will be submitted for publication elsewhere.

© 1999 American Mathematical Society

"the extension theorem of MacWilliams," because of the similarity to the extension theorems of Witt [**14**] and Arf [**1**] for bilinear and quadratic forms. In all these situations there is a fixed ambient space V, usually a finite dimensional vector space over a field. The space V is equipped with an auxiliary function, a weight function in coding theory, a bilinear or quadratic form otherwise. The linear automorphisms of V which preserve the auxiliary function form a group of *linear isometries*, often a classical group in the case of bilinear or quadratic forms, often a group of monomial transformations in coding theory. The *extension theorem* then determines conditions under which any injective linear transformation $f : W \to V$ from a subspace W of V which preserves the auxiliary function must in fact extend to a linear isometry of V itself.

2. Statement of the extension problem

Fix a finite associative ring R with 1. (Later, we will impose additional hypotheses on R, but we will try to be as general as possible for as long as possible.) Let R^n denote the free module consisting of n-tuples of elements from R. A right *linear code* of length n is a right submodule $C \subset R^n$. The *complete weight composition* is the function $c : R \times R^n \to \mathbb{Z}$ given by

$$c_r(x) = |\{i : x_i = r\}|, \quad r \in R, \quad x = (x_1, \ldots, x_n) \in R^n.$$

That is, the complete weight composition counts the number of entries in the n-tuple x which equal a particular element r in R.

Choose complex numbers a_r, $r \neq 0$ in R, and set $a_0 = 0$. Then the *weight function* determined by the a_r's is $w : R^n \to \mathbb{C}$ given by

$$w(x) = \sum_{r \in R} a_r c_r(x), \quad x \in R^n.$$

Since $a_0 = 0$, this sum is the same as the sum over $r \neq 0$.

EXAMPLE 2.1. For any ring R, choosing $a_r = 1$ for all $r \neq 0$ yields the *Hamming weight.*

EXAMPLE 2.2. For $R = \mathbb{Z}/k$, thought of as the integers j satisfying $-k/2 < j \leq k/2$, set $a_j = |j|$. The resulting weight function is then the *Lee weight.* The use of the Lee weight for linear codes over $\mathbb{Z}/4$ and its connections with nonlinear binary codes in [**3**], [**6**] has been an important motivation for the author's work.

EXAMPLE 2.3. The *Euclidean weight* for $R = \mathbb{Z}/k$ has $a_j = |j|^2$.

Notice that the Lee and Euclidean weight functions have some symmetry: $a_{-j} = a_j$. More generally, we define the *symmetry group* of a weight function w by

$$\mathrm{Sym}(w) = \{u \in \mathcal{U} : a_{ur} = a_r, \ r \in R\}.$$

Here $\mathcal{U}$ denotes the group of units in R. Since R is finite, all units are necessarily two-sided. The Lee and Euclidean weights have $\mathrm{Sym}(w) = \{\pm 1\}$.

Let U be a subgroup of $\mathcal{U}$. Multiplication defines a left action of U on the ring R, with each element acting as an additive group automorphism of R; $u \in U$ defines $r \mapsto ur$. We will write $r \approx s$ if $r = us$ for some $u \in U$. We set $\mathrm{orb}(r) = \{s \in R : r \approx s\}$, the *orbit* of $r \in R$ under U. Of course, $r \approx s$ if and only if $\mathrm{orb}(r) = \mathrm{orb}(s)$. Let $U\backslash R$ be the set of U-orbits in R. If $U \subset \mathrm{Sym}(w)$, then $a_r = a_s$ whenever $r \approx s$, and the value of a_r depends only on $\mathrm{orb}(r) \in U\backslash R$.

The subgroup U determines a *symmetrized weight composition* swc by

$$\mathrm{swc}_t(x) = |\{i : x_i \approx t\}| = \sum_{r \in \mathrm{orb}(t)} c_r(x).$$

Note that $\mathrm{swc}_s(x) = \mathrm{swc}_t(x)$ if $\mathrm{orb}(s) = \mathrm{orb}(t)$. Provided $U \subset \mathrm{Sym}(w)$, the weight function w can be written as

$$w(x) = \sum_{t \in U \backslash R} a_t \, \mathrm{swc}_t(x), \quad x \in R^n. \tag{2.1}$$

Let us now consider the linear automorphisms of R^n which preserve one of our auxiliary functions: either a weight function w or a symmetrized weight composition swc. A right linear transformation $f : R^n \to R^n$ is a right *monomial transformation* if there exist a permutation σ of $\{1, 2, \ldots, n\}$ and units $u_1, u_2, \ldots, u_n$ in R such that

$$f(x_1, x_2, \ldots, x_n) = (u_1 x_{\sigma(1)}, u_2 x_{\sigma(2)}, \ldots, u_n x_{\sigma(n)}),$$

for $(x_1, x_2, \ldots, x_n) \in R^n$. If, in addition, the units $u_1, \ldots, u_n$ lie in a subgroup $U \subset \mathcal{U}$ of the group of units of R, we say that f is a right *U-monomial transformation.* It is easy to verify that the right U-monomial transformations form a group under composition; the group is isomorphic to the n-fold wreath product of U.

In [**16**, Proposition 2, Theorem 9], the author proved the next two results about automorphisms which preserve a symmetrized weight composition; the second result is the extension theorem for symmetrized weight compositions over finite Frobenius rings. The definition of a Frobenius ring is somewhat technical (see [**11**] or [**15**]); for finite rings it is equivalent to the character module $\widehat{R} = \mathrm{Hom}_{\mathbb{Z}}(R, \mathbb{T})$ being free as a one-sided R-module. Here, $\mathbb{T}$ is the multiplicative group of unit complex numbers.

PROPOSITION 2.4. *Let $f : R^n \to R^n$ be a right linear automorphism. Then f preserves* swc, *i.e.,* $\mathrm{swc}_t(f(x)) = \mathrm{swc}_t(x)$, *for all $t \in U \backslash R$, $x \in R^n$, if and only if f is a right U-monomial transformation.*

THEOREM 2.5. *Suppose R is a finite Frobenius ring, and suppose U is a subgroup of the group of units in R. If $C \subset R^n$ is a right linear code and $f : C \to R^n$ is an injective right linear homomorphism which preserves the symmetrized weight composition* swc, *then f extends to a right U-monomial transformation of R^n.*

The corresponding results for a weight function w are the main items discussed in this paper. For the counterpart of Proposition 2.4, we must assume that the linear automorphism is already a monomial transformation. This result was also proved in [**16**, Proposition 10].

PROPOSITION 2.6. *Suppose a weight function w has symmetry group* $\mathrm{Sym}(w)$. *Then a right monomial transformation on R^n preserves w if and only if it is a* $\mathrm{Sym}(w)$*-monomial transformation.*

The following states the extension problem for weight functions over finite Frobenius rings, the counterpart to Theorem 2.5.

EXTENSION PROBLEM. *Suppose R is a finite Frobenius ring and that w is a weight function with symmetry group* $\mathrm{Sym}(w)$. *Determine conditions on the weight function w in order that every injective right linear homomorphism $f : C \to R^n$*

which preserves w, $C \subset R^n$ a right linear code, extends to a right monomial transformation on R^n which preserves w, i.e., a right $\mathrm{Sym}(w)$*-monomial transformation on R^n.*

COROLLARY 2.7. *Suppose w is a weight function with symmetry group* $\mathrm{Sym}(w)$ *for which the extension problem is solvable. Then the group of right linear automorphisms of R^n which preserve w is exactly the group of right* $\mathrm{Sym}(w)$*-monomial transformations.*

PROOF. Simply take $C = R^n$. □

3. Reducing to the weight composition case

In this section we describe two approaches to solving the extension problem for weight functions. Both approaches reduce the extension problem to the weight composition case covered by Theorem 2.5.

Suppose that $C \subset R^n$ is a right linear code with $f : C \to R^n$ a right linear homomorphism which preserves a weight function w. We assume that w has symmetry group $\mathrm{Sym}(w)$.

We utilize linearity: both the code C as well as $f : C \to R^n$ are right linear. What happens if we replace x by xs? We will discuss two ways of answering this question.

First approach. Notice that w can be written in the form

$$w(x) = \sum_{i=1}^{n} a_{x_i}.$$

This allows us to conclude that

$$w(xs) = \sum_{i=1}^{n} a_{x_i s} = \sum_{r \in R} a_{rs}\, c_r(x). \tag{3.1}$$

Let U be a subgroup of $\mathrm{Sym}(w)$. Recall that $r \approx t$ if $r = ut$ for some $u \in U$. Since $U \subset \mathrm{Sym}(w)$, if $r \approx t$, then $a_{rs} = a_{uts} = a_{ts}$. This allows us to rewrite (3.1) as

$$w(xs) = \sum_{t \in U\backslash R} \mathrm{swc}_t(x)\, a_{ts}. \tag{3.2}$$

Let $\mathcal{A}$ be the matrix of size $(|U\backslash R| - 1) \times (|R| - 1)$ whose (t, s) entry is a_{ts}. (We restrict $t \in U\backslash R$ and $s \in R$ to be non-zero, since $a_0 = 0$.) This leads to a very general version of the extension theorem.

THEOREM 3.1. *Suppose R is a finite Frobenius ring with weight function w. If the matrix $\mathcal{A}$ has maximal rank $|U\backslash R| - 1$, then the extension problem is solvable for w. The extension is a U-monomial transformation.*

PROOF. If f preserves w, then the rank condition and (3.2) imply that f preserves swc. Now apply Theorem 2.5. □

REMARK 3.2. If R is a commutative ring, then the value of a_{ts} depends only on the orbits of t and s. In this case, let $\mathcal{A}$ be square of size $|U\backslash R| - 1$ with (t, s) entry a_{ts}, for t, s nonzero elements of $U\backslash R$. The extension problem is solvable if $\det \mathcal{A} \neq 0$.

While this theorem seems very general, it is often difficult to apply. See Section 8 for some examples.

Our second approach, even though it is much less general, leads to conditions which are comparatively easy to verify. This second approach will occupy the remainder of the paper.

Second approach. For convenience, set $\delta_r = \delta_r(x) = c_r(f(x)) - c_r(x)$. Weight preservation says that

$$\sum_{r\neq 0} a_r \delta_r(x) = 0, \quad x \in C.$$

Notice that

$$c_r(xs) = \sum_{q:qs=r} c_q(x).$$

The linearity of C and f allows us to write the weight preservation condition as

$$\sum_{r\neq 0} a_r \left(\sum_{q:qs=r} \delta_q(x) \right) = 0, \quad x \in C, \quad s \in R. \tag{3.3}$$

We write (3.3) in matrix form. Let A be a row vector of length $|R| - 1$, with typical entry a_r indexed by $r \neq 0$ in R. Similarly, let Δ be a square matrix of size $|R| - 1$ whose rows and columns are indexed by $r, s \neq 0$ in R, with (r, s)-entry equal to $\sum_{q:qs=r} \delta_q(x)$. Thus (3.3) takes the form

$$A\Delta = 0. \tag{3.4}$$

The basic strategy is to exploit the structure of (3.4) in order to conclude that $\sum_{q\in \mathrm{orb}(t)} \delta_q(x) = 0$. Since the latter is equivalent to $\mathrm{swc}_t(f(x)) = \mathrm{swc}_t(x)$, swc is preserved by f, and we may apply Theorem 2.5 to prove the extension theorem. How to go about exploiting the structure of (3.4) is the subject of subsequent sections.

4. Semigroup rings

Let S be a finite semigroup whose operation is written as multiplication. Assume S has both a 0 and a 1 (different). The *complex semigroup ring* $\mathbb{C}[S]$ is then

$$\mathbb{C}[S] = \left\{ \sum_{s\in S} b_s e_s : b_s \in \mathbb{C} \right\},$$

a complex vector space with basis e_s, $s \in S$, whose multiplication is determined by the semigroup multiplication: $e_s e_t = e_{st}$. The one-dimensional subspace spanned by e_0 is a two-sided ideal in $\mathbb{C}[S]$, and its quotient

$$\mathbb{C}_0[S] = \mathbb{C}[S]/(e_0)$$

is called the *reduced* complex semigroup ring associated to S; $\mathbb{C}_0[S]$ has dimension $|S| - 1$ over $\mathbb{C}$.

Of particular interest to us is the semigroup we will denote by $S = R^\star$, the multiplicative semigroup of a finite ring. Then $\mathbb{C}_0[R^\star]$ has dimension $|R| - 1$. We are interested in the left regular representation of $\mathbb{C}_0[R^\star]$, i.e., $\mathbb{C}_0[R^\star]$ acting on itself by left multiplication. If $b = \sum_{r\neq 0} b_r e_r \in \mathbb{C}_0[R^\star]$, what is the matrix L_b with

respect to the basis $\{e_r\}$ for the linear transformation given by left multiplication by b?

The (r,s)-entry of L_b is the coefficient of e_r in be_s. But

$$be_s = \left(\sum_{q\neq 0} b_q e_q\right) e_s = \sum_{r\neq 0}\left(\sum_{q:qs=r} b_q\right) e_r,$$

so that the (r,s)-entry of L_b is $\sum_{q:qs=r} b_q$. This proves the next proposition.

PROPOSITION 4.1. *In* (3.4), *i.e.*, $A\Delta = 0$, *which expresses the weight preservation property of a linear homomorphism* $f : C \to R^n$, *the matrix* Δ *equals the matrix associated to left multiplication by* $\delta = \sum_{r\neq 0} \delta_r(x)e_r$ *in the reduced complex semigroup ring* $\mathbb{C}_0[R^\star]$.

To exploit the equation $A\Delta = 0$, we seek a better basis for $\mathbb{C}_0[R^\star]$. The basic idea is that the reduced semigroup ring $B = \mathbb{C}_0[R^\star]$ is an Artinian algebra over $\mathbb{C}$, whereby it admits a direct sum decomposition, as a left module over itself,

$$(4.1) \qquad {}_BB = \bigoplus V_i,$$

where the V_i are indecomposable left B-modules. Each projective indecomposable V_i in turn admits a composition series whose successive quotients are irreducible left B-modules.

By choosing a vector space basis for B over $\mathbb{C}$ which is adapted to the direct sum decomposition and the composition series, the matrix for the left regular representation will take on a block triangular form. If P is the change of basis matrix, expressing the new adapted basis in terms of the old basis of the e_r's, then $P^{-1}\Delta P$ is the matrix for the left regular representation in terms of the new adapted basis; $P^{-1}\Delta P$ is block triangular. Finally, our weight preservation equation, $A\Delta = 0$, can then be written as

$$(AP)(P^{-1}\Delta P) = 0.$$

This decomposition of $\mathbb{C}_0[R^\star]$ can be made very explicit for chain rings, as we shall see in Section 6. The decomposition of $\mathbb{C}_0[R^\star]$ will be expressed in terms of the Fourier transform, to which we turn next.

5. Fourier transform

Since we will make heavy use of the Fourier transform for finite abelian groups, this section establishes notation and records some standard facts.

Let G be a finite abelian group. A *character* on G is a group homomorphism $\pi : G \to \mathbb{T}$ from G to the multiplicative group of unit complex numbers. The collection of all characters on G, denoted $\widehat{G}$, is itself a finite abelian group under pointwise multiplication. The inverse π^{-1} of π in $\widehat{G}$ is just the complex conjugate $\overline{\pi}$.

Let $f : G \to \mathbb{C}$ be any complex-valued function on G. The *Fourier transform* of f is $\hat{f} : \widehat{G} \to \mathbb{C}$ given by $\hat{f}(\pi) = \sum_{x\in G} f(x)\pi(x)$.

The statement of the Poisson summation formula depends upon a choice of subgroup $H \subset G$. Define the *annihilator* $(\widehat{G} : H)$ of H in $\widehat{G}$ to be

$$(\widehat{G} : H) = \{\pi \in \widehat{G} : \pi(h) = 1,\ h \in H\}.$$

Then $(\widehat{G} : H) \cong \widehat{G/H}$ and $|(\widehat{G} : H)| = |G|/|H|$. The statement that follows, found in [**12**, §1.10, Theorem 10], generalizes [**9**, Lemma 11, p. 144].

THEOREM 5.1 (Poisson Summation Formula). *For every $x \in G$,*

$$\sum_{h \in H} f(hx) = \frac{1}{|(\widehat{G} : H)|} \sum_{\pi \in (\widehat{G}:H)} \hat{f}(\pi)\bar{\pi}(x).$$

6. Decomposing the semigroup ring

Starting in this section, we concentrate on the case where R is a finite chain ring, i.e., a finite commutative local ring with principal maximal ideal $\mathfrak{m} = Rm$. Our main task is to understand the structure of the reduced semigroup ring $\mathbb{C}_0[R^\star]$. What makes this particularly amenable to attack is the relatively simple ideal structure of the ring R. This and other useful facts are summarized in the next result. The reader may supply the proof or refer to [**16**, Lemma 13].

LEMMA 6.1. *Let $(R, \mathfrak{m})$ be a finite chain ring, with $\mathfrak{m} = Rm$. Then the following hold.*

1. *There exists an $l \geq 0$ such that $\mathfrak{m}^l \neq 0$, but $\mathfrak{m}^{l+j} = 0$ for all $j \geq 1$.*
2. *Each ideal $\mathfrak{m}^i$ is principal with $\mathfrak{m}^i = R(m^i)$.*
3. *Every ideal in R is equal to one of the $\mathfrak{m}^i$, $i = 0, 1, \ldots, l+1$.*
4. *R is Frobenius.*

Examples of these rings include all finite fields, the rings $\mathbb{Z}/p^l$ where p is prime, and the Galois rings $GR(p^l, n)$, [**10**, Chapter XVI].

The full group of units $\mathcal{U}$ acts on R on the left by multiplication. The orbits are $\mathcal{U} = R \setminus \mathfrak{m}$ itself, $\mathfrak{m} \setminus \mathfrak{m}^2, \mathfrak{m}^2 \setminus \mathfrak{m}^3, \ldots, \mathfrak{m}^l \setminus 0$, and 0, where $\setminus$ denotes the set-theoretic difference. Set $\mathcal{O}_0 = \mathcal{U} = R \setminus \mathfrak{m}$, $\mathcal{O}_i = \mathfrak{m}^i \setminus \mathfrak{m}^{i+1}$, and $\mathcal{O}_{l+1} = 0$. Also, set $M_i = |\mathcal{O}_i|$.

Define a relation $\leq$ on R by $y \leq x$ if $y = ax$ for some $a \in R$. The relation $\leq$ is reflexive and transitive, and $x \leq y$, $y \leq x$ implies that x, y lie in the same $\mathcal{U}$-orbit. Thus we see that $\leq$ induces a well-defined partial ordering on the set of $\mathcal{U}$-orbits of R. This works for any finite ring ([**15**]). What is special for R is that $\leq$ is actually a total ordering, with

$$0 = \mathcal{O}_{l+1} \leq \mathcal{O}_l \leq \mathcal{O}_{l-1} \leq \cdots \leq \mathcal{O}_1 \leq \mathcal{O}_0.$$

We now write down a new basis for the reduced semigroup ring $B = \mathbb{C}_0[R^\star]$. For a character π of the group of units $\mathcal{U}$ and an orbit $\mathcal{O}_i$, we say that the pair $(\pi, \mathcal{O}_i)$ is *admissible* if the pointwise stabilizer subgroup $\mathcal{U}_i = \mathrm{Stab}(\mathcal{O}_i)$ of the orbit $\mathcal{O}_i$ is contained in $\ker \pi$. Because R is commutative, $\mathcal{U}_i$ depends only upon the orbit $\mathcal{O}_i$, not on a particular element in the orbit. Note that $\mathcal{U}_i \subset \mathcal{U}_{i+1}$.

Another way to say that the pair $(\pi, \mathcal{O}_i)$ is admissible is that $\pi \in (\widehat{\mathcal{U}} : \mathcal{U}_i)$. Since $|(\widehat{\mathcal{U}} : \mathcal{U}_i)| = |\mathcal{U}|/|\mathcal{U}_i| = |\mathcal{O}_i|$, we see that the number of admissible pairs equals $|R|$. The zero orbit $\mathcal{O}_{l+1}$ has $\mathcal{U}_{l+1} = \mathcal{U}$, so that the trivial character $\pi = 1$ is the only admissible character for $\mathcal{O}_{l+1} = 0$. In dealing with the reduced semigroup ring $\mathbb{C}_0[R^\star]$, the admissible pair $(\pi = 1, \mathcal{O}_{l+1} = 0)$ will be dropped, leaving $|R| - 1 = \dim \mathbb{C}_0[R^\star]$ other admissible pairs.

For each admissible pair $(\pi, \mathcal{O}_i)$, $\pi \in (\widehat{\mathcal{U}} : \mathcal{U}_i)$, define an *admissible orbit sum* by

$$s(\pi, \mathcal{O}_i) = \frac{1}{M_i} \sum_{u \in \mathcal{U}/\mathcal{U}_i} \pi(u) e_{um^i} \in \mathbb{C}_0[R^\star].$$

Recall that $M_i = |\mathcal{O}_i|$, and note that $\mathcal{O}_i = \{um^i : u \in \mathcal{U}/\mathcal{U}_i\}$. Also, $\pi(u)$ for $u \in \mathcal{U}/\mathcal{U}_i$ is well-defined, since $\pi \in (\widehat{\mathcal{U}} : \mathcal{U}_i)$. Notice that $(\pi, \mathcal{O}_0)$ is admissible for every $\pi \in \widehat{\mathcal{U}}$, since $\mathcal{U}_0 = \{1\}$.

For any character $\pi \in \widehat{\mathcal{U}}$, let i_π be the largest integer j such that $(\pi, \mathcal{O}_j)$ is admissible. That is, $\mathcal{U}_{i_\pi} \subset \ker \pi$, but $\mathcal{U}_j \not\subset \ker \pi$ for $j > i_\pi$.

PROPOSITION 6.2. *For any element $b = \sum_{r \neq 0} b_r e_r$ in $\mathbb{C}_0[R^\star]$, and for any admissible orbit sum $s(\pi, \mathcal{O}_i)$, their product satisfies the following formula.*

$$b\, s(\pi, \mathcal{O}_i) = \sum_{k=0}^{i_\pi - i} \left(\sum_{u \in \mathcal{U}/\mathcal{U}_k} b_{um^k} \bar{\pi}(u) \right) s(\pi, \mathcal{O}_{i+k}).$$

PROOF. Group the terms of $b = \sum_{r \neq 0} b_r e_r$ into sums over orbits:

$$b = \sum_{k=0}^{l} \sum_{u \in \mathcal{U}/\mathcal{U}_k} b_{um^k} e_{um^k}.$$

Now focus on the product

$$\left(\sum_{u \in \mathcal{U}/\mathcal{U}_k} b_{um^k} e_{um^k} \right) s(\pi, \mathcal{O}_i) = \frac{1}{M_i} \sum_{u \in \mathcal{U}/\mathcal{U}_k} \sum_{v \in \mathcal{U}/\mathcal{U}_i} b_{um^k} \pi(v) e_{uvm^{i+k}}. \tag{6.1}$$

We wish to know the coefficient of $e_{wm^{i+k}}$, where $w \in \mathcal{U}/\mathcal{U}_{i+k}$. This term will arise from $u \in \mathcal{U}/\mathcal{U}_k$, $v \in \mathcal{U}/\mathcal{U}_i$, which satisfy $uv = w$ in $\mathcal{U}/\mathcal{U}_{i+k}$.

For fixed $w \in \mathcal{U}/\mathcal{U}_{i+k}$ and fixed $u \in \mathcal{U}/\mathcal{U}_k$, select one solution $v_0 \in \mathcal{U}/\mathcal{U}_i$ so that $uv_0 = w$. The other solutions $v = v_0 x$ for $uv = w$ are parameterized by elements x in the kernel $\mathcal{U}_{i+k}/\mathcal{U}_i$ of the natural surjection $\mathcal{U}/\mathcal{U}_i \to \mathcal{U}/\mathcal{U}_{i+k}$. In (6.1) there will then be a term of the form

$$\sum_{x \in \mathcal{U}_{i+k}/\mathcal{U}_i} \pi(v_0 x) = \begin{cases} (M_i/M_{i+k})\pi(v_0), & \pi \in (\widehat{\mathcal{U}} : \mathcal{U}_{i+k}), \\ 0, & \pi \notin (\widehat{\mathcal{U}} : \mathcal{U}_{i+k}). \end{cases}$$

When $\pi \in (\widehat{\mathcal{U}} : \mathcal{U}_{i+k})$, the value $\pi(v_0)$ depends only on u, w, in which case $\pi(v_0) = \bar{\pi}(u)\pi(w)$. Then the expression in (6.1) simplifies to

$$\left(\sum_{u \in \mathcal{U}/\mathcal{U}_k} b_{um^k} e_{um^k} \right) s(\pi, \mathcal{O}_i) = \begin{cases} \left(\sum_{u \in \mathcal{U}/\mathcal{U}_k} b_{um^k} \bar{\pi}(u) \right) s(\pi, \mathcal{O}_{i+k}), & \pi \in (\widehat{\mathcal{U}} : \mathcal{U}_{i+k}), \\ 0, & \pi \notin (\widehat{\mathcal{U}} : \mathcal{U}_{i+k}). \end{cases}$$

From this the desired formula follows. □

THEOREM 6.3. *The structure of the Artinian ring $\mathbb{C}_0[R^\star]$ has the following features.*

(1) *The admissible orbit sums $s(\pi, \mathcal{O}_0)$, $\pi \in \widehat{\mathcal{U}}$, are primitive orthogonal idempotents in $\mathbb{C}_0[R^\star]$ whose sum equals 1.*

(2) *For each character $\pi \in \widehat{\mathcal{U}}$, the subspace spanned by the admissible orbit sums $s(\pi, \mathcal{O}_i)$ is the projective indecomposable submodule V_π generated by the idempotent $s(\pi, \mathcal{O}_0)$.*

(3) *For each character* $\pi \in \widehat{\mathcal{U}}$, *let* i_π *be the largest integer such that* $(\pi, \mathcal{O}_{i_\pi})$ *is admissible. Then* $(\pi, \mathcal{O}_i)$ *is admissible for* $i \leq i_\pi$. *Moreover, the subspaces* V_π^i *spanned by* $s(\pi, \mathcal{O}_i), s(\pi, \mathcal{O}_{i+1}), \ldots, s(\pi, \mathcal{O}_{i_\pi})$ *are submodules of* $\mathbb{C}_0[R^\star]$, *with* $\dim_{\mathbb{C}} V_\pi^i = i_\pi - i + 1$. *The submodules* V_π^i *form a composition series for* V_π:

$$V_\pi = V_\pi^0 \supset V_\pi^1 \supset \cdots \supset V_\pi^{i_\pi} \supset 0.$$

(4) *The left regular representation for an element* $b = \sum_{r \neq 0} b_r e_r \in \mathbb{C}_0[R^\star]$, *expressed in terms of the basis of admissible orbit sums, has the block diagonal form*

$$\begin{pmatrix} \ddots & & \\ & N_\pi & \\ & & \ddots \end{pmatrix},$$

where each N_π *is lower triangular of size* $(i_\pi + 1) \times (i_\pi + 1)$. *The matrix* N_π *has the form*

$$N_\pi = \begin{pmatrix} \hat{b}(\bar{\pi}, 0) & 0 & 0 & \cdots & 0 \\ \hat{b}(\bar{\pi}, 1) & \hat{b}(\bar{\pi}, 0) & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \ddots & \vdots \\ \hat{b}(\bar{\pi}, i_\pi - 1) & \hat{b}(\bar{\pi}, i_\pi - 2) & \cdots & \hat{b}(\bar{\pi}, 0) & 0 \\ \hat{b}(\bar{\pi}, i_\pi) & \hat{b}(\bar{\pi}, i_\pi - 1) & \cdots & \hat{b}(\bar{\pi}, 1) & \hat{b}(\bar{\pi}, 0) \end{pmatrix},$$

where

$$\hat{b}(\bar{\pi}, j) = \sum_{u \in \mathcal{U}/\mathcal{U}_j} b_{um^j} \bar{\pi}(u), \quad j = 0, 1, \ldots, i_\pi.$$

PROOF. With the exception of the idempotents $s(\pi, \mathcal{O}_0)$ being primitive, all these statements follow immediately from the formula in Proposition 6.2 and the orthogonality relations on characters.

Since the idempotents $s(\pi, \mathcal{O}_0)$, $\pi \in \widehat{\mathcal{U}}$, are orthogonal, the Artinian ring $B = \mathbb{C}_0[R^\star]$ splits as a direct sum of rings:

$$B = \bigoplus_{\pi \in \widehat{\mathcal{U}}} Bs(\pi, \mathcal{O}_0).$$

The idempotent $s(\pi, \mathcal{O}_0)$ is primitive if and only if the ring $Bs(\pi, \mathcal{O}_0)$ is local.

Inside $Bs(\pi, \mathcal{O}_0)$ consider the subspace V_π^1; it is clearly an ideal. Every element $x \in Bs(\pi, \mathcal{O}_0)$ has the form $x = x_0 s(\pi, \mathcal{O}_0) + x'$, where $x_0 \in \mathbb{C}$ and $x' \in V_\pi^1$. Standard arguments show that x is a unit in $Bs(\pi, \mathcal{O}_0)$ if and only if $x_0 \neq 0$. Thus x is a unit if and only if $x \notin V_\pi^1$. This implies that $Bs(\pi, \mathcal{O}_0)$ is a local ring with maximal ideal V_π^1, as desired. □

7. Extension theorem

We continue to assume that $(R, \mathfrak{m})$ is a finite chain ring with $\mathfrak{m} = Rm$. We also assume that w is a weight function of the typical form $w(x) = \sum a_r c_r(x)$. In the next result, please be aware that the subgroup U need *not* be a subgroup of $\mathrm{Sym}(w)$, the symmetry group of w.

THEOREM 7.1. *Let U be any subgroup of $\mathcal{U}$. Suppose the weight function w satisfies $\hat{a}(\pi, i_\pi) = \sum_{u \in \mathcal{U}/\mathcal{U}_{i_\pi}} a_{um^{i_\pi}} \pi(u) \neq 0$ for all $\pi \in (\widehat{\mathcal{U}} : U)$. Then for any right linear code $C \subset R^n$, every injective right linear homomorphism $f : C \to R^n$ which preserves w extends to a U-monomial transformation on R^n.*

PROOF. In the general developments described above, the approach is to utilize the weight preservation equation $A\Delta = 0$ in order to show that the symmetrized weight composition determined by U is preserved. The result will then follow from the extension theorem for weight compositions, Theorem 2.5.

We make use of Theorem 6.3 to pick a better basis for $\mathbb{C}_0[R^\star]$: the basis consisting of the admissible orbit sums $s(\pi, \mathcal{O}_j)$, $\pi \in \widehat{\mathcal{U}}$, $j = 0, 1, \ldots, i_\pi$. Then $A\Delta = 0$ implies $(AP)(P^{-1}\Delta P) = 0$, where P is the change of basis matrix whose columns are the coefficients of the new basis elements $s(\pi, \mathcal{O}_j)$ in terms of the old basis elements e_r.

The entries of the row vector AP are simply $\hat{a}(\pi, i)/M_i$, where

$$\hat{a}(\pi, i) = \sum_{u \in \mathcal{U}/\mathcal{U}_i} a_{um^i} \pi(u).$$

The matrix $P^{-1}\Delta P$ is block triangular, as in Therorem 6.3.

For a fixed character π, the block parameterized by π in the matrix equation $(AP)(P^{-1}\Delta P) = 0$ yields the following system of equations:

$$\begin{aligned}
\frac{1}{M_0}\hat{a}(\pi, 0)\hat{\delta}(\bar{\pi}, 0) + \frac{1}{M_1}\hat{a}(\pi, 1)\hat{\delta}(\bar{\pi}, 1) + \cdots + \frac{1}{M_{i_\pi}}\hat{a}(\pi, i_\pi)\hat{\delta}(\bar{\pi}, i_\pi) &= 0 \\
\frac{1}{M_1}\hat{a}(\pi, 1)\hat{\delta}(\bar{\pi}, 0) + \cdots + \frac{1}{M_{i_\pi}}\hat{a}(\pi, i_\pi)\hat{\delta}(\bar{\pi}, i_\pi - 1) &= 0 \\
&\vdots = \vdots \\
\frac{1}{M_{i_\pi}}\hat{a}(\pi, i_\pi)\hat{\delta}(\bar{\pi}, 0) &= 0.
\end{aligned}$$

Since we are assuming that $\hat{a}(\pi, i_\pi) \neq 0$ for all $\pi \in (\widehat{\mathcal{U}} : U)$, we see by induction that $\hat{\delta}(\bar{\pi}, j) = 0$ for $\pi \in (\widehat{\mathcal{U}} : U)$ and $j = 0, 1, \ldots, i_\pi$. Note that $(\pi, \mathcal{O}_j)$ being admissible for $\pi \in (\widehat{\mathcal{U}} : U)$ means that $\pi \in (\widehat{\mathcal{U}} : \mathcal{U}_j)$ as well, so that $\pi \in (\widehat{\mathcal{U}} : U \cdot \mathcal{U}_j)$.

We now apply the Poisson summation formula, Theorem 5.1. The difference $\mathrm{swc}_t(f(x)) - \mathrm{swc}_t(x)$ of the symmetrized weight compositions has the form

$$\mathrm{swc}_t(f(x)) - \mathrm{swc}_t(x) = \sum_{r \in \mathrm{orb}(t)} (c_r(f(x)) - c_r(x)) = \sum_{r \in \mathrm{orb}(t)} \delta_r(x).$$

More than just a sum over a U-orbit, it is, in fact, a sum over the coset of t for the subgroup $U/(U \cap \mathcal{U}_t)$ of $\mathcal{U}/\mathcal{U}_t$. (We write $\mathcal{U}_t$ for the stabilizer subgroup of t in $\mathcal{U}$. The $\mathcal{U}$-orbit of t is some $\mathcal{O}_i$. The characters of $\mathcal{U}/\mathcal{U}_t$ are exactly those characters for which $(\pi, \mathcal{O}_i)$ is admissible.) The Poisson summation formula states that coset sums are equal to sums of transforms over annihilators. Since we know that $\hat{\delta}(\bar{\pi}, j) = 0$ for $\pi \in (\widehat{\mathcal{U}} : U)$ and $j = 0, 1, \ldots, i_\pi$, these sums of transforms over annihilators vanish. Thus the symmetrized weight composition is preserved, and the theorem follows from Theorem 2.5. □

COROLLARY 7.2. *Suppose w is any weight function with $a_r > 0$ for $r \neq 0$. Then any weight preserving linear homomorphism on a submodule extends to a monomial transformation.*

PROOF. Taking $U = \mathcal{U}$, we see that the only character in $(\widehat{\mathcal{U}} : U)$ is the trivial character $\pi = 1$. For $\pi = 1$, it is clear that $\hat{a}(\pi, i_\pi) \neq 0$, since it equals a sum of positive a_r's. □

The solution of the extension problem now follows from Theorem 7.1 simply by taking U to be the symmetry group of the weight function w. We record this result next.

THEOREM 7.3 (Extension Theorem). *Let $U = \mathrm{Sym}(w)$, the symmetry group of the weight function w. If $\hat{a}(\pi, i_\pi) = \sum_{u \in \mathcal{U}/\mathcal{U}_{i_\pi}} a_{um^{i_\pi}} \pi(u) \neq 0$ for all $\pi \in (\widehat{\mathcal{U}} : U)$, then the extension problem is solvable for w.*

REMARK 7.4. Suppose we are in the situation of Theorem 7.1, where U is some subgroup of $\mathcal{U}$ and $\hat{a}(\pi, i_\pi) \neq 0$ for all $\pi \in (\widehat{\mathcal{U}} : U)$. Then any $f : C \to R^n$ which preserves w extends to a U-monomial transformation on R^n. Beware that the extension of f need not preserve w on all of R^n (a priori, just on C). But if U is a subgroup of the symmetry group of w, then Proposition 2.6 applies to show that the extension also preserves w on R^n.

8. Examples

We conclude with some examples which illustrate both the uses and the limitations of the theorems of Section 7.

EXAMPLE 8.1. Let $R = \mathbb{Z}/2^{l+1}$. This is a finite chain ring with $\mathfrak{m} = (2)$. If we concentrate on the case where $U = \mathcal{U}$, then only the trivial character $\pi = 1$ arises in $(\widehat{\mathcal{U}} : U)$. For $\pi = 1$, $i_\pi = l$, and $\hat{a}(\pi, i_\pi) = a_{2^l}$. Thus, as long as $a_{2^l} \neq 0$, Theorem 7.1 says that a weight preserving $f : C \to R^n$ extends to a monomial transformation. As in Remark 7.4, the extension may not preserve the weight function on all of R^n.

A similar result holds for $R = \mathbb{Z}/p^{l+1}$ with p prime. The condition on w is that

$$a_{p^l} + a_{2p^l} + \cdots + a_{(p-1)p^l} \neq 0. \tag{8.1}$$

EXAMPLE 8.2. In [**4**], Constantinescu, Heise, and Honold prove an extension theorem for what they call *homogeneous* weight functions on $\mathbb{Z}/m$. For the case where $m = p^{l+1}$ is a prime power, it is a direct consequence of the definition that homogeneous weight functions satisfy (8.1). Thus the extension theorem in [**4**], in the case where $m = p^{l+1}$, also follows from Theorem 7.1.

EXAMPLE 8.3. Here is a further illustration of Remark 7.4. Let $R = \mathbb{F}_5$ and take $a_i = i$, for $i = 0, 1, 2, 3, 4$. The symmetry group of w is trivial.

In R^2, let C be the vector subspace spanned by the vector $(1, 4)$, so that

$$C = \{(0,0), (1,4), (2,3), (3,2), (4,1)\}.$$

Every non-zero vector in C has $w(x) = 5$. Thus the linear transformation $f : C \to R^2$ determined by $f(1,4) = (2,3)$ preserves w. Corollary 7.2 says that f extends to a monomial transformation. In fact, f extends to $2I$, i.e., scalar multiplication by 2. But $2I$ does not preserve w on all of R^2.

Now let us try to apply the extension theorem with $U = \{1\}$, the symmetry group of w. The group of units $\mathcal{U}$ is cyclic of order 4, and every character $\pi \in \widehat{\mathcal{U}}$ is admissible. In particular, consider the character π of order 2 in $\mathcal{U}$: $\pi(2^j) = (-1)^j$, for $j = 0, 1, 2, 3$. We then compute that

$$\hat{a}(\pi) = a_1 - a_2 + a_4 - a_3 = 0.$$

Thus the extension theorem does not apply.

It is easy to verify that the group of weight preserving automorphisms on R^2 is precisely the symmetric group Σ_2. Since f is not the restriction of a permutation, f does not extend to a weight preserving automorphism.

EXAMPLE 8.4. Let $R = \mathbb{Z}/8$, with $U = \pm 1$, as for the Lee or Euclidean weight functions. The nonzero U-orbits are $\{1,7\}$, $\{3,5\}$, $\{2,6\}$, and $\{4\}$. We assume $U \subset \mathrm{Sym}(w)$, so that $a_1 = a_7$, etc. Since R is commutative, the matrix $\mathcal{A}$ of Remark 3.2 is:

$$\mathcal{A} = \begin{pmatrix} a_1 & a_3 & a_2 & a_4 \\ a_3 & a_1 & a_2 & a_4 \\ a_2 & a_2 & a_4 & 0 \\ a_4 & a_4 & 0 & 0 \end{pmatrix}.$$

Then $\det \mathcal{A} = 2a_4^3(a_3 - a_1)$. This determinant is clearly nonzero for the Lee and Euclidean weight functions, so Theorem 3.1 implies the extension theorem in this case.

Similarly explicit calculations can be made for other small chain rings, proving the extension theorem in those settings. What is still missing is a uniform approach to the Lee and Euclidean weight functions for all chain rings.

REMARK 8.5. Notice that the factors of $\det \mathcal{A}$ above are exactly the $\hat{a}$'s which occur in Theorem 7.1. This pattern has appeared in all the calculations that the author has performed on various chain rings. For chain rings, we conjecture that $\det \mathcal{A}$ always factors into a product of $\hat{a}$'s, and hence that Theorem 3.1 and Theorem 7.1 are equivalent, provided $U \subset \mathrm{Sym}(w)$.

REMARK 8.6 (Added in proof). For chain rings, the conjecture in Remark 8.5 is true. This result will appear in subsequent work of the author.

References

[1] Č. Arf, *Untersuchungen über quadratische Formen in Körpern der Charakteristik* 2. I., J. Reine Angew. Math. **183** (1941), 148–167.

[2] K. Bogart, D. Goldberg, and J. Gordon, *An elementary proof of the MacWilliams theorem on equivalence of codes*, Inform. and Control **37** (1978), 19–22.

[3] A. R. Calderbank, A. R. Hammons, Jr., P. V. Kumar, N. J. A. Sloane, and P. Solé, *A linear construction for certain Kerdock and Preparata codes*, Bull. Amer. Math. Soc. (N. S.) **29** (1993), 218–222.

[4] I. Constantinescu, W. Heise, and Th. Honold, *Monomial extensions of isometries between codes over $\mathbb{Z}_m$*, Proceedings of the Fifth International Workshop on Algebraic and Combinatorial Coding Theory (ACCT '96) (Sozopol, Bulgaria), Unicorn, Shumen, 1996, pp. 98–104.

[5] D. Y. Goldberg, *A generalized weight for linear codes and a Witt-MacWilliams theorem*, J. Combin. Theory Ser. A **29** (1980), 363–367.

[6] A. R. Hammons, Jr., P. V. Kumar, A. R. Calderbank, N. J. A. Sloane, and P. Solé, *The $\mathbb{Z}_4$-linearity of Kerdock, Preparata, Goethals, and related codes*, IEEE Trans. Inform. Theory **IT-40** (1994), 301–319.

[7] F. J. MacWilliams, *Error-correcting codes for multiple-level transmission*, Bell System Tech. J. **40** (1961), 281–308.

[8] ———, *Combinatorial problems of elementary abelian groups*, Ph.D. thesis, Radcliffe College, Cambridge, Mass., 1962.
[9] ——— and N. J. A. Sloane, *The theory of error-correcting codes*, North-Holland Mathematical Library, vol. 16, North-Holland, Amsterdam, New York, Oxford, 1978.
[10] B. R. McDonald, *Finite rings with identity*, Pure and Applied Mathematics, vol. 28, Marcel Dekker, Inc., New York, 1974.
[11] T. Nakayama, *On Frobeniusean algebras.* I., Ann. of Math. (2) **40** (1939), 611–633; II., **42** (1941), 1–21.
[12] A. Terras, *Fourier analysis on finite groups and applications*, UCSD lecture notes, 1992.
[13] H. N. Ward and J. A. Wood, *Characters and the equivalence of codes*, J. Combin. Theory Ser. A **73** (1996), 348–352.
[14] E. Witt, *Theorie der quadratischen Formen in beliebigen Körpern*, J. Reine Angew. Math. **176** (1937), 31–44.
[15] J. A. Wood, *Duality for modules over finite rings and applications to coding theory*, submitted.
[16] ———, *Extension theorems for linear codes over finite rings*, Applied Algebra, Algebraic Algorithms and Error-Correcting Codes (T. Mora and H. Mattson, eds.), Springer-Verlag, Berlin, 1997, LNCS 1255, pp. 329–340.
[17] ———, *Semigroup rings and the extension theorem for linear codes*, Proceedings of the Thirty-Fifth Allerton Conference on Communication, Control, and Computing, 1997, to appear.

Department of Mathematics, Computer Science & Statistics, Purdue University Calumet, Hammond, Indiana 46323–2094 USA
E-mail address: wood@calumet.purdue.edu

This page intentionally left blank

Selected Titles in This Series

(*Continued from the front of this publication*)

200 **F. Dias, J.-M. Ghidaglia, and J.-C. Saut, Editors,** Mathematical problems in the theory of water waves, 1996

199 **G. Banaszak, W. Gajda, and P. Krasoń, Editors,** Algebraic K-theory, 1996

198 **Donald G. Saari and Zhihong Xia, Editors,** Hamiltonian dynamics and celestial mechanics, 1996

197 **J. E. Bonin, J. G. Oxley, and B. Servatius, Editors,** Matroid theory, 1996

196 **David Bao, Shiing-shen Chern, and Zhongmin Shen, Editors,** Finsler geometry, 1996

195 **Warren Dicks and Enric Ventura,** The group fixed by a family of injective endomorphisms of a free group, 1996

194 **Seok-Jin Kang, Myung-Hwan Kim, and Insok Lee, Editors,** Lie algebras and their representations, 1996

193 **Chongying Dong and Geoffrey Mason, Editors,** Moonshine, the Monster, and related topics, 1996

192 **Tomek Bartoszyński and Marion Scheepers, Editors,** Set theory, 1995

191 **Tuong Ton-That, Kenneth I. Gross, Donald St. P. Richards, and Paul J. Sally, Jr., Editors,** Representation theory and harmonic analysis, 1995

190 **Mourad E. H. Ismail, M. Zuhair Nashed, Ahmed I. Zayed, and Ahmed F. Ghaleb, Editors,** Mathematical analysis, wavelets, and signal processing, 1995

189 **S. A. M. Marcantognini, G. A. Mendoza, M. D. Morán, A. Octavio, and W. O. Urbina, Editors,** Harmonic analysis and operator theory, 1995

188 **Alejandro Adem, R. James Milgram, and Douglas C. Ravenel, Editors,** Homotopy theory and its applications, 1995

187 **G. W. Brumfiel and H. M. Hilden,** $SL(2)$ representations of finitely presented groups, 1995

186 **Shreeram S. Abhyankar, Walter Feit, Michael D. Fried, Yasutaka Ihara, and Helmut Voelklein, Editors,** Recent developments in the inverse Galois problem, 1995

185 **Raúl E. Curto, Ronald G. Douglas, Joel D. Pincus, and Norberto Salinas, Editors,** Multivariable operator theory, 1995

184 **L. A. Bokut′, A. I. Kostrikin, and S. S. Kutateladze, Editors,** Second International Conference on Algebra, 1995

183 **William C. Connett, Marc-Olivier Gebuhrer, and Alan L. Schwartz, Editors,** Applications of hypergroups and related measure algebras, 1995

182 **Selman Akbulut, Editor,** Real algebraic geometry and topology, 1995

181 **Mila Cenkl and Haynes Miller, Editors,** The Čech Centennial, 1995

180 **David E. Keyes and Jinchao Xu, Editors,** Domain decomposition methods in scientific and engineering computing, 1994

179 **Yoshiaki Maeda, Hideki Omoro, and Alan Weinstein, Editors,** Symplectic geometry and quantization, 1994

178 **Hélène Barcelo and Gil Kalai, Editors,** Jerusalem Combinatorics '93, 1994

177 **Simon Gindikin, Roe Goodman, Frederick P. Greenleaf, and Paul J. Sally, Jr., Editors,** Representation theory and analysis on homogeneous spaces, 1994

176 **David Ballard,** Foundational aspects of "non"standard mathematics, 1994

175 **Paul J. Sally, Jr., Moshe Flato, James Lepowsky, Nicolai Reshetikhin, and Gregg J. Zuckerman, Editors,** Mathematical aspects of conformal and topological field theories and quantum groups, 1994

174 **Nancy Childress and John W. Jones, Editors,** Arithmetic geometry, 1994

173 **Robert Brooks, Carolyn Gordon, and Peter Perry, Editors,** Geometry of the spectrum, 1994

(See the AMS catalog for earlier titles)

This page intentionally left blank

ISBN 0-8218-0817-6

AMS *on the* Web
www.ams.org