Z_4-Goethals Codes, Decoding and Designs

by

Kalle Ranto

To be presented, with the permission of the Faculty of Mathematics and Natural Sciences of the University of Turku, for public criticism in Auditorium XXI of the University on October 25th, 2002, at 12 noon

University of Turku
Department of Mathematics
FIN-20014 Turku, Finland

2002

SUPERVISOR

DOCENT JYRKI LAHTONEN
Department of Mathematics
University of Turku
FIN-20014 Turku
Finland

REVIEWERS

PROFESSOR VICTOR ZINOVIEV
Institute for Problems of Information Transmission
Russian Academy of Sciences
Bol'shoi Karetnyi per. 19
GSP-4, Moscow, 101447
Russia

DR. GARY MCGUIRE
Department of Mathematics
National University of Ireland
Maynooth, Co. Kildare
Ireland

OPPONENT

PROFESSOR TOR HELLESETH
Department of Informatics
University of Bergen
N-5020 Bergen
Norway

ISBN 951-29-2314-9
ISSN 1239-1883
Painosalama Oy
Turku, Finland
2002

Acknowledgements

I would like to thank my supervisor Docent Jyrki Lahtonen for his constant support during this work. Without his suggestions for research and valuable comments on my work I would not have finished this thesis.

I thank Professor Emeritus Aimo Tietäväinen for introducing me the fascinating field of coding theory and his friendly guidance during all these years. I also thank Docent Iiro Honkala, Dr. Tero Laihonen, and Ph. Lic. Petri Rosendahl for many inspiring discussions on and off the topic.

I thank all my colleagues in the Department of Mathematics and Turku Centre for Computer Science TUCS for nice working atmosphere and especially Tuire Huuskonen for doughnuts.

The Department of Mathematics and Turku Centre for Computer Science TUCS have provided excellent working conditions which I hereby gratefully acknowledge.

Special thanks are due to Professor Victor Zinoviev and Dr. Gary McGuire for the preliminary examination of the thesis and their invaluable remarks.

Finally, I thank my family, my lovely wife Sanna for her steadfast support and love, and my son Samuli for being such a cheerful boy.

Turku
September 2002 Kalle Ranto

Contents

Introduction

Error-correcting codes are nowadays used widely in telecommunications and electronics and the theory of these codes can be studied in the framework of engineering, physics, or mathematics. In this thesis we study one specific family of error-correcting codes, namely the $\mathbf{Z}_4$-Goethals codes, from mathematical viewpoint leaving the practical details to a minimum.

This work continues the study started by Hammons et al. in the revolutionary article [19] which triggered off the research on $\mathbf{Z}_4$-codes and Galois rings in coding theory. The binary nonlinear Goethals codes were introduced already in 1970's [16, 17] but the work of Hammons et al. gave a fresh viewpoint to these classical codes. For example, from the $\mathbf{Z}_4$-perspective it is straightforward to introduce the generalized family of $\mathbf{Z}_4$-Goethals codes [22] which will be the main objects of study in this thesis.

The binary Goethals codes are very good: they have four times as many codewords as BCH codes of the same length and minimum distance. Unfortunately, the binary Goethals codes are nonlinear and it is a difficult task to implement them efficiently. However, the seminal paper [19] showed how these codes can be seen as linear codes over $\mathbf{Z}_4$ and this extra structure makes them easier to handle.

In order to apply the $\mathbf{Z}_4$-Goethals codes in practice we should have an efficient decoding algorithm which can correct errors occurred in the messages encoded with these codes. We will develop a uniform decoding algorithm which is applicable to all $\mathbf{Z}_4$-Goethals codes and which corrects all errors up to the theoretical error-correcting capability.

Another objective of this thesis is to construct some new families of t-designs, actually 3-designs, from codewords of the $\mathbf{Z}_4$-Goethals codes. The t-designs are combinatorial objects which were originally motivated by statistics and experimental design but which are nowadays studied also purely as combinatorial structures, see [33] for example. We analyze the low-weight codewords of the $\mathbf{Z}_4$-Goethals codes and construct several new families of 3-designs from them.

The mathematical methods used in this thesis belong mostly to known algebraic and combinatorial machinery. However, there is one special feature which has not appeared in the literature: the appearance of Dickson polynomials in solving equations related to the $\mathbf{Z}_4$-Goethals codes.

Next we outline the structure of the thesis.

In Chapter 1 we give some definitions and results from algebra which are used frequently. We introduce in some detail the finite fields and the Galois rings and some elementary results on them.

In Chapter 2 we develop the theory of error-correcting codes such that the $\mathbf{Z}_4$-Goethals codes can be defined and studied. In the latter part of this chapter we will define the t-designs and sketch some known results in design theory which are needed in the later chapters.

In Chapter 3 we describe the decoding problem in more details and then a uniform decoding algorithm for all $\mathbf{Z}_4$-Goethals codes is given. The analysis branches into three parts which are considered in separate sections.

In Chapter 4 the classification of the low-weight codewords is done to the extent which allows us to construct new designs. We introduce several new infinite families of 3-designs and postpone the main proof to the following section. This proof is divided into cases which are considered one by one. In the last section we describe a special connection between the 3-designs with block sizes 7 and 8 with the affine geometry.

In Chapter 5 we generalize the 3-designs from the previous chapter to some of the generalized $\mathbf{Z}_4$-Goethals codes introduced in [22]. Also the question of nonequivalence of these 3-designs is briefly considered.

The material after the two preliminary chapters are mainly from articles [46, 47]. The results in Chapter 5 are previously unpublished.

Chapter 1

Algebraic preliminaries

We start by recalling some properties of algebraic structures and results which are needed in the later chapters. Some basic notions are not defined and the reader may find them in [29, 30, 37] or some other algebra textbook.

1.1 Finite fields

The purpose of this section is to describe shortly the structure and arithmetic of the finite fields. Informally, fields are algebraic structures with the usual four operations: addition, subtraction, multiplication, and division. A finite field is a field with only a finite number of elements.

Let $\mathbf{Z}$ denote a ring of integers with natural addition and multiplication. Every positive integer k generates an ideal $\langle k \rangle = \{kn \mid n \in \mathbf{Z}\}$ and the corresponding residue class ring $\mathbf{Z}_k = \mathbf{Z}/\langle k \rangle$ is a ring with k elements and characteristic k. The ring $\mathbf{Z}_k$ is a field if and only if k is prime. In this case the prime number is denoted by p and the field by $\mathbf{F}_p$.

The ring of polynomials with coefficients in $\mathbf{Z}_k$ and indeterminate x is denoted by $\mathbf{Z}_k[x]$ and $\langle f(x) \rangle = \{f(x)g(x) \mid g(x) \in \mathbf{Z}_k[x]\}$ denotes an ideal generated by $f(x)$. The next theorem gives the structure of all finite fields. For proofs and more details see [37, Chapters 1 and 2].

Theorem 1.1. *Every finite field has p^m elements with some prime p and positive integer m. For every prime p and every positive integer m there exists a monic irreducible polynomial $f(x) \in \mathbf{F}_p[x]$ of degree m. The residue class ring $\mathbf{F}_p[x]/\langle f(x) \rangle$ is the unique finite field with p^m elements up to isomorphism.*

We denote *the* finite field with $q = p^m$ elements by $\mathbf{F}_q$ and its multiplicative group by $\mathbf{F}_q^* = \mathbf{F}_q \setminus \{0\}$.

Theorem 1.2. *There exists $\alpha \in \mathbf{F}_q^*$ such that $\mathbf{F}_q^* = \{1, \alpha, \alpha^2, \ldots, \alpha^{q-2}\}$.*

The generator α in the previous theorem is called a *primitive element*.

1.1.1 Equations and Kloosterman sums

From now on we consider only the extensions of the binary field $\mathbf{F}_2$, i.e., the fields $\mathbf{F} = \mathbf{F}_q$ with $q = 2^m$. These finite fields have the following properties:

$$x+x=0, \quad x^{2^m}=x, \quad \text{and} \quad (x+y)^{2^i}=x^{2^i}+y^{2^i} \quad \text{for every } x,y \in \mathbf{F} \text{ and } i \geq 0$$

and these facts are used frequently without mentioning. Many concepts in this section can be defined also in a more general setting but they may look quite different.

The main results in this thesis and some preliminary facts below are valid only for odd m. This restriction is mentioned when needed.

Definition 1.3. A *trace function* $\mathrm{Tr} : \mathbf{F} \to \mathbf{F}_2$ is defined by

$$\mathrm{Tr}(x) = x + x^2 + x^{2^2} + \cdots + x^{2^{m-1}}.$$

With the identity $x^{2^m} = x$ it is easy to see that $\mathrm{Tr}(x^2) = \mathrm{Tr}(x)$. When m is odd the next well known lemma shows how the roots of quadratic equations are computed.

Lemma 1.4. *Let m be odd. The quadratic equation $x^2 + x = a$ with $a \in \mathbf{F}$ has two roots $\theta = \sum_{j=0}^{(m-1)/2} a^{4^j}$ and $\theta + 1$ in $\mathbf{F}$, if $\mathrm{Tr}(a) = 0$, and no roots in $\mathbf{F}$, if $\mathrm{Tr}(a) = 1$. In the latter case the two roots $\theta + \alpha$ and $\theta + \alpha + 1$ are in the quadratic extension $\mathbf{F}(\alpha)$ where α satisfies the equation $\alpha^2 + \alpha = 1$.*

An equation $x^2 + bx = a$ where $b \in \mathbf{F}^*$ can be transformed to $(x/b)^2 + x/b = a/b^2$ and the condition in the previous lemma changes to $\mathrm{Tr}\left(a/b^2\right) = 0$.

From now on, and especially in the following well known result, $\gcd(m,k)$ denotes the *greatest common divisor* of m and k.

Lemma 1.5. *The equation $x^{2^k} + x = a$ with $a \in \mathbf{F}$ has $2^{\gcd(m,k)}$ roots in $\mathbf{F}$, if $\mathrm{Tr}(a) = 0$, and no roots in $\mathbf{F}$, if $\mathrm{Tr}(a) = 1$.*

In Chapter 4 we count the number of solutions to certain systems of equations and come up with character sums.

Definition 1.6. A *Kloosterman sum* $K(a)$ for $a \in \mathbf{F}^*$ is defined as

$$K(a) = \sum_{\eta \in \mathbf{F}^*} (-1)^{\mathrm{Tr}\left(\eta + \frac{a}{\eta}\right)}.$$

Clearly, $K(a) = K(a^2)$ since $x \mapsto x^2$ is an automorphism of $\mathbf{F}$, the so called Frobenius automorphism.

The Kloosterman sums are closely related to $\mathbf{Z}_4$-Goethals codes as can be seen in [26, 28]. Here we record the following theorem by Helleseth and Zinoviev [25] that will be used in the proof of Theorem 4.5. We abbreviate $\mathbf{F} \setminus \{0,1\}$ by $\mathbf{F}^{**}$.

Theorem 1.7. *For every* $a \in \mathbf{F}^{**}$ $\quad K\left(a^3(a+1)\right) = K\left(a(a+1)^3\right)$.

This theorem could also be proved for odd m by substituting $a \mapsto a/(1+a)$ to the identity

$$K\left(\frac{a}{1+a^4}\right) = K\left(\frac{a^3}{1+a^4}\right)$$

from [51]. For odd m there is also a proof using elliptic curves and their isogenies, see [43].

1.1.2 Affine geometry and polynomials

In this subsection we introduce an affine geometry over the finite field $\mathbf{F}$ and relating polynomials which are needed in the analysis of low-weight codewords.

Let α be a primitive element of $\mathbf{F}$ with a minimal polynomial $f(x) \in \mathbf{F}_2[x]$, that is, $\mathbf{F} = \mathbf{F}_2[x]/\langle f(x)\rangle$. The field $\mathbf{F}$ can be viewed as an m-dimensional vector space over $\mathbf{F}_2$ with a basis $\{1, \alpha, \alpha^2, \ldots, \alpha^{m-1}\}$. This basis is now identified with the unit vectors $\{(1,0,\ldots,0),(0,1,\ldots,0),\ldots,(0,0,\ldots,1)\}$ and $\mathbf{F}$ with a vector space $\mathbf{F}_2^m$.

Definition 1.8. An *affine geometry* $AG(\mathbf{F})$ consists of all cosets $z+U$ of all subspaces U of $\mathbf{F}$ with the normal inclusion relation. A coset $z+U$ of an r-dimensional subspace U is called an *r-flat*.

A 1-flat is a coset $z+\{0,y\} = \{z, z+y\}$ and clearly any two points z and y are on a unique 1-flat. A 2-flat is a coset $z+\{0,y,w,y+w\} = \{z, z+y, z+w, z+y+w\}$ and it is easy to see that any three points are on a unique 2-flat. A 3-flat is a coset $x_1+\{0,x_2,x_3,x_2+x_3,x_4,x_2+x_4,x_3+x_4,x_2+x_3+x_4\} = \{x_1, x_1+x_2, x_1+x_3, x_1+x_2+x_3, x_1+x_4, x_1+x_2+x_4, x_1+x_3+x_4, x_1+x_2+x_3+x_4\}$ and any four points, which are not a 2-flat, are on a unique 3-flat.

Definition 1.9. A polynomial of the form $x^{2^r} + l_{r-1}x^{2^{r-1}} + \cdots + l_1x^2 + l_0x$, where $l_i \in \mathbf{F}$, is called *linearized* and a linearized polynomial plus a constant term is called *affine*.

We can naturally relate any subspace U and r-flat $z+U$ to the polynomials

$$L(x) = \prod_{\beta \in U}(x+\beta) \quad \text{and} \quad A(x) = \prod_{\beta \in z+U}(x+\beta).$$

For details and a proof for the next theorem see [37, Section 3.4].

Theorem 1.10. *There is one-to-one correspondence between subspaces of* $\mathbf{F}$ *and linearized polynomials whose all zeros are simple and in* $\mathbf{F}$. *Similarly, r-flats correspond exactly to the affine polynomials of degree* 2^r *with all zeros simple and in* $\mathbf{F}$.

Definition 1.11. Let k be a positive integer. The kth *elementary symmetric polynomial* in variables $x_1,\ldots,x_n$ is $\sigma_k(x_i)=\sum_{1\le i_1<\cdots<i_k\le n} x_{i_1}\ldots x_{i_k}$ and the *sum of* k*th powers* is $S_k(x_i)=\sum_{i=1}^n x_i^k$.

It is easy to see that

$$(x+x_1)\cdots(x+x_n)=x^n+\sigma_1(x_i)x^{n-1}+\sigma_2(x_i)x^{n-2}+\cdots+\sigma_n(x_i).$$

Example 1.12. By Theorem 1.10 a 2-flat $\{x_1,x_2,x_3,x_4\}$ can be represented as an affine polynomial $A(z)=x^4+a_2x^2+a_1x+a_0$. On the other hand, we have $A(x)=x^4+\sigma_1(x_i)x^3+\sigma_2(x_i)x^2+\sigma_3(x_i)x+\sigma_4(x_i)$, so we conclude that x_i's form a 2-flat if and only if $\sigma_1(x_i)=0$, that is, $x_1+x_2+x_3+x_4=0$.

Similarly $\{x_1,\ldots,x_8\}$ form a 3-flat if and only if $\sigma_1(x_i)=\sigma_2(x_i)=\sigma_3(x_i)=\sigma_5(x_i)=0$.

The next theorem is [37, Theorem 1.75] modified to $\mathbf{F}[x_1,\ldots,x_n]$.

Theorem 1.13 (Newton's formula). *The power sums S_i and the elementary symmetric polynomials σ_i in n variables satisfy the following relations:*

$$\begin{aligned} S_k+\sigma_1S_{k-1}+\sigma_2S_{k-2}+\cdots+\sigma_nS_{k-n}&=0, && \text{if } k>n\\ S_k+\sigma_1S_{k-1}+\sigma_2S_{k-2}+\cdots+\sigma_k\ k\quad&=0, && \text{if } n\ge k. \end{aligned}$$

1.1.3 Dickson polynomials

In this thesis we use the properties of the Dickson polynomials several times. For example, in the decoding algorithm in Chapter 3 we need to find all the roots of equations of the form $D_n(x,u)=v$ where $D_n(x,u)$ is a certain Dickson polynomial.

Definition 1.14. A *Dickson polynomial* (of the first kind) of degree n in indeterminate x and with parameter u is

$$D_n(x,u)=\sum_{i=0}^{\lfloor n/2\rfloor}\frac{n}{n-i}\binom{n-i}{i}(-u)^ix^{n-2i}.$$

Let $\sigma_1=x_1+x_2$, $\sigma_2=x_1x_2$, and $S_n=x_1^n+x_2^n$ be the first and second elementary symmetric polynomials and the sum of nth powers in two variables. Dickson polynomials arise from Waring's formula [37, Theorem 1.76] in the following manner:

$$S_n=x_1^n+x_2^n=\sum_{i=0}^{\lfloor n/2\rfloor}\frac{n}{n-i}\binom{n-i}{i}(-\sigma_2)^i\sigma_1^{n-2i}=D_n(\sigma_1,\sigma_2) \tag{1.1}$$

If we let $\sigma_2=u$ and $\sigma_1=x+u/x$, this functional equation can be written as $D_n(x+u/x,u)=x^n+(u/x)^n$.

Dickson polynomials can be defined over any commutative ring but we study these polynomials only over the finite field $\mathbf{F} = \mathbf{F}_q$ with $q = 2^m$. We state a few basic properties of these polynomials. Most of them can be found from the survey [36] and the others are easy exercises.

Lemma 1.15. *The polynomials $D_n(x,u)$ satisfy (n, l, $k \geq 0$)*

(i) $D_{n+2}(x,u) = xD_{n+1}(x,u) + uD_n(x,u)$ *with initial values* $D_0(x,u) = 0$ *and* $D_1(x,u) = x$;

(ii) $D_{nl}(x,u) = D_n\left(D_l(x,u), u^l\right)$;

(iii) $D_n(x,1)D_l(x,1) = D_{n+l}(x,1) + D_{|n-l|}(x,1)$;

(iv) $D_{2^k}(x,u) = x^{2^k}$;

(v) $D_{2^k+1}(x,u+v) = D_{2^k+1}(x,u) + D_{2^k+1}(x,v) + x^{2^k+1}$;

(vi) $D_{2^k+1}\left(x,x^2\right) = \begin{cases} 0, & \text{if } k \text{ is odd} \\ x^{2^k+1}, & \text{if } k \text{ is even.} \end{cases}$

The last two facts are consequences of the relation

$$D_{2^k+1}(x,u) = x^{2^k+1} + ux^{2^k-1} + u^2x^{2^k-3} + u^4x^{2^k-7} + \cdots + u^{2^{k-1}}x \tag{1.2}$$

which follows from Lucas' theorem for binomial coefficients, see [38, Theorem 13.28].

Definition 1.16. A polynomial $f(x) \in \mathbf{F}[x]$ is called a *permutation polynomial* if the associated function $f : \mathbf{F} \to \mathbf{F},\ c \mapsto f(c)$ permutes the elements of $\mathbf{F}$, i.e., f is a bijection.

Let $s = \gcd(n, q-1)$ and $r = \gcd(n, q+1)$. Clearly, when $u = 0$ the Dickson polynomial $D_n(x,0) = x^n$ is a permutation polynomial if and only if $s = 1$. The following theorem [40] (or [36, Theorem 3.2]) settles the cases with $u \neq 0$.

Theorem 1.17. *If $u \in \mathbf{F}^*$, the Dickson polynomial $D_n(x,u)$ is a permutation polynomial if and only if $s = 1 = r$, that is,* $\gcd\left(n, q^2-1\right) = 1$.

From now on we assume that $u \in \mathbf{F}^*$ and we simplify the formulas below by using u^2 instead of u.The proof of the next theorem can be found from [10] (or [36, Theorem 3.26']).

Theorem 1.18. *Let $x_0 \in \mathbf{F}$ be a solution to the equation $D_n\left(x,u^2\right) = v$. Then the total number of solutions in $\mathbf{F}$ is*

$$\begin{cases} s, & \text{if } v \neq 0 \text{ and } \mathrm{Tr}\left(u/x_0\right) = 0 \\ r, & \text{if } v \neq 0 \text{ and } \mathrm{Tr}\left(u/x_0\right) = 1 \\ (s+r)/2, & \text{if } v = 0. \end{cases}$$

In Chapter 3 we will always have $s = 1$ and in this case we deduce the following lemma [46].

Lemma 1.19. *Let $s = 1$ and $D_n\left(x, u^2\right) \neq 0$. Then*

$$\mathrm{Tr}\left(\frac{u}{x}\right) = \mathrm{Tr}\left(\frac{u^n}{D_n\left(x, u^2\right)}\right).$$

Proof. Clearly, $x \neq 0$ since $D_n\left(x, u^2\right) \neq 0$. Assume $\mathrm{Tr}(u/x) = 0$. By Lemma 1.4 this means that we can express x in the form $\gamma + u^2/\gamma$ where $\gamma \in \mathbf{F}$. Then γ^n and u^{2n}/γ^n are also in $\mathbf{F}$. By (1.1) they are the roots of the quadratic equation $T^2 + D_n\left(x, u^2\right) T + u^{2n} = 0$ and hence $\mathrm{Tr}\left(u^n / D_n\left(x, u^2\right)\right) = 0$.

Assume that $\mathrm{Tr}\left(u^n / D_n\left(x, u^2\right)\right) = 0$. This implies that the roots γ and u^{2n}/γ of the equation $T^2 + D_n\left(x, u^2\right) T + u^{2n} = 0$ are in $\mathbf{F}$. We have assumed that $s = 1$ and, therefore, γ has a unique nth root $\gamma^{1/n}$ in $\mathbf{F}$. Then $y = \gamma^{1/n} + u^2/\gamma^{1/n}$ satisfies the equation $D_n\left(y, u^2\right) = D_n\left(x, u^2\right)$ by (1.1). Moreover, $\mathrm{Tr}(u/y) = 0$ and by Theorem 1.18 we conclude that $x = y$. □

As can be seen in the previous proof, solving the roots of Dickson polynomial equation can be done by Cardano's method for solving a cubic equation. This was known already to Dickson, see [12, 13]. We specialize this fact for the cases needed in Chapter 3.

Theorem 1.20. *Let m be odd, $q = 2^m$, $s = 1$, and $v \in \mathbf{F}^*$. Then we have an effective procedure for solving all the roots $x \in \mathbf{F}$ of the equation*

$$D_n\left(x, u^2\right) = v.$$

Proof. When $\mathrm{Tr}(u^n/v) = \mathrm{Tr}(u/x) = 0$ we find a unique root x as in the proof of Lemma 1.19. In the computations we have to solve one quadratic equation and this can be done using Lemma 1.4.

When $\mathrm{Tr}(u^n/v) = \mathrm{Tr}(u/x) = 1$ we find the roots γ and u^{2n}/γ of the equation $T^2 + vT + u^{2n} = 0$ in the quadratic extension of $\mathbf{F}$ using Lemma 1.4. If there does not exist an nth root of γ in this extension, the equation has no roots in $\mathbf{F}$. If there exists one nth root of γ, then there are r such roots, each of which gives a different solution to the equation. According to Theorem 1.18 these are all the solutions. Although the nth roots $\gamma^{1/n}$ are no longer in $\mathbf{F}$, the roots $x = \gamma^{1/n} + u^2/\gamma^{1/n}$ still are. □

Example 1.21. Let us consider the roots $x \in \mathbf{F}$ of a cubic equation $D_3(x, 1) = x^3 + x = v \in \mathbf{F}^*$ when m is odd. Clearly, we have $s = \gcd(3, 2^m - 1) = 1$ and $r = \gcd(3, 2^m + 1) = 3$. By Theorem 1.18 and Lemma 1.19 there is a unique root

in $\mathbf{F}$ if and only if $\mathrm{Tr}(1/v) = 0$. Berlekamp, Rumsey, and Solomon [5] have proved this for all m with the condition $\mathrm{Tr}(1/v) \neq \mathrm{Tr}(1)$.

A simple counting argument then gives us the following fact [34, page 591] which we need in Subsection 4.3.2.

Let m be odd. The cubic equation $x^3 + x = a$ has 3 roots in $\mathbf{F}$ for $(q-2)/6$ values of $a \in \mathbf{F}^*$.

1.2 Galois rings

We introduce now Galois rings as they appear in [39, pages 307–335]. The interested reader is referred to this textbook for details. The construction of these rings is given as an analogy to the construction of the finite fields. A less abstract and less ring theoretical construction is given in the next subsection using the finite field arithmetic.

Definition 1.22. Let p^e be a prime power and m a positive integer. A *Galois ring* $GR(p^e, m)$ is a Galois extension of $\mathbf{Z}_{p^e}$ of degree m.

A Galois ring $GR(p^e, m)$ has p^{em} elements and characteristic p^e.

Theorem 1.23. *For every prime power p^e and every positive integer m there exists a monic basic irreducible polynomial $f(x) \in \mathbf{Z}_{p^e}[x]$ of degree m. The residue class ring $\mathbf{Z}_{p^e}[x]/\langle f(x)\rangle$ is a unique Galois ring with p^{em} elements and characteristic p^e up to isomorphism.*

1.2.1 Witt vectors

The Galois rings can be seen as Witt vector rings which are studied, e.g., in [30, pages 497–505]. As an example we show how the Galois ring $GR(4, m)$ can be identified with $\mathbf{F} \times \mathbf{F}$ if the operations are chosen suitably.

Definition 1.24. The *ring of Witt vectors* $W_2(\mathbf{F})$ of length 2 over $\mathbf{F}$ is a set of ordered pairs $\mathbf{F} \times \mathbf{F}$ equipped with addition and multiplication as follows:

$$\begin{aligned}(a_1, a_2) \;+\; (b_1, b_2) \;&=\; (\, a_1 + b_1 \,,\, a_2 + b_2 + a_1 b_1 \,) \\ (a_1, a_2) \;\cdot\; (b_1, b_2) \;&=\; (\quad a_1 b_1 \quad,\quad a_1^2 b_2 + a_2 b_1^2 \quad).\end{aligned}$$

We adapt the general results [30, Theorems 8.26 and 8.27] to the present case.

Theorem 1.25. *$W_2(\mathbf{F})$ is a commutative ring with a zero element $(0,0)$ and a unit element $(1,0)$. The ring $W_2(\mathbf{F})$ has a subring $W_2(\mathbf{F}_2)$ isomorphic to $\mathbf{Z}_4$.*

Let $R = W_2(\mathbf{F})$. Identifying $W_2(\mathbf{F}_2) = \{(0,0), (1,0), (0,1), (1,1)\}$ with $\mathbf{Z}_4$ and especially $(1,0) + (1,0) = (0,1)$ with 2 we can state the following result.

Theorem 1.26. *The non-units of R form a maximal ideal* $\langle 2 \rangle$ *and R is a local ring. In addition, R is a Galois extension of* $\mathbf{Z}_4$*, that is,* $R = GR(4,m)$.

Proof. By the multiplication rule, an element (a_1,a_2) has an inverse $\left(a_1^{-1}, a_2 a_1^{-4}\right)$ if and only if $a_1 \neq 0$. On the other hand, the ideal $\langle 2 \rangle$ generated by 2 is clearly maximal and contains exactly the non-units since $2(a_1,a_2) = \left(0,a_1^2\right)$. By [39, Theorem V.1] R is a local ring.

The local ring R is an *extension* of the local ring $\mathbf{Z}_4$ since $\mathbf{Z}_4 \subset R$. If the maximal ideal of the subring generates the maximal ideal in the extension, this extension is called *unramified*. The element 2 generates the maximal ideals in both $\mathbf{Z}_4$ and R, which makes this extension unramified and by [39, Theorem XV.4] it is also Galois. □

Let α be a primitive element of $\mathbf{F}$ and $\beta = (\alpha,0) \in R$. As $\beta^i = (\alpha^i,0)$ this β generates a cyclic subgroup of order $q-1$ in the multiplicative group of units R^*. This subgroup together with the zero element

$$\mathscr{T} = \{0,1,\beta,\ldots,\beta^{q-2}\} = \{(0,0),(1,0),(\alpha,0),\ldots,(\alpha^{q-2},0)\}$$

is called the *Teichmüller set*.

Lemma 1.27. *Every element of R can be expressed uniquely as* $A + 2B$ *where* $A,B \in \mathscr{T}$.

Proof. The Frobenius map $x \mapsto x^2$ is an automorphism of $\mathbf{F}$. Thus any element of R can be expressed as $\left(a_1,a_2^2\right) = (a_1,0) + 2(a_2,0)$. □

1.2.2 Equations

In this thesis the Galois rings are needed in constructions of good linear codes over $\mathbf{Z}_4$. In this setting we come up with systems of equations over the Galois ring R. Now we show how such equations can be turned into an equivalent system of equations over the finite field $\mathbf{F}$.

The modulo 2 reduction mapping from $\mathbf{Z}_4$ to $\mathbf{Z}_4/\langle 2 \rangle = \mathbf{F}_2$

$$\mu^* :\ 0 \mapsto 0,\ 1 \mapsto 1,\ 2 \mapsto 0,\ 3 \mapsto 1$$

can be extended naturally to the Galois ring R.

Definition 1.28. The *modulo* 2 *reduction mapping* is defined as $\mu : R \to R/\langle 2 \rangle = \mathbf{F}, \quad (a_1,a_2) \mapsto a_1$.

The μ-mapping is a bijection between the Teichmüller set $\mathscr{T}$ and the finite field $\mathbf{F}$. Hence the sums below and codes in the next chapter are indexed interchangeably with $\mathscr{T}$ or $\mathbf{F}$ depending on the situation.

As an example we prove the following lemma from [21] with Witt vectors.

Lemma 1.29. *Let* $(c_X)_{X\in\mathscr{T}} \in \mathbf{Z}_4^{2^m}$ *and* $C_j = \{\mu(X) \mid c_X = j\}$ *for* $j \in \mathbf{Z}_4$. *The equation*

$$\sum_{X\in\mathscr{T}} c_X X = A + 2B, \qquad A,B \in \mathscr{T}$$

is equivalent to the following system of two equations over $\mathbf{F}$

$$\sum_{x\in C_1\cup C_3} x = a \qquad \text{and} \qquad \sum_{\substack{x,y\in C_1\cup C_3\\ x<y}} xy + \sum_{x\in C_2\cup C_3} x^2 = b^2$$

where $a = \mu(A)$, $b = \mu(B)$, *and* $\leq$ *is some total order on* $\mathbf{F}$.

Proof. The equation considered is equal to

$$\sum_{x\in\mathbf{F}} c_x(x,0) = (a,0) + 2(b,0) = \left(a,b^2\right), \qquad a,b \in \mathbf{F}.$$

By dividing the sum to three parts according to the sets C_j we get

$$\begin{aligned}
&\sum_{x\in C_1} (1,0)\cdot(x,0) + \sum_{x\in C_2} (0,1)\cdot(x,0) + \sum_{x\in C_3} (1,1)\cdot(x,0)\\
&\quad= \sum_{x\in C_1} (x,0) + \sum_{x\in C_2} \left(0,x^2\right) + \sum_{x\in C_3} \left(x,x^2\right)\\
&\quad= \left(\sum_{x\in C_1} x, \sum_{\substack{x,y\in C_1\\ x<y}} xy\right) + \left(0, \sum_{x\in C_2} x^2\right) + \left(\sum_{x\in C_3} x, \sum_{x\in C_3} x^2 + \sum_{\substack{x,y\in C_3\\ x<y}} xy\right)\\
&\quad= \left(\sum_{x\in C_1\cup C_3} x, \sum_{\substack{x,y\in C_1\cup C_3\\ x<y}} xy + \sum_{x\in C_2\cup C_3} x^2\right) = \left(a,b^2\right)
\end{aligned}$$

and the claim follows. □

Chapter 2

Combinatorial preliminaries

We give some basic definitions and properties of error-correcting codes and combinatorial designs which are relevant in this thesis. In Subsection 2.1.3 we define the $\mathbf{Z}_4$-Goethals codes which are studied in the forthcoming chapters.

2.1 Error-correcting codes

Assume that a message word $\mathbf{c}$ over some alphabet is sent to a noisy communication channel (e.g. mobile network, hard disk, compact disk). The noise may cause some errors to the message and a receiver of the message should somehow figure out what message was sent.

The most studied subject within the theory of error-correcting codes, at least from the mathematical viewpoint, is the theory of block codes. In this setting the message words form a subset, called *code*, of all words of a fixed length n. The errors are considered to be changes of symbols, i.e., the noise can change letters of the message to other ones but can not for example shorten or lengthen the message. The reader without background in coding theory can consult [38, 44] for more extensive treatment of the subject.

In this work we are mainly interested in linear codes over $\mathbf{F}_2$ and $\mathbf{Z}_4$ which are considered next.

2.1.1 Linear codes over $\mathbf{F}_2$

The words of length n over the binary field $\mathbf{F}_2$ form a vector space $\mathbf{F}_2^n$ where addition and scalar multiplication are done componentwise. We define the Hamming weight $w_H(\mathbf{x})$ of a vector $\mathbf{x} \in \mathbf{F}_2^n$ to be the number of nonzero coordinates and the Hamming distance $d_H(\mathbf{x},\mathbf{y}) = w_H(\mathbf{x}-\mathbf{y})$ between two vectors $\mathbf{x}$ and $\mathbf{y}$ to be the number of coordinates where they differ.

Definition 2.1. A *binary code* of length n is a nonempty subset of $\mathbf{F}_2^n$. A $[n,k,d]$ *linear binary code* C is a k-dimensional subspace of $\mathbf{F}_2^n$ with a *minimum distance*

$$d = d_H(C) = \min_{\substack{\mathbf{x},\mathbf{y}\in C \\ \mathbf{x}\neq\mathbf{y}}} d_H(\mathbf{x},\mathbf{y}).$$

Assume that we use the codewords in some code C with a minimum distance d as a message words. The receiver of the message gets then the vector

$$\mathbf{r} = \mathbf{c} + \mathbf{e}$$

where the error vector $\mathbf{e}$ is nonzero in the error coordinates. If the weight of the error vector is less than $\lfloor (d-1)/2 \rfloor$, the transmitted message word $\mathbf{c}$ is the nearest codeword to the received word $\mathbf{r}$ in the Hamming metric. Therefore the receiver can decide which codeword was transmitted and the code C is said to have an *error-correcting capability* equal to $\lfloor (d-1)/2 \rfloor$.

Definition 2.2. We have the usual *inner product* $\mathbf{x}\cdot\mathbf{c} = \sum_{i=1}^{n} x_i c_i$ in the vector space $\mathbf{F}_2^n$ and a *dual code* of a linear code C is the orthogonal complement

$$C^{\perp} = \{\mathbf{x} \in \mathbf{F}_2^n \mid \mathbf{x}\cdot\mathbf{c} = 0 \text{ for all } \mathbf{c} \in C\}.$$

Definition 2.3. Let C be a code of length n and A_i be the number of codewords of weight i. The vector $(A_i)_{i=0}^n$ is called the *weight distribution* of C and the corresponding polynomial

$$\sum_{i=0}^{n} A_i w^{n-i} x^i = \sum_{\mathbf{c}\in C} w^{n-w_H(\mathbf{c})} x^{w_H(\mathbf{c})}$$

in two variables w and x is called the *weight enumerator* of C.

Clearly, a linear code has $A_0 = 1$, $A_i = 0$ for all $0 < i < d$, and $A_d \neq 0$. The famous MacWilliams theorem for binary linear codes can now be stated [38, Theorem 5.1.]. This theorem implies that we can count the weight distribution of $C^{\perp}$ from the weight distribution of C.

Theorem 2.4. *If binary linear codes C and $C^{\perp}$ have weight distributions $(A_i)_{i=0}^n$ and $(B_i)_{i=0}^n$, respectively, then*

$$\sum_{k=0}^{n} B_k w^{n-k} x^k = \frac{1}{|C|} \sum_{i=0}^{n} A_i (w+x)^{n-i} (w-x)^i. \tag{2.1}$$

As a linear code C is a subspace of $\mathbf{F}_2^n$ it has a basis. If we write the basis vectors as rows of a matrix G, we get a *generator matrix* of C. Another way

to describe a linear code is via its *parity-check matrix* H which is the generator matrix of the dual code $C^\perp$. Then we have a relation

$$\mathbf{c} \in C \qquad \text{if and only if} \qquad \mathbf{c}H^T = \mathbf{0}$$

where H^T is the transpose of H.

In this thesis most of the codes considered have dimensions k which are only little less than the length n. Thus the parity-check matrix having only $n-k$ rows gives a more compact description than the generator matrix.

Let $p : X \to X$ be a permutation of the coordinate set $X = \{1,2,\ldots,n\}$ of the words in $\mathbf{F}_2^n$. The permutation p acts naturally on codewords $(c_i) \mapsto (c_{p(i)})$ and codes $p(C) = \{p(\mathbf{c}) \mid \mathbf{c} \in C\}$.

Definition 2.5. Two binary codes C and C^* are *equivalent* if $C^* = p(C)$ for some permutation $p : X \to X$. Otherwise they are *nonequivalent*.

Usually, one is interested only in nonequivalent codes as the equivalent codes are just permuted versions of each other. For example, a decoding algorithm for a code is immediately applicable to an equivalent code, and often equivalent codes are thought to be the same.

Below we have some examples of extended binary cyclic codes of length $q = 2^m$. Parity-check matrices of these codes can be described with a primitive element α of $\mathbf{F} = \mathbf{F}_q$ and the coordinate set $X = \mathbf{F}$.

Example 2.6 (Extended Hamming codes). Let us consider the binary extended Hamming code $\mathscr{H}$ of length $q = 2^m$ with a parity-check matrix

$$H_{\mathscr{H}} = \begin{pmatrix} 1 & 1 & 1 & 1 & \ldots & 1 \\ 0 & 1 & \alpha & \alpha^2 & \ldots & \alpha^{q-2} \end{pmatrix}.$$

We get an $(m+1) \times q$-matrix over $\mathbf{F}_2$ by replacing the powers of α with the corresponding binary column vectors in the vector space $\mathbf{F}_2^m$ presentation. The first row implies that all codewords have even Hamming weight. It is well known that $\mathscr{H}$ is a $[q, q-m-1, 4]$ code and the dual $\mathscr{H}^\perp$ is a $[q, m+1, q/2]$ code with the weight distribution (other B_i's are zero)

$$B_0 = 1, \quad B_{q/2} = 2q-2, \quad \text{and} \quad B_q = 1.$$

Example 2.7 (Extended two-error-correcting BCH codes). As the second example we consider certain subcodes of $\mathscr{H}$ in the case where m is odd. Let $\mathscr{B}_k$ be a linear code defined by a parity-check matrix

$$H_{\mathscr{B}_k} = \begin{pmatrix} 1 & 1 & 1 & 1 & \ldots & 1 \\ 0 & 1 & \alpha & \alpha^2 & \ldots & \alpha^{q-2} \\ 0 & 1 & \alpha^{2^k+1} & \alpha^{(2^k+1)2} & \ldots & \alpha^{(2^k+1)(q-2)} \end{pmatrix}$$

where $1 \leq k \leq (m-1)/2$ and $\gcd(m,k) = 1$. The code $\mathscr{B}_1$ is the usual two-error-correcting extended BCH (Bose–Chaudhuri–Hocquenghem) code. We know ([4] or [9, Section 4.3]) that the codes $\mathscr{B}_k$ are pairwise nonequivalent and have parameters $[q, q-2m-1, 6]$. Their duals $\mathscr{B}_k^\perp$ are $[q, 2m+1, q/2-\sqrt{q/2}]$ codes with the weight distribution

$$B_0 = 1, \qquad B_{q/2-\sqrt{q/2}} = (q-1)\frac{q}{2}, \qquad B_{q/2} = q^2+q-2,$$
$$B_{q/2+\sqrt{q/2}} = (q-1)\frac{q}{2}, \quad \text{and} \quad B_q = 1.$$

Observe that the codes we for convenience choose to call BCH-codes are often also referred to as BCH-like codes. Our terminology is motivated by the fact that the weight distributions of these codes are identical. For the same reason we prefer Goethals codes to Goethals-like codes as a name for codes $\mathscr{G}_k$ below.

Example 2.8 (Reed–Muller codes). One of the most studied families of block codes are the Reed–Muller codes $RM(r,m)$. In this thesis we need only two of them, namely $RM(m-2,m)$ and $RM(m-3,m)$, and we omit the general definition. The definition and the results below can be found from [38, Chapter 13].

(i) $RM(r,m)$ is a binary linear $[q, \sum_{i=0}^{r}\binom{m}{i}, 2^{m-r}]$ code;

(ii) $RM(0,m) \subset RM(1,m) \subset \cdots \subset RM(m,m) = \mathbf{F}_2^q$;

(iii) $RM(m-2,m) = \mathscr{H}$;

(iv) Let m be odd. $RM(m-3,m)$ is defined by a parity-check matrix

$$H_{RM} = \begin{pmatrix} 1 & 1 & 1 & 1 & \dots & 1 \\ 0 & 1 & \alpha & \alpha^2 & \dots & \alpha^{q-2} \\ 0 & 1 & \alpha^{2^1+1} & \alpha^{(2^1+1)2} & \dots & \alpha^{(2^1+1)(q-2)} \\ 0 & 1 & \alpha^{2^2+1} & \alpha^{(2^2+1)2} & \dots & \alpha^{(2^2+1)(q-2)} \\ \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 1 & \alpha^{2^k+1} & \alpha^{(2^k+1)2} & \dots & \alpha^{(2^k+1)(q-2)} \end{pmatrix}$$

where $k = (m-1)/2$ and therefore $RM(m-3,m) \subset \mathscr{B}_k \subset RM(m-2,m)$;

(v) We can identify every object in the affine geometry $AG(\mathbf{F})$ with a binary (incidence) vector of length q by the rule: the vector has 1 in a coordinate α^i (or 0) if and only if the object contains the point α^i (or 0). The minimum weight codewords of $RM(r,m)$ are exactly the incidence vectors of $(m-r)$-flats. In addition, these minimum weight codewords generate the code $RM(r,m)$ as a vector space.

2.1.2 Linear codes over $\mathbf{Z}_4$

We have already seen how the construction of finite fields can be generalized to construct Galois rings. Similarly the construction of some good linear codes over $\mathbf{F}_2$ is now generalized to get good linear codes over $\mathbf{Z}_4$. The results in this subsection are mostly from [19].

Words of length n over the alphabet $\mathbf{Z}_4$ form a free $\mathbf{Z}_4$-module $\mathbf{Z}_4^n$ with componentwise addition and scalar multiplication. This module is not a vector space since $\mathbf{Z}_4$ is not a field. Hence we can not define linear codes as subspaces but submodules. This characterizes the same feature as subspaces: a sum $\mathbf{c}+\mathbf{d}$ of any two codewords $\mathbf{c}$ and $\mathbf{d}$ is always a codeword.

Definition 2.9. A *linear* $\mathbf{Z}_4$*-code* of length n is a submodule of $\mathbf{Z}_4^n$.

We define the Hamming distance for words over $\mathbf{Z}_4$ as above but we have another useful metric, too.

Definition 2.10. A *Lee weight* $w_L : \mathbf{Z}_4 \to \mathbf{Z}$ of an element in $\mathbf{Z}_4$ is defined as

$$w_L(0) = 0, \quad w_L(1) = w_L(3) = 1, \quad w_L(2) = 2$$

and a Lee weight of a vector $\mathbf{c} \in \mathbf{Z}_4^n$ is naturally: $w_L(\mathbf{c}) = \sum_{i=1}^n w_L(c_i)$.

The *Lee distance* is defined as $d_L(\mathbf{x},\mathbf{y}) = w_L(\mathbf{x}-\mathbf{y})$ and the *minimum Lee distance* $d_L(\mathscr{C})$ of a $\mathbf{Z}_4$-code $\mathscr{C}$ as $d_H(\mathscr{C})$ but respect to the Lee metric. The code $\mathscr{C}$ is said to have an error-correcting capability equal to $\lfloor (d_L(\mathscr{C})-1)/2 \rfloor$.

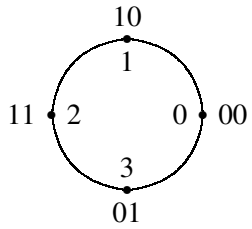

Figure 2.1: Gray map

Definition 2.11. A *Gray map* $\phi : \mathbf{Z}_4^n \to \mathbf{F}_2^{2n}$ is defined first for one component

$$\phi(0) = 00, \quad \phi(1) = 10, \quad \phi(2) = 11, \quad \phi(3) = 01$$

and then for the whole vector $\mathbf{c} = (c_1, \ldots, c_n)$ as

$$\phi(\mathbf{c}) = (c_{1L}, c_{2L}, \ldots, c_{nL} \mid c_{1R}, c_{2R}, \ldots, c_{nR}) = (\mathbf{c}_L \mid \mathbf{c}_R)$$

where $\phi(c_i) = (c_{iL}, c_{iR})$.

The bit order of the Gray image vector is chosen just for technical reasons in the proof of Corollary 4.6. The importance of the Gray map can be seen from Figure 2.1: it preserves the weights and distances when mapping $\mathbf{Z}_4$-words to binary words of double length. This well known fact is stated as an easy lemma without a proof.

Lemma 2.12. *The Gray map* $\phi : (\mathbf{Z}_4^n, d_L) \to \left(\mathbf{F}_2^{2n}, d_H\right)$ *is an isometry of metric spaces, that is,* ϕ *is a bijection and* $d_H(\phi(\mathbf{x}), \phi(\mathbf{y})) = d_L(\mathbf{x},\mathbf{y})$ *for all* $\mathbf{x},\mathbf{y} \in \mathbf{Z}_4^n$.

The weights of codewords in a code $\mathscr{C}$ can be described with a weight enumerator as in the case of the binary codes. Sometimes it is useful to count how many 1's, 2's, and 3's there is in a codeword. Sometimes we do not distinguish between 1's and 3's as they are both units in $\mathbf{Z}_4$ as opposed to 2's. Sometimes only Hamming weight counts. Thus we need several different weight enumerators.

Definition 2.13. The *support* of a vector $\mathbf{c}$ is $\chi(\mathbf{c}) = \{k \mid c_k \neq 0\}$ and the *multiplicity* of $i \in \mathbf{Z}_4$ in $\mathbf{c}$ is $n_i(\mathbf{c}) = |\{k \mid c_k = i\}|$. We define *complete*, *symmetrized*, *Lee weight*, and *Hamming weight enumerator* of $\mathbf{c}$ as

$$\begin{aligned}
\operatorname{cwe}(\mathbf{c}) &= W^{n_0(\mathbf{c})} X^{n_1(\mathbf{c})} Y^{n_2(\mathbf{c})} Z^{n_3(\mathbf{c})} \\
\operatorname{swe}(\mathbf{c}) &= W^{n_0(\mathbf{c})} X^{n_1(\mathbf{c})+n_3(\mathbf{c})} Y^{n_2(\mathbf{c})} \\
\operatorname{lwe}(\mathbf{c}) &= W^{n_0(\mathbf{c})} X^{n_1(\mathbf{c})+2n_2(\mathbf{c})+n_3(\mathbf{c})} \\
\operatorname{hwe}(\mathbf{c}) &= W^{n_0(\mathbf{c})} X^{n_1(\mathbf{c})+n_2(\mathbf{c})+n_3(\mathbf{c})}
\end{aligned}$$

and of a code $\mathscr{C}$, for example, as $\operatorname{cwe}(\mathscr{C}) = \sum_{\mathbf{c}\in\mathscr{C}} \operatorname{cwe}(\mathbf{c})$.

The variable W is usually unnecessary except with the zero word W^n.

Definition 2.2 can be straightforwardly generalized to the case of $\mathbf{Z}_4^n$: the sum in the inner product is now counted modulo 4. This defines the *dual code* $\mathscr{C}^\perp$ of a linear $\mathbf{Z}_4$-code $\mathscr{C}$. To state MacWilliams theorem (Theorem 2.4) in a generalized form we change the notation $\operatorname{cwe}(\mathscr{C})$ to $\operatorname{cwe}_{\mathscr{C}}(W,X,Y,Z)$.

Theorem 2.14. *For every linear $\mathbf{Z}_4$-code $\mathscr{C}$ and its dual $\mathscr{C}^\perp$ we have* ($i^2 = -1$)

$$\begin{aligned}
\operatorname{cwe}_{\mathscr{C}^\perp}(W,X,Y,Z) = \frac{1}{|\mathscr{C}|} \operatorname{cwe}_{\mathscr{C}}(&W+X+Y+Z, W+iX-Y-iZ, \\
&W-X+Y-Z, W-iX-Y+iZ).
\end{aligned}$$

With this theorem we can compute $\operatorname{cwe}(\mathscr{C}^\perp)$ when $\operatorname{cwe}(\mathscr{C})$ is known.

We can define permutations on the coordinate set X of $\mathbf{Z}_4^n$ as in the binary case. As $\mathbf{Z}_4$ is a ring with two units 1 and 3 we also allow "sign changes" in fixed coordinates when considering the equivalence of codes. Let $s : X \to \{1,3\}$ be a function and define its action on a codeword $\mathbf{c}$ by a rule: $(c_i) \mapsto (s(i) \cdot c_i)$.

Definition 2.15. Two $\mathbf{Z}_4$-codes $\mathscr{C}$ and $\mathscr{C}^*$ are *equivalent* if $\mathscr{C}^* = s \circ p(\mathscr{C})$ for some permutation $p : X \to X$ and function $s : X \to \{1,3\}$. Otherwise they are *nonequivalent*.

In Subsection 1.1.2 we identified the finite field $\mathbf{F}$ with the vector space $\mathbf{F}_2^m$. Now we do the same with the Galois ring R and the free module $\mathbf{Z}_4^m$. Let $\beta = (\alpha, 0)$ be a generator of the Teichmüller set $\mathscr{T}$ with a minimal polynomial $f(x) \in \mathbf{Z}_4[x]$. It can be shown that $R = \mathbf{Z}_4[x]/\langle f(x)\rangle$ and $\{1, \beta, \beta^2, \ldots, \beta^{m-1}\}$ is a basis of R as an extension over $\mathbf{Z}_4$. We identify this basis with the unit vectors $\{(1,0,\ldots,0)$, $(0,1,\ldots,0), \ldots, (0,0,\ldots,1)\}$ and the whole ring R with $\mathbf{Z}_4^m$.

In the previous subsection the extended binary cyclic codes were defined with parity-check matrices and a primitive element α. Now the parity-check matrices are defined similarly but the defining element is $\beta = (\alpha, 0)$ and the coordinate set $X = \mathscr{T}$.

Example 2.16 (Preparata and Kerdock codes). Let $m \geq 3$ be odd and $q = 2^m$. The $\mathbf{Z}_4$-Preparata code $\mathscr{P}$ of length q is defined by a parity-check matrix

$$H_{\mathscr{P}} = \begin{pmatrix} 1 & 1 & 1 & 1 & \dots & 1 \\ 0 & 1 & \beta & \beta^2 & \dots & \beta^{q-2} \end{pmatrix}.$$

By replacing the powers of β with the corresponding column vectors in $\mathbf{Z}_4^m$ we get an $(m+1) \times q$ matrix over $\mathbf{Z}_4$. It is known that $\mathscr{P}$ has $2^{2q-2m-2}$ codewords and $d_L(\mathscr{P}) = 6$. The dual code of $\mathscr{P}$ is the $\mathbf{Z}_4$-Kerdock code $\mathscr{K}$ with cwe ($W = 1$)

$$\begin{aligned} & 1 + X^q + Y^q + Z^q \\ & +2(q-1)\left(X^{q/2}Z^{q/2} + Y^{q/2}\right) \\ & +q(q-1)\Big(X^{q/4+\sqrt{q/8}}Y^{q/4+\sqrt{q/8}}Z^{q/4-\sqrt{q/8}} \\ & \qquad +X^{q/4+\sqrt{q/8}}Y^{q/4-\sqrt{q/8}}Z^{q/4-\sqrt{q/8}} \\ & \qquad +X^{q/4-\sqrt{q/8}}Y^{q/4-\sqrt{q/8}}Z^{q/4+\sqrt{q/8}} \\ & \qquad +X^{q/4-\sqrt{q/8}}Y^{q/4+\sqrt{q/8}}Z^{q/4+\sqrt{q/8}}\Big). \end{aligned}$$

When $m = 3$, the codes $\mathscr{P}$ and $\mathscr{K}$ are the same code. This $\mathbf{Z}_4$-Nodrstrom–Robinson code (or $\mathbf{Z}_4$-octacode) is the unique self-dual $\mathbf{Z}_4$-code of length 8, minimum distance 6 and with 256 codewords, see [19, Subsection IV.E].

Historical notes I

The interest in $\mathbf{Z}_4$-codes started about a decade ago with the seminal work of Hammons, Kumar, Calderbank, Sloane, and Solé [19]. There had been some earlier work, for example [41], but it was the article [19] which really started the theory of $\mathbf{Z}_4$-codes and coding theorists' interest in Galois rings.

The theory of $\mathbf{Z}_4$-codes has been fruitful in many fields of research but still the main achievement is the result in [19]: original binary nonlinear Preparata [45] and Kerdock [32] codes can be seen as Gray images of the linear $\mathbf{Z}_4$-codes $\mathscr{P}$ and $\mathscr{K}$. This gives an answer to the problem which was open for two decades: Why the binary Preparata and Kerdock codes satisfy the MacWilliams identity (2.1) although they are nonlinear? Since they are linear over $\mathbf{Z}_4$!

Actually, as explained in [19], the Gray images $\phi(\mathscr{K})$ are equivalent to the binary Kerdock codes but $\phi(\mathscr{P})$ are not equivalent to the binary Preparata codes, although their distance distributions are the same. This can be seen as follows: the

Table 2.1: Different choices for k with different codelengths

m	length	k	2^k+1
3	8	1	3
5	32	1,2	3,5
7	128	1,2,3	3,5,9
9	512	1,2, 4	3,5, 17
11	2048	1,2,3,4,5	3,5,9,17,33
13	8192	1,2,3,4,5,6	3,5,9,17,33,65
15	32768	1,2, 4, 7	3,5, 17, 129
17	131072	1,2,3,4,5,6,7,8	3,5,9,17,33,65,129,257
19	524288	1,2,3,4,5,6,7,8,9	3,5,9,17,33,65,129,257,513

binary Preparata codes (as well as their generalizations in [14, 2]) are subcodes of the *linear* Hamming codes $\mathscr{H}$, see [50], but the Gray images $\phi(\mathscr{P})$ are subcodes of *nonlinear* binary codes with the same distance distribution as $\mathscr{H}$, see [19].

The classical binary Nordstrom–Robinson code [42] is the binary Kerdock code of length 16 and hence equal to $\phi(\mathscr{K}) = \phi(\mathscr{P})$ when $m = 3$.

The binary Goethals codes [16, 17] and the first codes from a family of Delsarte and Goethals [11] are also formally dual nonlinear binary codes. This can be explained again with $\mathbf{Z}_4$-codes: Gray images $\phi(\mathscr{G}_1^{\perp})$ are equivalent to the binary Delsarte–Goethals codes and Gray images $\phi(\mathscr{G}_1)$ have the same weight distribution as the binary Goethals codes, see [19] and Definition 2.17 below.

2.1.3 $\mathbf{Z}_4$-Goethals codes $\mathscr{G}_k$

Now we are ready to introduce the main subject of this thesis.

Definition 2.17. Let $m \geq 3$ be odd. The $\mathbf{Z}_4$-Goethals code $\mathscr{G}_k$ of length $q = 2^m$ is defined by a parity-check matrix

$$H_{\mathscr{G}_k} = \begin{pmatrix} 1 & 1 & 1 & 1 & \dots & 1 \\ 0 & 1 & \beta & \beta^2 & \dots & \beta^{q-2} \\ 0 & 2 & 2\beta^{2^k+1} & 2\beta^{(2^k+1)2} & \dots & 2\beta^{(2^k+1)(q-2)} \end{pmatrix}$$

where $1 \leq k \leq (m-1)/2$ and $\gcd(m,k) = 1$ (see Table 2.1).

The codes $\mathscr{G}_1$ and $\mathscr{G}_k$ were introduced in [19] and [22], respectively, with the results stated in the next theorem. These codes have $2^{2q-3m-2}$ codewords which means that the binary codes $\phi(\mathscr{G}_k)$ have four times as many codewords as BCH codes of the same length and minimum distance.

We extend the reduction modulo 2 mapping μ^* from Subsection 1.2.2 to a mapping from $\mathbf{Z}_4^n$ to $\mathbf{F}_2^n$ by applying μ^* to all the components. We denote this extension by μ also.

Theorem 2.18. *(i)* $d_L(\mathscr{G}_k) = 8$;

(ii) $\mu(\mathscr{G}_k) = \{\mu(\mathbf{c}) \mid \mathbf{c} \in \mathscr{G}_k\} = \mathscr{B}_k$;

(iii) $\mathscr{G}_k \cap 2\mathbf{Z}_4^q = \{\mathbf{c} \in \mathscr{G}_k \mid \operatorname{cwe}(\mathbf{c}) = Y^i, 0 \le i \le q\} = \{2\mathbf{d} \mid \mu(\mathbf{d}) \in \mathscr{H}\}$.

In [22] it was also proved that $\operatorname{lwe}(\mathscr{G}_k)$ is the same for every k. This leads to a natural question: are some of the codes $\mathscr{G}_k$ equivalent?

Theorem 2.19. *The codes $\mathscr{G}_k$ are pairwise nonequivalent.*

Proof. Suppose that $\mathscr{G}_{k'} = s \circ p(\mathscr{G}_k)$ for some permutation $p : X \to X$ and function $s : X \to \{1,3\}$. We reduce this relation modulo 2: by the previous theorem $\mu(\mathscr{G}_{k'}) = \mathscr{B}_{k'}$ and $\mu(\mathscr{G}_k) = \mathscr{B}_k$ and therefore $\mathscr{B}_{k'} = p(\mathscr{B}_k)$. By Example 2.7 the codes $\mathscr{B}_k$ are pairwise nonequivalent and we must have $k = k'$. □

In [22] the codes $\mathscr{G}_k$ were defined without the condition $k \le (m-1)/2$. This restriction assures that we get exactly all the different codes since $\mathscr{G}_k = \mathscr{G}_{m-k}$, see [38, Problem (6) in Chapter 15].

The next theorem [19] allows us to reduce the number of cases that need to be considered in the proofs of Theorems 4.5 and 5.1. From now on we view the codewords of $\mathscr{G}_k$ to be indexed with the finite field $\mathbf{F}$.

Theorem 2.20. *The codes $\mathscr{G}_k$ are invariant under the doubly transitive group of affine permutations*

$$\psi_{a,b} : \mathbf{F} \to \mathbf{F}, \quad x \mapsto ax + b, \qquad a \in \mathbf{F}^*,\ b \in \mathbf{F}.$$

Low-weight codewords and supports

Now we start studying the low-weight codewords of the codes $\mathscr{G}_k$. By Lemma 1.29 a codeword $\mathbf{c} = (c_x)_{x \in \mathbf{F}} \in \mathscr{G}_k$ should satisfy the next four equations over $\mathbf{F}$

$$\begin{aligned} &\sum_{x \in \mathbf{F}} c_x = 0 \quad (\text{in } \mathbf{Z}_4) && \sum_{x \in C_1 \cup C_3} x = 0 \\ &\sum_{\substack{x,y \in C_1 \cup C_3 \\ x<y}} xy = \sum_{x \in C_2 \cup C_3} x^2 && \sum_{x \in C_1 \cup C_3} x^{2^k+1} = 0. \end{aligned} \tag{2.2}$$

With these equations and Theorem 2.18 we can analyze the codewords of Hamming weight 8 or less.

Lemma 2.21.

(i) *If* $\mathbf{c} \in \mathscr{G}_k$ *and* $\mathrm{hwe}(\mathbf{c}) = X^i$ *with* $1 \leq i \leq 6$, *then* $\mathrm{cwe}(\mathbf{c}) \in \{Y^4, Y^6\}$;

(ii) *If* $\mathbf{c} \in \mathscr{G}_k$ *and* $\mathrm{hwe}(\mathbf{c}) = X^7$, *then* $\mathrm{cwe}(\mathbf{c}) \in \{X^6Y, X^4YZ^2, X^2YZ^4, YZ^6\}$;

(iii) *If* $\mathbf{c}, \mathbf{d} \in \mathscr{G}_k$, $\mathrm{hwe}(\mathbf{c}) = \mathrm{hwe}(\mathbf{d}) = X^7$, *and* $\chi(\mathbf{c}) = \chi(\mathbf{d})$, *then* $\mathbf{c} = \pm\mathbf{d}$;

(iv) *If* $\mathbf{c} \in \mathscr{G}_k$ *and* $\mathrm{hwe}(\mathbf{c}) = X^8$, *then* $\mathrm{cwe}(\mathbf{c}) \in \{X^8, X^6Z^2, X^4Z^4, X^2Z^6, Z^8, X^5Y^2Z, X^3Y^2Z^3, XY^2Z^5, Y^8\}$;

(v) *If* $\mathbf{c}, \mathbf{d} \in \mathscr{G}_k$, $\mathrm{swe}(\mathbf{c}) = \mathrm{swe}(\mathbf{d}) = X^6Y^2$, *and* $\chi(\mathbf{c}) = \chi(\mathbf{d})$, *then* $\mathbf{c} = \pm\mathbf{d}$.

(vi) *If* $\mathbf{c}, \mathbf{d} \in \mathscr{G}_k$, $\mathrm{swe}(\mathbf{c}) \in \{X^8, Y^8\}$, *and* $\mathrm{swe}(\mathbf{d}) = X^6Y^2$, *then* $\chi(\mathbf{c}) \neq \chi(\mathbf{d})$.

Proof. The extended Hamming code $\mathscr{H}$ contains codewords of Hamming weight 4, 6, and 8, and by (iii) in Theorem 2.18 we have codewords of cwe-type Y^4, Y^6, and Y^8 in $\mathscr{G}_k$. The binary code $\mathscr{B}_k$ has codewords of Hamming weight 6 and 8 and by (ii) in Theorem 2.18 there could be codewords of swe-types X^6Y^j and X^8 in $\mathscr{G}_k$ for some $j \geq 0$.

If $j = 0$, there would be a codeword of Lee weight 6 which contradicts (i) in Theorem 2.18. For $j \in \{1,2\}$ we list all cwe-types which satisfy the first equation in (2.2). In addition, we list all cwe-types of swe-type X^8 which satisfy the same equation. This proves the items (i), (ii), and (iv).

Suppose we have two codewords of hwe-type X^7 with the same support. They must have 2's in the same position as otherwise we would contradict the condition $d_H(\mathscr{B}_k) = 6$. Even if the 2's were in the same position, considering 1's and 3's in the other 6 positions we always contradict (i) in Theorem 2.18 except in the case $\mathbf{c} = \pm\mathbf{d}$.

Assume we have two codewords of swe-type X^6Y^2 with the same support. Again 2's must be in the same positions by $d_H(\mathscr{B}_k) = 6$ and the fact $d_L(\mathscr{G}_k) = 8$ restricts the possibilities to $\mathbf{c} = \pm\mathbf{d}$.

Let $\mathbf{c}$ and $\mathbf{d}$ be codewords in the item (vi) and suppose they have the same support. If $\mathbf{c}$ is of swe-type X^8, then $2\mathbf{c}$ is of swe-type Y^8 and we can assume $\mathbf{c}$ to be of swe-type Y^8. Thus we have codeword $2\mathbf{d}$ of swe-type Y^6 within the support of $\mathbf{c}$ which contradicts the fact $d_H(\mathscr{H}) = 4$ by (iii) in Theorem 2.18. □

2.2 Designs

In this section we introduce t-designs and review some basic results about them. We also show how certain designs can be constructed from error-correcting codes. These designs are needed in the construction of new designs in Chapters 4 and 5. For the results in this section the reader is referred to [38, 33, 24].

Definition 2.22. A t-(v,k,λ) *design* is a pair (X,B) where X is a v-element set of *points* and B is a collection of k-element subsets of X (called *blocks*) with the property that every t-element subset of X is contained in exactly λ blocks. A design is *simple* if all the blocks are distinct; otherwise, the design is said to have *repeated blocks*.

Almost all of the designs in this thesis are simple and therefore the simplicity is not always mentioned. If a design has repeated blocks, it is explicitly stated.

Theorem 2.23. *If (X,B) is a t-(v,k,λ) design and T is any s-element subset of X, with $0 \leq s \leq t$, then the number of blocks containing T is*

$$b_s = |\{A \in B \mid T \subseteq A\}| = \lambda \tbinom{v-s}{t-s} / \tbinom{k-s}{t-s}.$$

In particular, b_s is an integer and (X,B) is a s-(v,k,b_s) design. The number of blocks is equal to b_0 satisfying

$$b_0 \tbinom{k}{t} = \lambda \tbinom{v}{t}.$$

Let $p : X \to X$ be a permutation of the point set X. There is a natural action of p to the blocks $b \subseteq X$ defined by $p(b) = \{p(a) \mid a \in b\}$ and to the whole t-design defined by $p(B) = \{p(b) \mid b \in B\}$.

Definition 2.24. Two t-designs (X,B) and (X,B^*) are *equivalent* (or *isomorphic*) if $B^* = p(B)$ for some permutation $p : X \to X$. Otherwise they are *nonequivalent*.

2.2.1 Designs from linear codes over $\mathbf{F}_2$

We present now the celebrated Assmus–Mattson theorem [1] which is a powerful tool in constructing t-designs from linear codes over finite fields. For simplicity we restrict ourselves to $\mathbf{F}_2$ and we can identify codewords with their supports.

Theorem 2.25 (Assmus–Mattson). *Let C be a binary $[n,k,d]$ linear code and $(B_i)_{i=0}^n$ the weight distribution of $C^\perp$. Suppose we can find an integer t, with $0 < t < d$, such that there are at most $d-t$ nonzero B_i's in the range $1 \leq i \leq n-t$. Then for any $i \geq d$ the supports of size i in C form a simple t-design.*

From now on we have $n = q = 2^m$.

Example 2.26 (Extended Hamming codes). We show how Theorem 2.25 is applied to Example 2.6. The Assmus–Mattson theorem is applicable with $t = 3$ since there are only one nonzero B_i in the range $1 \leq i \leq q-3$. So the supports of any fixed size in $\mathscr{H}$ define a simple 3-design. We can calculate the weight distribution of $\mathscr{H}$ by Theorem 2.4 and the corresponding λ's by Theorem 2.23. As an example we list below the three first 3-designs. We recall that the blocks of these designs can be identified with the supports of cwe-type Y^i in $\mathscr{G}_k$ by item (iii) in Theorem 2.18.

(i) The supports of size 4 in $\mathscr{H}$ form a 3-$(q,4,1)$ design.

(ii) The supports of size 6 in $\mathscr{H}$ form a 3-$\left(q,6,\frac{(q-4)(q-8)}{6}\right)$ design.

(iii) The supports of size 8 in $\mathscr{H}$ form a 3-$\left(q,8,\frac{(q-4)(q-6)(q^2-15q+71)}{120}\right)$ design.

Example 2.27 (Extended two-error-correcting BCH codes). We continue with Example 2.7 so $q=2^m$ with odd m. The Assmus–Mattson theorem is again applicable with $t=3$ as there are only three nonzero B_i's in the range $1\le i\le q-3$.

(i) The supports of size 6 in $\mathscr{B}_k$ form a 3-$\left(q,6,\frac{q-8}{6}\right)$ design.

(ii) The supports of size 8 in $\mathscr{B}_k$ form a 3-$\left(q,8,\frac{q^3-25q^2+246q-760}{120}\right)$ design.

Example 2.28 (Reed–Muller codes). We continue with Example 2.8. Instead of the Assmus–Mattson theorem we use the affine geometry $AG(\mathbf{F})$ to get 3-designs from the minimum weight codewords in $RM(m-3,m)$. Recall that these codewords are exactly the 3-flats in $AG(\mathbf{F})$.

Choose three distinct points from $AG(\mathbf{F})$. They define a unique 2-flat. We can choose a point outside this 2-flat in $q-4$ ways and this fifth point determines a 3-flat. Clearly, there are four choices which lead to the same 3-flat and thus there are $(q-4)/4$ different 3-flats which contain the three fixed points.

- The supports of size 8 in $RM(m-3,m)$ define a 3-$\left(q,8,\frac{q-4}{4}\right)$ design.

2.2.2 Designs from linear codes over $\mathbf{Z}_4$

For linear $\mathbf{Z}_4$-codes we do not have such a powerful tool as the Assmus–Mattson theorem above. There have been some attempts to generalize this theorem to $\mathbf{Z}_4$ but the results are much more complicated and restricted than the original one. This is natural as $\mathbf{Z}_4$ is a ring and not a field.

Tanabe [54] gives one Assmus–Mattson theorem for $\mathbf{Z}_4$-codes but it does not give any designs from the $\mathbf{Z}_4$-Goethals codes $\mathscr{G}_k$. The required calculations are messy and not included in this thesis; see also comments in [24].

An Assmus–Mattson type theorem by Shin, Kumar and Helleseth [52] does not imply our main results, Theorems 4.5 and 5.1, but it gives us the next theorem [52, Corollary 8] which is used in the proof of Corollary 4.8.

Theorem 2.29. *The supports of any fixed hwe-type in $\mathscr{G}_1$ form a* 3*-design possibly with repeated blocks.*

The proof of Theorem 2.29 makes use of the next theorem [51].

Theorem 2.30. *The supports of size* 7 *in $\mathscr{G}_1$ form a* 3-$\left(q,7,\frac{14}{3}(q-8)\right)$ *design.*

In Chapter 5 we try to generalize this theorem for the codes $\mathscr{G}_k$ with different values of k. Let us assume that we can prove the analogue of Theorem 2.30 for a code $\mathscr{G}_k$ with some value of $k > 1$. The analogue of Theorem 2.29 will then also hold. This is because a study of the proof of Theorem 2.29 in [52] reveals that a reference to Theorem 2.30 is the only step of the argument where the assumption $k = 1$ is needed.

We recall two classical related results [49, 3] in the form of one theorem. A binary distance invariant (for the definition see [38, p. 40]) code is called Preparata-like or Goethals-like if it has the same weight distribution as $\phi(\mathscr{P})$ or $\phi(\mathscr{G}_k)$, respectively.

Theorem 2.31. *The supports of fixed size in any Preparata-like code form a* 3*-design. The supports of fixed size in any Goethals-like code form a* 3*-design.*

From this theorem we derive one 3-design needed in Section 4.4. We can count the number of codewords of Hamming weight 8 in $\phi(\mathscr{G}_k)$ and hence the corresponding λ. This parameter can be derived also from [3, Theorem 3] or more directly from [28, Proposition 1].

Corollary 2.32. *The supports of size* 8 *in the Goethals-like code* $\phi(\mathscr{G}_k)$ *form a* $3\text{-}\left(2q, 8, \frac{(2q-4)(4q-17)}{60}\right)$ *design.*

Historical notes II

Research on constructing t-designs from $\mathbf{Z}_4$-codes started with articles [18, 20] where it was shown by computer searches that in the $\mathbf{Z}_4$-Golay code the supports of hwe-type X^{10} and X^{12} yield 5-$(24,10,36)$ and 5-$(24,12,1584)$ designs, respectively. These results were later proved analytically in three different ways [6, 53, 54].

In addition to the above interesting but restricted designs, Helleseth, Kumar, and Yang [23] have constructed an infinite family of 3-designs from the $\mathbf{Z}_4$-Preparata codes $\mathscr{P}$. The supports of hwe-type X^5 form a 3-$(2^m,5,10)$ design for all odd $m \geq 3$. Also the supports of the $\mathbf{Z}_4$-Kerdock codes $\mathscr{K}$ contain infinite families of 3-designs [55].

By Example 2.26 and Lemma 2.21 we see that supports of size ≤ 6 in the $\mathbf{Z}_4$-Goethals codes $\mathscr{G}_k$ yield classical 3-designs. Shin, Kumar, and Helleseth [51] settled the next case, i.e. supports of size 7 in $\mathscr{G}_1$, in Theorem 2.30. In Chapters 4 and 5 we find some 3-designs from supports of size 8 in $\mathscr{G}_k$.

For a survey the reader is referred to [24].

Chapter 3

Decoding algorithm

In this chapter we describe an algebraic decoding algorithm for all the $\mathbf{Z}_4$-Goethals codes $\mathscr{G}_k$ which corrects all errors up to the error-correcting capability. This algorithm has been presented in [46] and is a generalization of a complete decoding algorithm for $\mathscr{G}_1$ by Helleseth and Kumar [21].

3.1 Decoding problem

We have seen that $d_L(\mathscr{G}_k) = 8$ and thus look for an efficient decoding algorithm which corrects all errors with Lee weight at most 3. Next we describe one such an algorithm. As in Lemma 1.29 the variables in the Teichmüller set $\mathscr{T}$ and their modulo 2 reductions in $\mathbf{F}$ are denoted by X,Y,Z,A,B,C and x,y,z,a,b,c, respectively.

We modify the setting in Subsection 2.1.1 to $\mathbf{Z}_4$-domain: the receiver gets the word $\mathbf{r} \in \mathbf{Z}_4^q$ which differs from the original codeword $\mathbf{c}$ by an error word $\mathbf{e} = (e_X)_{X\in\mathscr{T}} \in \mathbf{Z}_4^q$, i.e., $\mathbf{r} = \mathbf{c} + \mathbf{e}$. We calculate the *syndrome* of the received vector

$$\mathbf{S} = \mathbf{r}H_{\mathscr{G}_k}^T = \mathbf{c}H_{\mathscr{G}_k}^T + \mathbf{e}H_{\mathscr{G}_k}^T = \mathbf{e}H_{\mathscr{G}_k}^T = (t, A+2B, 2C)$$

where $t \in \mathbf{Z}_4$ and $A,B,C \in \mathscr{T}$. This presentation with $\mathscr{T}$ is possible by Lemma 1.27 and with Lemma 1.29 it transforms to the following system of equations:

$$t = \sum_{x\in\mathbf{F}} e_x \quad (\text{in } \mathbf{Z}_4) \qquad\qquad a = \sum_{x\in E_1\cup E_3} x$$

$$b = \sum_{\substack{x,y\in E_1\cup E_3 \\ x<y}} xy + \sum_{x\in E_2\cup E_3} x^2 \qquad\qquad c = \sum_{x\in E_1\cup E_3} x^d$$

where we abbreviate $d = 2^k + 1$. Now the task for the decoder is: given any syndrome, decide what codeword was most likely sent, or, for any syndrome give the minimum weight codeword $\mathbf{e}$ (leader) in the corresponding coset $\mathbf{e} + \mathscr{C}$.

We will divide the discussion into four cases depending on the value of t. As examples we have expanded the resulting polynomial conditions in the case $k = 2$. The case $k = 1$ was described in [21].

Observing that syndrome

$$-\mathbf{S} = (-t, -(A+2B), -2C) = (-t, A+2(A+B), 2C)$$

corresponds to the error vector $-\mathbf{e}$ we can reduce the number of different error patterns that need to be considered. The case $t = 3$ is reduced to the case $t = 1$: If we have a syndrome $\mathbf{S} = (3, A+2B, 2C)$ we decode with a syndrome $-\mathbf{S} = (1, A+2(A+B), 2C)$ and get an error vector $\mathbf{e}$. The actual error vector is then $-\mathbf{e}$.

3.2 Case of $t = 0$

Theorem 3.1. *Let* $\mathbf{S} = (0, A+2B, 2C)$ *denote the syndrome of a coset.*

(i) If $a = b = c = 0$*, then* $\mathbf{0}$ *is the coset leader.*

(ii) If $a \neq 0$ *and* $c = \left(b^2/a + a\right)^d + \left(b^2/a\right)^d$*, then the coset leader has Lee weight* 2 *and is uniquely determined by* $x = b^2/a + a$*,* $e_X = 1$*,* $y = b^2/a$*, and* $e_Y = 3$*. In particular, if* $k = 2$*, the latter condition can be rewritten in the form* $a^8 + a^6 b^2 + b^8 + a^3 c = 0$*.*

(iii) If (i) and (ii) do not hold, then any coset leader has Lee weight ≥ 4*.*

Proof. (i) Clear.

(ii) Suppose we have an error of Lee weight 2 where $e_X = 1$, $e_Y = 3$, and $X \neq Y$. This leads to the syndrome equations

$$\begin{aligned} a &= x + y \\ b^2 &= xy + y^2 \\ c &= x^d + y^d. \end{aligned}$$

Since $X \neq Y$ it follows that $a = x + y \neq 0$. The first two equations have the unique solution

$$x = \frac{b^2}{a} + a \quad \text{and} \quad y = \frac{b^2}{a}$$

which satisfies the third equation if and only if

$$c = \left(\frac{b^2}{a} + a\right)^d + \left(\frac{b^2}{a}\right)^d.$$

(iii) If cases (i) and (ii) do not hold, we detect an error of Lee weight ≥ 4, since the conditions in (i) and (ii) describe all cosets of Lee weight 0 and 2, respectively, where $t = 0$.

□

3.3 Case of $t = 1$

Theorem 3.2. *Let* $\mathbf{S} = (1, A + 2B, 2C)$ *denote the syndrome of a coset.*

(i) If $b = 0$ *and* $c = a^d$*, then the coset leader has Lee weight* 1 *and is uniquely determined by* $x = a$ *and* $e_X = 1$.

(ii) If $b \neq 0$ *and* $c = a^d$*, then the coset leader has Lee weight* 3 *and is uniquely determined by* $x = a + b$*,* $e_X = 2$*,* $y = a$*, and* $e_Y = 3$.

(iii) If $b \neq 0$*,* $c \neq a^d$ *and* $\mathrm{Tr}\left(b^d / \left(a^d + c\right)\right) = 0$*, then the coset leader has Lee weight* 3*. The coset leader is uniquely determined by* $e_X = e_Y = 1$*,* $e_Z = 3$*,* $D_{d-2}\left(z + a, b^2\right) = \left(a^d + c\right) / b^2$*, and* x *and* y *are the zeros of* $T^2 + (z+a)T + b^2 + az = 0$*. In the case* $k = 2$*, the variable* z *should satisfy*

$$(z+a)^3 + b^2(z+a) = \left(a^5 + c\right) / b^2.$$

(iv) If $b \neq 0$*,* $c \neq a^d$*,* $\mathrm{Tr}\left(b^d / \left(a^d + c\right)\right) = 1$*, and*

$$p(T) = T^3 + aT^2 + \left(a^2 + b^2\right) T + \sigma_3$$

has three distinct zeros in $\mathbf{F}$ *where* σ_3 *satisfies*

$$D_n\left(\sigma_3 + a^3 + ab^2, b^6\right) = \left(a^d + c\right) \Big/ f$$

and

$$\begin{cases} n = d/3 \text{ and } f = 1, & \text{if } 2 \nmid k \\ n = (d-2)/3 \text{ and } f = b^2, & \text{if } 2 \mid k \end{cases}$$

then the coset leader has Lee weight 3 *and is uniquely determined such that* x, y, z *are the three distinct zeros of* $p(T)$ *in* $\mathbf{F}$ *and* $e_X = e_Y = e_Z = 3$*. Especially when* $k = 2$*, the term* σ_3 *should satisfy* $\sigma_3 = \left(c + a^5 + a^3 b^2 + ab^4\right) / b^2$.

(v) If none of (i)–(iv) hold, then any coset leader has Lee weight ≥ 5.

Proof. (i) Consider a single error in the location X with $e_X = 1$. Then $a = x$, $b = 0$, and $c = x^d = a^d$ and the coset leader with this syndrome is, therefore, uniquely determined by $x = a$ and $e_X = 1$.

(ii) In the case of an error of Lee weight 3 where $e_X = 2$, $e_Y = 3$, and $X \neq Y$, we obtain the syndrome equations

$$\begin{aligned} a &= y \\ b^2 &= x^2 + y^2 \\ c &= y^d. \end{aligned}$$

Since $X \neq Y$ we have $b = x + y \neq 0$. The above system of equations has a solution if and only if $c = a^d$ and in this case the solution gives the coset leader uniquely determined by

$$x = a + b \quad \text{and} \quad y = a$$

where $e_X = 2$ and $e_Y = 3$.

(iii) Suppose we have an error of Lee weight 3 where $e_X = e_Y = 1$ and $e_Z = 3$ such that X, Y, and Z are pairwise-distinct. We get the syndrome equations

$$\begin{aligned} a &= x + y + z \\ b^2 &= xy + xz + yz + z^2 \\ c &= x^d + y^d + z^d. \end{aligned}$$

If $B = 0$, we would have a codeword of Lee weight 4 in $\mathscr{P}$ with $e_X = e_Y = 1$ and $e_Z = e_A = 3$. By Example 2.16 we know that $d_L(\mathscr{P}) = 6$ and therefore $b \neq 0$. From the first two equations we see that $xy = az + b^2$ and using (1.1) and Lemma 1.15 we derive (notice that $d - 1 = 2^k$)

$$\begin{aligned} c =& D_d(x + y, xy) + z^d \\ =& D_d\left(z + a, az + b^2\right) + z^d \\ =& D_d(z + a, az) + D_d\left(z + a, b^2\right) + (z + a)^d + z^d \\ =& a^d + (z + a)D_{d-1}\left(z + a, b^2\right) + b^2 D_{d-2}\left(z + a, b^2\right) + (z + a)^d \\ =& a^d + b^2 D_{d-2}\left(z + a, b^2\right). \end{aligned}$$

All in all we have

$$D_{d-2}\left(z + a, b^2\right) = \frac{a^d + c}{b^2} \tag{3.1}$$

and $s = \gcd(d - 2, q - 1) = 2^{\gcd(k,m)} - 1 = 1$.

Assume we could solve z from the previous equation. Then we could find x and y as roots of the equation

$$T^2 + (z + a)T + b^2 + az = 0.$$

This has two roots in $\mathbf{F}$ if and only if

$$\mathrm{Tr}\left(\frac{b^2 + az}{(z + a)^2}\right) = \mathrm{Tr}\left(\frac{b}{z + a}\right) = \mathrm{Tr}\left(\frac{b^d}{a^d + c}\right) = 0$$

by Lemma 1.4, (3.1), and Lemma 1.19. So when we have this error pattern the above condition must hold and therefore we can also compute the unique root of (3.1) by Theorem 1.20.

(iv) Consider the error of Lee weight 3 with distinct error locations X, Y, and Z where $e_X = e_Y = e_Z = 3$. This leads to the syndrome equations

$$\begin{aligned} a &= x+y+z \\ b^2 &= xy+xz+yz+x^2+y^2+z^2 \\ c &= x^d+y^d+z^d. \end{aligned}$$

If B would be 0, we would have a codeword of Lee weight 4 with $e_X = e_Y = e_Z = e_A = 3$ in $\mathscr{P}$. Again, Example 2.16 implies $b \neq 0$. We know that x, y, and z are the zeros of the polynomial

$$p(T) = T^3 + aT^2 + \left(a^2+b^2\right)T + \sigma_3$$

where $\sigma_3 = xyz$. We need to find σ_3.

From the syndrome equations we get $xy = z^2+a^2+az+b^2$ and by (1.1) and Lemma 1.15

$$\begin{aligned} c =& D_d(x+y,xy)+z^d \\ =& D_d\left(z+a,z^2+a^2\right)+D_d(z+a,az)+D_d\left(z+a,b^2\right)+z^d \\ =& (k+1)(z+a)^d+a^d+D_d\left(z+a,b^2\right). \end{aligned}$$

If $2 \nmid k$, then $3 \mid d$ and

$$c = a^d + D_{d/3}\left(D_3\left(z+a,b^2\right),b^6\right).$$

If $2 \mid k$, then $3 \mid (d-2)$ and

$$\begin{aligned} c =& (z+a)^d+a^d+(z+a)D_{d-1}\left(z+a,b^2\right)+b^2D_{d-2}\left(z+a,b^2\right) \\ =& a^d+b^2D_{(d-2)/3}\left(D_3\left(z+a,b^2\right),b^6\right). \end{aligned}$$

In addition,

$$D_3\left(z+a,b^2\right) = p(z)+\sigma_3+a^3+ab^2 = \sigma_3+a^3+ab^2 \tag{3.2}$$

and we conclude that

$$D_n\left(\sigma_3+a^3+ab^2,b^6\right) = \frac{a^d+c}{f} \tag{3.3}$$

where

$$\begin{cases} n = d/3 \text{ and } f = 1, & \text{if } 2 \nmid k \\ n = (d-2)/3 \text{ and } f = b^2, & \text{if } 2 \mid k. \end{cases}$$

The polynomial $p(T)$ has three zeros in $\mathbf{F}$ if and only if (3.2) has three roots in $\mathbf{F}$. By Theorem 1.18 ($s = 1$, $r = 3$) and Lemma 1.19 this requires that $\sigma_3 + a^3 + ab^2 \neq 0$ and

$$\mathrm{Tr}\left(\frac{b}{z+a}\right) = \mathrm{Tr}\left(\frac{b^3}{\sigma_3 + a^3 + ab^2}\right) = 1.$$

By Lemma 1.19 ($s = \gcd(n, q-1) = 1$) and (3.3) the above trace condition is equivalent to

$$\mathrm{Tr}\left(\frac{b^{3n}}{D_n\left(\sigma_3 + a^3 + ab^2, b^6\right)}\right) = \mathrm{Tr}\left(\frac{b^d}{a^d + c}\right) = 1$$

but this is always true as otherwise we would be in the case (iii). This means that, when σ_3 satisfies (3.3), then $p(T) = 0$ has either zero or three roots.

It is straightforward to see that

$$r = \gcd(n, q+1) = \begin{cases} 1, & \text{if } 3 \nmid k \\ 3, & \text{if } 3 \mid k. \end{cases}$$

When $3 \nmid k$ we can find the unique root of (3.3) by Theorem 1.20 and then get the zeros x, y and z of $p(T)$. When $3 \mid k$ we compute three roots of (3.3) which are then the candidate values for σ_3. For two of the candidates the resulting polynomial $p(T)$ has no zeros, and for the correct candidate σ_3 the polynomial has three zeros, which are then x, y, and z.

(v) In all other cases, when $t = 1$ we detect an error of Lee weight ≥ 5.

□

Of all the cases, (iv) is computationally the most demanding. Syndrome with the coset leader of Lee weight 5 and $t = 1$ gives in the worst case three different guesses for σ_3 and for none of them $p(T)$ has three zeros.

Time consumption can be reduced by using more lookup tables. One table could have "true" in index δ if and only if $x^3 + x = \delta$ has three roots. With the aid of such a table one can quickly check when $p(T)$ has three zeros. Another table could list all $(q+1)$th roots of unity in the quadratic extension of $\mathbf{F}$. This can be used to speed up the computation of nth roots in this larger field.

3.4 Case of $t = 2$

Theorem 3.3. *Let* $\mathbf{S} = (2, A + 2B, 2C)$ *denote the syndrome of a coset.*

(i) If $a = c = 0$*, then the coset leader has Lee weight* 2 *and is uniquely determined by* $x = b$ *and* $e_X = 2$.

(ii) If $a \neq 0$, $c = D_d\left(a, b^2\right)$, and $\mathrm{Tr}(b/a) = 0$, then the coset leader has Lee weight 2 and is uniquely determined such that x and y are zeros of $T^2 + aT + b^2 = 0$ and $e_X = e_Y = 1$. Especially when $k = 2$, then c should be $a^5 + a^3b^2 + ab^4$.

(iii) If $a \neq 0$, $c = D_d\left(a, a^2 + b^2\right)$, and $\mathrm{Tr}(b/a) = 1$, then the coset leader has Lee weight 2 and is uniquely determined such that x and y are zeros of $T^2 + aT + a^2 + b^2 = 0$ and $e_X = e_Y = 3$. In particular, if $k = 2$, then c should be $a^5 + a^3b^2 + ab^4$.

(iv) If (i)–(iii) do not hold, then any coset leader has Lee weight ≥ 4.

Proof. (i) Consider a single error in the location X with $e_X = 2$. Then $a = c = 0$ and $b^2 = x^2$.

(ii) In the case of an error of Lee weight 2 where $e_X = e_Y = 1$ and $X \neq Y$ we obtain the syndrome equations

$$\begin{aligned} a &= x + y \\ b^2 &= xy \\ c &= x^d + y^d. \end{aligned}$$

Since $X \neq Y$ we have $a \neq 0$. The first two equations imply that x and y are the roots of $T^2 + aT + b^2 = 0$. By Lemma 1.4 this can happen if and only if

$$\mathrm{Tr}\left(\frac{b^2}{a^2}\right) = \mathrm{Tr}\left(\frac{b}{a}\right) = 0.$$

Then x and y obey the third equation if and only if $c = D_d(x + y, xy) = D_d\left(a, b^2\right)$ which is given explicitly in (1.2).

(iii) Assume error of Lee weight 2 where $e_X = e_Y = 3$ and $X \neq Y$. As mentioned in the beginning of this section, we can now consider error $-\mathbf{e}$ as in the case (ii) with one difference: we replace b^2 by $(a+b)^2 = a^2 + b^2$. So $x + y = a \neq 0$, $xy = a^2 + b^2$, and the equation $T^2 + aT + a^2 + b^2 = 0$ should have two roots in $\mathbf{F}$. This condition is equivalent to

$$\mathrm{Tr}\left(\frac{a^2 + b^2}{a^2}\right) = \mathrm{Tr}\left(\frac{b}{a}\right) + 1 = 0.$$

(iv) In all other cases than (i)-(iii) with $t = 2$ an error of Lee weight ≥ 4 is detected.

□

By Lemma 1.15 we get that

$$D_d\left(a, a^2+b^2\right) = D_d\left(a, b^2\right) + \begin{cases} a^d, & \text{if } 2 \nmid k \\ 0, & \text{if } 2 \mid k. \end{cases}$$

In the case $2 \mid k$ we could implement the algorithm in a slightly different order: if $c = D_d\left(a, b^2\right)$, then we may branch into the cases (ii) and (iii) according to the value of $\mathrm{Tr}(b/a)$.

Historical notes III

The $\mathbf{Z}_4$-Kerdock codes have a Hadamard-transform soft-decision decoding algorithm presented already in the seminal paper [19]. In the same article an algebraic syndrome decoder for the $\mathbf{Z}_4$-Preparata codes was introduced. This algorithm includes similar case-by-case analysis as the decoder above.

Helleseth and Kumar [21] presented a complete decoding algorithm for the $\mathbf{Z}_4$-Goethals code $\mathscr{G}_1$. Our algorithm above generalizes this to all codes $\mathscr{G}_k$ except that our algorithm works only up to the error-correcting capability and is thus not complete. Some of the cases in the complete decoder [21] can be generalized with Dickson polynomials for every k but we could not solve two hard cases.

There has been an intensive search for other good linear $\mathbf{Z}_4$-codes, see for example tables in [31], but only a few have been found. These include two remarkable linear $\mathbf{Z}_4$-codes discovered in [7, 8]: they have length 32, minimum distances 12 and 14, and 2^{37} and 2^{32} codewords, respectively. The 5-error-correcting code has similar algebraic decoding algorithm [48] as above but for the 6-error-correcting code this approach seems to fail. For this latter code another approach is outlined in [35].

Chapter 4

New 3-designs from codes $\mathscr{G}_1$

In this chapter we derive many families of 3-designs with block size 8 from the $\mathbf{Z}_4$-Goethals code $\mathscr{G}_1$. In the next chapter we generalize these designs for certain other values of k. The results in this chapter are taken from [47].

4.1 Classification of supports of size 8

In order to get small 3-designs with block size 8 from the codes $\mathscr{G}_k$ we have to analyze the supports of size 8. Below we abbreviate sentences by using phrase "support of swe-type X^8" instead of "support of codeword of swe-type X^8".

We have seen in Lemma 2.21 that all possible swe-types of supports of size 8 are Y^8, X^8, and X^6Y^2. Let us consider more closely the relations between the $\mathbf{Z}_4$-code $\mathscr{G}_k$ and the binary codes $\mathscr{H}$ and $\mathscr{B}_k$. By Theorem 2.18 the supports of swe-type Y^8 can be identified with codewords of Hamming weight 8 in $\mathscr{H}$. By the same theorem the supports of swe-type X^8 are codewords in $\mathscr{B}_k$ but not all codewords of Hamming weight 8 in $\mathscr{B}_k$ are necessarily supports of swe-type X^8 — they can be μ-images of codewords with larger supports.

Definition 4.1. Let $\mathbf{c} \in \mathscr{B}_k$ have a support S of size i. If there is a codeword $\mathbf{d} \in \mathscr{G}_k$ of swe-type X^i such that $\mu(\mathbf{d}) = \mathbf{c}$, we say that $\mathbf{c}$ can be *lifted exactly* to $\mathscr{G}_k$. The set of codewords which can be lifted exactly to $\mathscr{G}_k$ is denoted by $\mathscr{B}_k^*$.

Lemma 4.2. *Supports of hwe-type X^8 in $\mathscr{G}_k$ divide into the following distinct classes:*

(A) Supports of size 8 in $\mathscr{H} \setminus \mathscr{B}_k$;

(B) Supports of size 8 in $\mathscr{B}_k \setminus \mathscr{B}_k^*$;

(C) Supports of size 8 in $\mathscr{B}_k^*$;

(D) Supports of swe-type X^6Y^2.

Proof. The classes (A)–(B) are clearly distinct and contain all supports of cwe-type Y^8 in $\mathcal{G}_k$ which are not in (C). The class (C) contains all supports of swe-type X^8 in $\mathcal{G}_k$. By (vi) in Lemma 2.21 the class (D) is distinct from (A)–(C). □

The relation between the codewords and the corresponding supports are simple in the classes (A) and (B): there is exactly one codeword for each support. By (v) and (vi) in Lemma 2.21 there are always two codewords for each support in the class (D). The class (C) is more complicated. For example, there are codewords like 11111111 and 11113333 which have the same support. For further analysis of the class (C) we need to introduce the concept of lifting rank.

Definition 4.3. Let S be a subset of the index set $\mathbf{F}$. The *lifting rank* of S is $4^{k_1}2^{k_2}$ if a generator matrix of a subcode $\mathcal{G}_k|_S = \{\mathbf{c} \in \mathcal{G}_k \mid \chi(\mathbf{c}) \subseteq S\}$ is permutation-equivalent to a matrix of the form

$$G_S = \begin{pmatrix} I_{k_1} & A & B \\ 0 & 2I_{k_2} & 2C \end{pmatrix}.$$

From now on we consider only the lifting ranks of supports of swe-type X^8 and hence we always have $k_1 = 1$. We abbreviate by saying that such a support has (lifting) rank k_2.

The rank counts linearly independent codewords of cwe-type Y^4 within the support. It is easy to see that $0 \leq k_2 \leq 3$. The supports of rank 3 are special: they are 3-flats in the affine geometry $AG(\mathbf{F})$, that is, minimum weight words in $RM(m-3,m)$, see Subsection 1.1.2 and Example 2.8. In the next lemma we analyze the possible ranks and the corresponding subcodes. This analysis divides the class (C) into five subclasses.

Lemma 4.4. *Supports of swe-type X^8 in $\mathcal{G}_k$ divide into the following distinct classes:*

(i) *S has rank 3 and* $\operatorname{cwe}\left(\mathcal{G}_k|_S\right) = X^8 + 14X^4Z^4 + Z^8 + \left(W^8 + 14W^4Y^4 + Y^8\right)$.

(ii) *S has rank 1 and* $\operatorname{cwe}\left(\mathcal{G}_k|_S\right) = X^6Z^2 + 2X^4Z^4 + X^2Z^6 + \left(W^8 + 2W^4Y^4 + Y^8\right)$.

(iii) *S has rank 0 and* $\operatorname{cwe}\left(\mathcal{G}_k|_S\right) = X^6Z^2 + X^2Z^6 + \left(W^8 + Y^8\right)$.

(iv) *S has rank 0 and* $\operatorname{cwe}\left(\mathcal{G}_k|_S\right) = X^8 + Z^8 + \left(W^8 + Y^8\right)$.

(v) *S has rank 0 and* $\operatorname{cwe}\left(\mathcal{G}_k|_S\right) = 2X^4Z^4 + \left(W^8 + Y^8\right)$.

Proof. If S has rank 3, it is a 3-flat in $AG(\mathbf{F})$ and a codeword in $RM(m-3,m)$. A $\mathbf{Z}_4$-word of cwe-type X^8 and with a 3-flat support satisfies all the equations (2.2) by Examples 1.12 and 2.8. We can take any 2-flat within the 3-flat and change 1's to 3's in these positions obtaining another codeword in $\mathcal{G}_k$. The 3-flat contains 14 different 2-flats and the cwe of the subcode follows.

If $S = \{x_1, x_2, \ldots, x_8\}$ has rank ≥ 1 but is not a 3-flat, there is a 2-flat, say, $\{x_1, x_2, x_3, x_4\}$ in S and we can extend it to a 3-flat $\{x_1, x_2, x_3, x_4, x_5, y_1, y_2, y_3\}$, $y_i \notin S$. This 3-flat support is in the class (i) and considering case-by-case we see that the 2-flat $\{x_1, x_2, x_3, x_4\}$ must have either 1 or 3 positions with a 3-symbol. So only the combination (ii) can exist and then codewords 11131113 and 11133331 have the same support, that is, in a codeword of cwe-type X^6Z^2 both 2-flats include one 3-position. All other possibilities contradict with $d_L(\mathscr{G}_k) = 8$.

The classes (iii)–(v) clearly list all types of supports of rank 0. □

In Example 4.10 we will see that when $m = 5$ only the classes (i) and (ii) are nonempty. By computer we have checked that with $m \in \{7, 9\}$ all classes are nonempty and it is reasonable to expect that this is true also with $m \geq 11$.

4.2 Main results

We state now the main theorem and deduce some corollaries. All the design families in this chapter are new in the sense that they are not listed in [33, Table 3.31]: the known infinite families of simple t-designs with $t \geq 3$. From now on $k = 1$ and we consider only the code $\mathscr{G}_1$.

Theorem 4.5. *The class (ii) defines a* 3-$\left(q, 8, \frac{14}{3}(q-8)\right)$ *design.*

The proofs of Theorem 4.5 and Corollary 4.6 are postponed to Sections 4.3 and 4.4, respectively.

Corollary 4.6. *The class (C) forms a* 3-$\left(q, 8, \frac{32q^2-985q+5892}{60}\right)$ *design.*

Corollary 4.7. *The class (B) defines a* 3-$\left(q, 8, \frac{(q-8)(q-32)(q-49)}{120}\right)$ *design.*

Proof. Subtract λ in Corollary 4.6 from λ in (ii) in Example 2.27. □

Corollary 4.8. *The class (D) forms a* 3-$\left(q, 8, \frac{56}{15}(q-8)(q-12)\right)$ *design.*

Proof. By Theorem 2.29 the codewords of hwe-type X^8 define a 3-design with repeated blocks. We can count its parameter $\lambda^* = (q^4 - 25q^3 + 1269q^2 - 21390q + 100648)/120$ from cwe$(\mathscr{G}_1^\perp)$ [52] by Theorems 2.14 and 2.23. This design contains codewords of swe-types Y^8, X^8, and X^6Y^2 by Lemma 2.21. We drop out all codewords of swe-types Y^8 and X^8, and by (iii) in Example 2.26 and λ' in (4.7) in page 53 we get a 3-design with λ equal to

$$\lambda^* - \lambda_{2.26(\mathrm{iii})} - \lambda' = \frac{112}{15}(q-8)(q-12).$$

We take the supports of the remaining codewords and by item (v) in Lemma 2.21 we get a simple 3-design with a parameter $\lambda/2$. □

Corollary 4.9. *The supports of size* 8 *in* $\mathscr{G}_1$ *form a* 3-$(q,8,\lambda)$ *design with*

$$\lambda = \frac{q^4 - 25q^3 + 693q^2 - 10030q + 44712}{120}.$$

Proof. Add λ in (iii) in Example 2.26 to λ in Corollary 4.8. □

Example 4.10 (3-designs with $q = 32$). The designs of length 32 are quite different from the longer ones. By counting the parameters of all designs above we see that the classes (iii)–(v) and (B) are empty. All in all we get only three new designs:

- 3-$(32,8,112)$ design (class (ii))
- 3-$(32,8,1792)$ design (class (D))
- 3-$(32,8,5523)$ design (all supports of size 8)

Duursma et al. [15] noticed that for the length 32 the automorphism group of $\mathscr{G}$ is 3-homogeneous (any 3-subset can be mapped to an arbitrary 3-subset) and hence codewords of any fixed cwe-type form a 3-design possibly with repeated blocks. Applying this result to the second design we can split it into 3-$(32,8,672)$ and 3-$(32,8,1120)$ designs corresponding to the cwe-types X^5Y^2Z and $X^3Y^2Z^3$, respectively.

Interestingly, we have 3-$(32,6,112)$, 3-$(32,7,112)$, and 3-$(32,8,112)$ designs by (ii) in Example 2.26, Theorem 2.30, and Theorem 4.5, respectively.

Example 4.11 (3-designs with $q = 128$). Now all classes (i)–(v) and (A)–(D) are nonempty and we get all five new designs:

- 3-$(128,8,560)$ design (class (ii))
- 3-$(128,8,6735)$ design (class (C))
- 3-$(128,8,7584)$ design (class (B))
- 3-$(128,8,51968)$ design (class (D))
- 3-$(128,8,1884347)$ design (all supports of size 8)

We claim by computer calculations that the design from class (D) no longer splits into two designs corresponding the cwe-types X^5Y^2Z and $X^3Y^2Z^3$.

We can verify also the existence of the following designs by computer:

- 3-$(128,8,2688)$ design (class (iii))
- 3-$(128,8,3456)$ design (classes (iv) and (v))

and we claim that the class (iv) alone do not define a 3-design.

Example 4.12 (3-designs with $q = 512$). We do not list the parameters of the five new designs anymore but remark that, again, by computer we get:

- 3-$(512, 8, 56448)$ design (class (iii))
- 3-$(512, 8, 72576)$ design (classes (iv) and (v))

Conjecture 4.13. *The class (iii) forms a* 3*-design.*

4.3 Proof of Theorem 4.5

First of all, we want to acknowledge that the following proof and its character sum methods imitate greatly the proof of Theorem 2.30 from [51]. As we will see in Section 4.5 Theorems 2.30 and 4.5 are geometrically linked and equivalent. Nevertheless, we present our proof below for self-containedness — it is also shorter and more uniform than the proof in [51].

To prove the main theorem we have to show that any three distinct coordinate positions are included in equally many supports of cwe-type X^6Z^2 and rank 1. By Theorem 2.20 we can assume that these positions are 0, 1, and an arbitrary element $a \in \mathbf{F}^{**}$. In this section all supports and codewords are assumed to be of cwe-type X^6Z^2 and rank 1 unless otherwise stated.

Lemma 4.4 shows that codewords (of this considered type) can be identified with their supports and we know that the support is a union of two 2-flats and both of them contain one 3-position. In other words, codeword is split into two 2-flats like: 1113 and 1113. This leads to a total of 22 combinations of positions 0, 1, and a among the two 2-flats and 1's and 3's as shown in Table 4.1. The number of codewords belonging to each combination with a fixed a is also shown.

We verify next the different frequencies and by summing them up we see that λ is equal to $14(q-8)/3$ and the supports, indeed, form a 3-design.

Assume that we have a codeword which is counted in the case (0b), that is, the corresponding support includes the positions 0, 1, and a. Using permutation $x \mapsto x/a$ and Theorem 2.20 we get a codeword which includes the positions 0, $1/a$ and 1. This permuted codeword is counted in the case (0b$'$) with a parameter $1/a \in \mathbf{F}^{**}$. Conversely, the codewords counted in (0b) are permuted versions of codewords in (0b$'$) and therefore we need to prove the frequency only for one of them.

With the same permutation we can link the cases (1a)–(3b) with (1$'$)–(3$'$). Another permutation $x \mapsto x+1$ links the case (0b$'$) with (0b$''$) and cases (1$'$)–(3$'$) with (1$''$)–(3$''$). We conclude that it suffices to prove only the cases (0a), (0b), and (1a)–(3b).

Table 4.1: All combinations of three coordinates

Case	1 1 1 3	1 1 1 3	Frequency
	x_1 x_2 x_3 x_4	y_1 y_2 y_3 y_4	
(0a)	0 1 a		$(q-8)/6$
(0b)	0 1 a		$(q-8)/6$
(0b′)	0 a 1		$(q-8)/6$
(0b″)	1 a 0		$(q-8)/6$
(1a)	0 1	a	$\frac{2(q-8)}{3}$
(1b)	0 1	a	
(2a)	0 1	a	$\frac{q-8}{2}$
(2b)	1 0	a	
(3a)	0 1	a	$\frac{q-8}{6}$
(3b)	1 0	a	
(1′)	0 a	1	$\frac{2(q-8)}{3}$
	0 a	1	
(2′)	0 a	1	$\frac{q-8}{2}$
	a 0	1	
(3′)	0 a	1	$\frac{q-8}{6}$
	a 0	1	
(1″)	1 a	0	$\frac{2(q-8)}{3}$
	1 a	0	
(2″)	1 a	0	$\frac{q-8}{2}$
	a 1	0	
(3″)	1 a	0	$\frac{q-8}{6}$
	a 1	0	

4.3.1 Syndrome equations

Next we consider the equations which the support $\{x_1,x_2,x_3,x_4,y_1,y_2,y_3,y_4\}$ from Table 4.1 should satisfy. The sets $\{x_1,x_2,x_3,x_4\}$ and $\{y_1,y_2,y_3,y_4\}$ form the two 2-flats and 3's are thought to be in the positions x_4 and y_4. By (2.2) and the 2-flat structure the following equations should hold:

$$\begin{aligned}
\sigma_1(x_1,x_2,x_3,x_4) &= 0\\
\sigma_1(y_1,y_2,y_3,y_4) &= 0\\
\sigma_2(x_1,x_2,x_3,x_4,y_1,y_2,y_3,y_4) &= x_4^2+y_4^2\\
S_3(x_1,x_2,x_3,x_4,y_1,y_2,y_3,y_4) &= 0
\end{aligned}$$

where σ_j and S_j are the jth elementary symmetric polynomial and the sum of jth powers, respectively, see Definition 1.11 and Example 1.12.

We abbreviate the regularly used terms $\sigma_j(x_1,x_2,x_3,x_4)$ and $\sigma_j(x_1,x_2,x_3)$ to $\sigma_j(x_i)$ and $\sigma'_j(x_i)$, respectively. Similar notations hold for S_3's and y_i's.

We simplify the third equation with the first two equations:

$$\sigma_2'(x_i)+\sigma_2'(y_i)=\sigma_1(x_i)\sigma_1(y_i)+\sigma_1'(x_i)x_4+x_4^2+\sigma_1'(y_i)y_4+y_4^2=0.$$

By Theorem 1.13 the identity $S_3=\sigma_1^3+\sigma_1\sigma_2+\sigma_3$ holds and the fourth equation becomes

$$\begin{aligned}S_3(x_i)+S_3(y_i)=&\sigma_1(x_i)^3+\sigma_1(x_i)\sigma_2(x_i)+\sigma_3(x_i)\\&+\sigma_1(y_i)^3+\sigma_1(y_i)\sigma_2(y_i)+\sigma_3(y_i)=\sigma_3(x_i)+\sigma_3(y_i)=0.\end{aligned}$$

All in all the considered support should satisfy

$$\begin{aligned}\sigma_1(x_i)&=\sigma_1(y_i)=0\\ \sigma_2'(x_i)&=\sigma_2'(y_i)\\ \sigma_3(x_i)&=\sigma_3(y_i).\end{aligned}\tag{4.1}$$

If the variables x_i and y_i are distinct, the corresponding codeword is of the desired type and rank. The items (i)–(iii) from Lemma 2.21 imply easily that the only possible overlapping of the variables x_i and y_i satisfying (4.1) is the case where the 2-flats are equal and $x_4=y_4$, that is, they form the support $\{0,1,a,a+1\}$ of cwe-type Y^4. So the solutions of (4.1) have one extra codeword which must be excluded.

4.3.2 Cases (0a) and (0b)

In the case (0a) we set $x_1=0$, $x_2=1$, and $x_3=a$. By (4.1) we have $x_4=a+1$ and therefore $\sigma_2'(x_i)=a$ and $\sigma_3(x_i)=a^2+a$. We have four unknown variables y_i which satisfy by (4.1)

$$\begin{aligned}\sigma_1'(y_i)&=y_4\\ \sigma_2'(y_i)&=a\\ \sigma_3(y_i)=\sigma_2'(y_i)y_4+\sigma_3'(y_i)&=a\sigma_1'(y_i)+\sigma_3'(y_i)=a^2+a.\end{aligned}$$

We think of $\sigma_1'(y_i)=\sigma$ as a free variable and the above equations show that y_1, y_2, and y_3 are zeros of the polynomial

$$p(T)=T^3+\sigma_1'(y_i)T^2+\sigma_2'(y_i)T+\sigma_3'(y_i)=T^3+\sigma T^2+aT+a\sigma+a^2+a.$$

Clearly, interchanging the roles of the variables y_1, y_2, and y_3 affects neither the above polynomial nor the corresponding codeword. Therefore the polynomials $p(T)$ that have three distinct zeros in $\mathbf{F}$ correspond to the codewords in the case (0a) or possibly to the extra codeword.

The polynomial $p(T)$ has always three distinct zeros in its splitting field as $p(T)$ and its derivative $p'(T)=T^2+a$ have no common zeros. The question is: for how many values of σ all zeros of $p(T)$ are in $\mathbf{F}$.

We substitute $T = U + \sigma$ and $p(T)$ transforms to $U^3 + (\sigma^2 + a)U + a^2 + a$. For $\sigma = \sqrt{a}$ this polynomial has only one zero in $\mathbf{F}$ and we can ignore that case. We substitute again with $U = (\sigma + \sqrt{a})V$ and divide by $(\sigma + \sqrt{a})^3$ and get

$$V^3 + V + \frac{a^2 + a}{(\sigma + \sqrt{a})^3}.$$

By Example 1.21 this polynomial has three zeros in $\mathbf{F}$ for $(q-2)/6$ values of σ since $a^2 + a \neq 0$ and $x \mapsto x^3$ is a bijection $\mathbf{F}^* \to \mathbf{F}^*$. Our substitutions preserve the number of zeros and hence $p(T)$ has three zeros in $\mathbf{F}$ for $(q-2)/6$ values of σ.

The codeword of cwe-type Y^4 would have $\{y_1, y_2, y_3\} = \{0, 1, a\}$, $\sigma = a + 1$, and $p(T) = T^3 + (a+1)T^2 + aT$. Excluding this extra codeword we have all in all $(q-8)/6$ codewords in the case (0a) as claimed in Table 4.1.

In the case (0b) we have $x_1 = 0$, $x_2 = 1$, $x_4 = a$, and $x_3 = a + 1$. The automorphism $x \mapsto x + 1$ links the case (0b) with (0a) and the frequencies are the same.

4.3.3 Cases (1a) and (1b)

We have $x_1 = 0$, $x_2 = 1$, and $y_1 = a$ in the case (1a). Now there are unknown variables in both 2-flats and the calculations are more complicated. We denote the variable x_3 by x and the elementary symmetric polynomials of y_2 and y_3 by $\sigma_1 = y_2 + y_3$ and $\sigma_2 = y_2 y_3$. The variables y_2 and y_3 are zeros of the polynomial $T^2 + \sigma_1 T + \sigma_2$ and by Lemma 1.4 the condition $\mathrm{Tr}\left(\sigma_2/\sigma_1^2\right) = 0$ must hold.

The extra codeword of cwe-type Y^4 has the support $\{0, 1, a, a+1\}$ and then $\sigma_1 \in \{1, a, a+1\}$. On the other hand if $\sigma_1 \in \{0, 1, a, a+1\}$ then the 2-flats would overlap or the support would have rank 3. As rank 3 contradicts (4.1), the only possible codeword is of cwe-type Y^4. To exclude this extra word we can restrict ourselves to the cases $\sigma_1 \in \mathbf{F}^a = \mathbf{F} \setminus \{0, 1, a, a+1\}$. We make this same restriction also in the forthcoming subsections.

By (4.1) we know that $x_4 = x + 1$, $y_4 = a + \sigma_1$, $x = a\sigma_1 + \sigma_2$ and

$$x^2 + x = a\sigma_2 + a\sigma_1(a + \sigma_1) + \sigma_2(a + \sigma_1) = \sigma_1\sigma_2 + a^2\sigma_1 + a\sigma_1^2. \tag{4.2}$$

We substitute the value of x from the third equation to (4.2) and get a quadratic equation in the unknown σ_2

$$\sigma_2^2 + (\sigma_1 + 1)\sigma_2 = \left(a^2 + a\right)\sigma_1(\sigma_1 + 1). \tag{4.3}$$

As σ_2 is an element of $\mathbf{F}$, again by Lemma 1.4, the condition

$$\mathrm{Tr}\left(\frac{\left(a^2 + a\right)\sigma_1}{\sigma_1 + 1}\right) = \mathrm{Tr}\left(\frac{\left(a^2 + a\right)\sigma_1}{\sigma_1 + 1} + a^2 + a\right) = \mathrm{Tr}\left(\frac{a^2 + a}{\sigma_1 + 1}\right) = 0 \tag{4.4}$$

must hold. We simplified the condition using the identity $\mathrm{Tr}(a^2) = \mathrm{Tr}(a)$.

By dividing (4.3) by σ_1^2 from both sides, the other trace condition takes the form

$$\mathrm{Tr}\left(\frac{\sigma_2}{\sigma_1^2}\right) = \mathrm{Tr}\left(\frac{\sigma_2^2}{\sigma_1^2} + \frac{\sigma_2}{\sigma_1}\right) + \mathrm{Tr}\left(a^2+a\right) + \mathrm{Tr}\left(\frac{a^2+a}{\sigma_1}\right) = \mathrm{Tr}\left(\frac{a^2+a}{\sigma_1}\right) = 0.$$

Therefore we should count the number

$$\begin{aligned} N_a &= \left|\left\{\sigma_1 \in \mathbf{F}^a \;\middle|\; \mathrm{Tr}\left(\tfrac{a^2+a}{\sigma_1}\right) = 0 \text{ and } \mathrm{Tr}\left(\tfrac{a^2+a}{\sigma_1+1}\right) = 0\right\}\right| \\ &= \frac{1}{4}\sum_{i,j=0}^{1} \sum_{\sigma_1 \in \mathbf{F}^a} (-1)^{i\cdot\mathrm{Tr}\left(\frac{a^2+a}{\sigma_1}\right) + j\cdot\mathrm{Tr}\left(\frac{a^2+a}{\sigma_1+1}\right)} \\ &= \frac{1}{4}(N_{0,0} + N_{0,1} + N_{1,0} + N_{1,1}) \end{aligned}$$

where $N_{i,j}$ is the inner sum in the second line.

The number of codewords in the case (1a) is twice the number N_a. This can be seen as follows: for every σ_1 which satisfies the trace conditions we have two solutions σ_2 and $\sigma_2 + \sigma_1 + 1$ for (4.3). The roles of y_2 and y_3 can be changed without affecting the codeword and hence σ_2 corresponds to one codeword. The other solution $\sigma_2 + \sigma_1 + 1$ gives a different codeword since $\sigma_1 \neq 1$. It also satisfies the trace condition $\mathrm{Tr}\left((\sigma_2 + \sigma_1 + 1)/\sigma_1^2\right) = \mathrm{Tr}\left(\sigma_2/\sigma_1^2\right) = 0$ by the identity $\mathrm{Tr}\left((a+1)/a^2\right) = 0$.

Clearly, $N_{0,0} = q - 4$. In the calculation of $N_{0,1}$ we use the substitution $z = (a^2+a)/(\sigma_1+1)$

$$\begin{aligned} N_{0,1} &= \sum_{\sigma_1 \in \mathbf{F}^a} (-1)^{\mathrm{Tr}\left(\frac{a^2+a}{\sigma_1+1}\right)} = \sum_{z \in \mathbf{F}\setminus\{a^2+a,0,a,a+1\}} (-1)^{\mathrm{Tr}(z)} \\ &= -(-1)^{\mathrm{Tr}(a^2+a)} - (-1)^{\mathrm{Tr}(0)} - (-1)^{\mathrm{Tr}(a)} - (-1)^{\mathrm{Tr}(a+1)} = -2. \end{aligned}$$

By using the substitution $z = (a^2+a)/\sigma_1$

$$N_{1,0} = \sum_{\sigma_1 \in \mathbf{F}^a} (-1)^{\mathrm{Tr}\left(\frac{a^2+a}{\sigma_1}\right)} = \sum_{z \in \mathbf{F}\setminus\{0,a^2+a,a+1,a\}} (-1)^{\mathrm{Tr}(z)} = -2.$$

By the substitution $z = 1/\sigma_1$ we get

$$N_{1,1} = \sum_{\sigma_1 \in \mathbf{F}^a} (-1)^{\mathrm{Tr}\left(\frac{a^2+a}{\sigma_1} + \frac{a^2+a}{\sigma_1+1}\right)} = \sum_{z \in \mathbf{F}\setminus\left\{0,1,\frac{1}{a},\frac{1}{a+1}\right\}} (-1)^{\mathrm{Tr}\left((a^2+a)z + \frac{(a^2+a)z}{z+1}\right)}.$$

As in (4.4) we drop z from the last numerator and substitute $u = z+1$ and $w = (a^2+a)u$.

$$N_{1,1} = \sum_{u \in \mathbf{F} \setminus \left\{1, 0, \frac{a+1}{a}, \frac{a}{a+1}\right\}} (-1)^{\mathrm{Tr}\left(\left(a^2+a\right)u + a^2 + a + \frac{a^2+a}{u}\right)}$$

$$= \sum_{w \in \mathbf{F} \setminus \{a^2+a, 0, a^2+1, a^2\}} (-1)^{\mathrm{Tr}\left(w + \frac{\left(a^2+a\right)^2}{w}\right)} = K\left(a^2+a\right) + 1$$

where $K\left(a^2+a\right)$ is the Kloosterman sum, see Definition 1.6 and the remark below it.By combining the above results we have

$$N_a = \frac{1}{4}\left(q - 7 + K\left(a^2+a\right)\right).$$

The case (1b) goes almost as above. Now $y_4 = a$, $y_1 = a+\sigma_1$, $x = \sigma_1^2 + a\sigma_1 + \sigma_2$, the equation (4.2) still holds, but instead of (4.3) we get

$$\sigma_2^2 + (\sigma_1+1)\sigma_2 = \left(a^2+a\right)\sigma_1(\sigma_1+1) + \sigma_1^2(\sigma_1+1)^2.$$

Therefore the task is to calculate the number

$$N'_a = \left|\left\{\sigma_1 \in \mathbf{F}^a \;\middle|\; \mathrm{Tr}\left(\tfrac{a^2+a}{\sigma_1} + \sigma_1 + 1\right) = 0 \text{ and } \mathrm{Tr}\left(\tfrac{a^2+a}{\sigma_1+1} + \sigma_1\right) = 0\right\}\right|$$

For every σ_1 counted in N'_a we get two codewords as in the case (1a) but this time every codeword is counted three times in the number $2N'_a$. This follows from the observation that among the three coordinates y_1, y_2, and y_3 we can choose two coordinates with three ways. The two chosen are identified with σ_1 and σ_2 and the third one is equal to $\sigma_1 + a$. Therefore the number of codewords in the case (1b) is equal to $2N'_a/3$.

As above we know that $N'_{0,0} = q-4$. With the substitution $z = \sigma_1 + 1$ we have

$$N'_{0,1} = \sum_{\sigma_1 \in \mathbf{F}^a} (-1)^{\mathrm{Tr}\left(\frac{a^2+a}{\sigma_1+1} + \sigma_1\right)} = \sum_{z \in \mathbf{F}^a} (-1)^{\mathrm{Tr}\left(\frac{a^2+a}{z} + z + 1\right)} = -K\left(a^2+a\right) - 3$$

$$N'_{1,0} = \sum_{\sigma_1 \in \mathbf{F}^a} (-1)^{\mathrm{Tr}\left(\frac{a^2+a}{\sigma_1} + \sigma_1 + 1\right)} = -K\left(a^2+a\right) - 3$$

$$N'_{1,1} = \sum_{\sigma_1 \in \mathbf{F}^a} (-1)^{\mathrm{Tr}\left(\frac{a^2+a}{\sigma_1} + \frac{a^2+a}{\sigma_1+1} + 1\right)} = -N_{1,1} = -K\left(a^2+a\right) - 1.$$

Then $N'_a = \left(q - 11 - 3K\left(a^2+a\right)\right)/4$ and the total number of codewords in the cases (1a) and (1b) together is equal to the number in Table 4.1:

$$2N_a + \frac{2}{3}N'_a = \frac{q - 7 + K\left(a^2+a\right)}{2} + \frac{q - 11 - 3K\left(a^2+a\right)}{6} = \frac{2(q-8)}{3}.$$

4.3.4 Cases (2a) and (2b)

The situation in the case (2a) is: $x_1 = 0$, $x_4 = 1$, and $y_1 = a$. As above we denote $x = x_3$, $\sigma_1 = y_2 + y_3$, and $\sigma_2 = y_2 y_3$. We have by (4.1) that $x_2 = x+1$, $y_4 = a+\sigma_1$, and (4.2) holds, but this time the equation for σ_2' gives

$$x^2 + x = a\sigma_1 + \sigma_2.$$

By combining this with (4.2) we get $\sigma_2 = \sigma_1\left(a\sigma_1 + a^2 + a\right)/(\sigma_1 + 1)$. As we are interested in roots x which are in $\mathbf{F}$ the variable σ_1 should satisfy

$$\mathrm{Tr}\left(a\sigma_1 + \frac{\sigma_1\left(a\sigma_1 + a^2 + a\right)}{\sigma_1 + 1}\right) = \mathrm{Tr}\left(\frac{a^2\sigma_1}{\sigma_1 + 1}\right) = \mathrm{Tr}\left(\frac{a^2}{\sigma_1 + 1} + a^2\right) = 0 \quad (4.5)$$

by Lemma 1.4. On the other hand σ_1 should also satisfy

$$\begin{aligned}\mathrm{Tr}\left(\frac{\sigma_2}{\sigma_1^2}\right) &= \mathrm{Tr}\left(\frac{a\sigma_1 + a^2 + a}{\sigma_1(\sigma_1+1)}\right) + \mathrm{Tr}\left(\frac{a^2\sigma_1}{\sigma_1+1}\right) \\ &= \mathrm{Tr}\left(\frac{\left(a^2+a\right)(\sigma_1+1)}{\sigma_1(\sigma_1+1)} + \frac{a^2\sigma_1(\sigma_1+1)}{\sigma_1(\sigma_1+1)}\right) \\ &= \mathrm{Tr}\left(\frac{a^2+a}{\sigma_1} + a^2\right) = 0.\end{aligned} \quad (4.6)$$

In the first line we added a term which is equal to zero by (4.5).

This time we are interested in the number

$$M_a = \left|\left\{\sigma_1 \in \mathbf{F}^a \;\middle|\; \mathrm{Tr}\left(\tfrac{a^2+a}{\sigma_1} + a\right) = 0 \text{ and } \mathrm{Tr}\left(\tfrac{a^2}{\sigma_1+1} + a\right) = 0\right\}\right|$$

which is the number of codewords in the case (2a): for every σ_1 satisfying the trace conditions there is one σ_2 and with them we get solutions x and $x+1$ for the equation (4.2), but they correspond to the same codeword.

We count the number M_a as above. Clearly $M_{0,0} = q-4$ and

$$\begin{aligned}M_{0,1} &= \sum_{\sigma_1 \in \mathbf{F}^a} (-1)^{\mathrm{Tr}\left(\frac{a^2}{\sigma_1+1}+a\right)} = \sum_{z \in \mathbf{F}\setminus\left\{a^2+a, a, \frac{a}{a+1}, 0\right\}} (-1)^{\mathrm{Tr}(z)} \\ &= -2 - (-1)^{\mathrm{Tr}(a)} - (-1)^{\mathrm{Tr}\left(\frac{a}{a+1}\right)} \\ M_{1,0} &= \sum_{\sigma_1 \in \mathbf{F}^a} (-1)^{\mathrm{Tr}\left(\frac{a^2+a}{\sigma_1}+a\right)} = (-1)^{\mathrm{Tr}(a)} N_{1,0} = -2(-1)^{\mathrm{Tr}(a)}.\end{aligned}$$

We use the substitutions $z = 1/\sigma_1$, $u = z+1$, and $w = \left(a^2+a\right)u$ and then

$$\begin{aligned} M_{1,1} &= \sum_{\sigma_1 \in \mathbf{F}^a} (-1)^{\mathrm{Tr}\left(\frac{a^2+a}{\sigma_1}+\frac{a^2}{\sigma_1+1}\right)} = \sum_{z \in \mathbf{F}\setminus\left\{0,1,\frac{1}{a},\frac{1}{a+1}\right\}} (-1)^{\mathrm{Tr}\left(\left(a^2+a\right)z+\frac{a^2}{z+1}+a^2\right)} \\ &= \sum_{u \in \mathbf{F}\setminus\left\{0,1,\frac{a+1}{a},\frac{a}{a+1}\right\}} (-1)^{\mathrm{Tr}\left(\left(a^2+a\right)u+\frac{a^2}{u}+a\right)} \\ &= \sum_{w \in \mathbf{F}\setminus\{0,a^2+a,a^2+1,a^2\}} (-1)^{\mathrm{Tr}\left(w+\frac{a^3(a+1)}{w}+a\right)} \\ &= (-1)^{\mathrm{Tr}(a)} K\left(a^3(a+1)\right) - 2 - (-1)^{\mathrm{Tr}\left(\frac{1}{a+1}\right)}. \end{aligned}$$

We conclude that

$$M_a = \frac{1}{4}\left(q-8-3(-1)^{\mathrm{Tr}(a)} + (-1)^{\mathrm{Tr}(a)} K\left(a^3(a+1)\right)\right).$$

The case (2b) is linked with the case (2a) by the automorphism $x \mapsto x+1$. Therefore the total number of codewords in the cases (2a) and (2b) is equal to

$$M_a + M_{a+1} = \frac{2q-16+(-1)^{\mathrm{Tr}(a)}\left(K\left(a^3(a+1)\right) - K\left((a+1)^3 a\right)\right)}{4} = \frac{q-8}{2}$$

by Theorem 1.7. This is exactly the frequency given in Table 4.1.

4.3.5 Cases (3a) and (3b)

We have the following dependencies in the case (3a): $x_1 = 0$, $x_4 = 1$, and $y_4 = a$. As before we denote $x = x_3$, $\sigma_1 = y_2 + y_3$, and $\sigma_2 = y_2 y_3$. By (4.1) we know that $x_2 = x+1$, $y_1 = a+\sigma_1$, (4.2) holds, and $x^2+x = \sigma_1^2 + a\sigma_1 + \sigma_2$. As in the previous cases we can solve $\sigma_2 = (a+1)\sigma_1(\sigma_1+a)/(\sigma_1+1)$ and the trace conditions get forms

$$\mathrm{Tr}\left(\frac{\sigma_2}{\sigma_1^2}\right) = \mathrm{Tr}\left(\frac{(a+1)(\sigma_1+a)}{\sigma_1(\sigma_1+1)}\right) = 0$$

and

$$\begin{aligned} \mathrm{Tr}\left(\sigma_1^2 + a\sigma_1 + \sigma_2\right) &= \mathrm{Tr}\left(\sigma_1^2 + a\sigma_1 + \frac{(a+1)\sigma_1(\sigma_1+a)}{\sigma_1+1}\right) = \mathrm{Tr}\left(\frac{\sigma_1^3+a^2\sigma_1}{\sigma_1+1}\right) \\ &= \mathrm{Tr}\left(\frac{\sigma_1^3+a^2\sigma_1}{\sigma_1+1} + \sigma_1^2 + \sigma_1\right) = \mathrm{Tr}\left(\frac{(a+1)^2\sigma_1}{\sigma_1+1}\right) = 0. \end{aligned}$$

We claim that the number of solutions to these two mutual trace equations is equal to M_{a+1}: the substitution $a \mapsto a+1$ transforms the middle term in (4.6) to

the former equation and the middle expression in (4.5) to the latter equation. Like in the case (1b) every codeword is calculated three times and hence the number of codewords in the case (3a) is equal to $M_{a+1}/3$.

The cases (3a) and (3b) are connected via the automorphism $x \mapsto x+1$ and thus the number of codewords in the case (3b) is equal to $M_a/3$. The total number of codewords in the cases (3a) and (3b) is then

$$\frac{M_{a+1}+M_a}{3} = \frac{q-8}{6}$$

as claimed in Table 4.1. This concludes our proof for the main theorem.

4.4 Proof of Corollary 4.6

We prove that the number of supports of swe-type X^8 that include three fixed coordinates does not depend on the coordinates.

Let us consider some consequences of Definition 2.11 and Corollary 2.32. If $\mathbf{c} \in \mathscr{G}_1$ is some codeword with three fixed coordinates, we can choose the corresponding positions of $\phi(\mathbf{c})$ either from $\mathbf{c}_L$ or $\mathbf{c}_R$. These eight left/right-combinations of "binary" positions give us sets of codewords which we can count.

Take for example all three positions from the left side. The codewords of $\phi(\mathscr{G}_1)$ that include these "binary" positions are images of $\mathbf{Z}_4$-codewords that have either 1 or 2 in the three coordinates. If some position is chosen from the right side then the corresponding $\mathbf{Z}_4$-codeword should have either 2 or 3 in this coordinate. We illustrate half of the combinations in Table 4.2. The remaining four combinations are obtained by multiplying the whole table by -1.

By Corollary 2.32 there are $\lambda_b = (2q-4)(4q-17)/60$ supports $\phi(\mathbf{c})$ of size 8 in $\phi(\mathscr{G}_1)$ containing three "binary" positions. In Table 4.2 we list all possible cwe-types of the corresponding $\mathbf{Z}_4$-codewords $\mathbf{c}$ of Lee weight 8. The frequency column gives the number of codewords in *one* column.

In the case (a) the frequencies come from (i) in Example 2.26 and in the cases (b) and (c) from Table 4.3 or [51]. We conclude that the codewords in the case (d) in all left/right-combinations, that is, the codewords of swe-type X^8, form a 3-design with repeated blocks and

$$\lambda' = 8? = 8\left(\frac{(2q-4)(4q-17)}{60} - \frac{5(q-8)}{3} - 1\right) = \frac{4(4q^2-75q+404)}{15}. \quad (4.7)$$

We make this design simple using Lemma 4.4, Example 2.28, and Theorem 4.5. For every codeword $\mathbf{c}$ of swe-type X^8 there is a codeword $-\mathbf{c}$ with the same support and it can be excluded. This settles the supports of rank 0. For the supports of rank 3 and 1 there are still 7 and 1 extra codewords, respectively, and therefore the simple design has

$$\lambda = \frac{\lambda'}{2} - 7\lambda_{2.28} - \lambda_{4.5} = \frac{32q^2-985q+5892}{60}.$$

Table 4.2: Half of the eight left/right-combinations

Case	LLL	LLR	LRL	RLL	Frequency
(a)	222 2	222 2	222 2	222 2	1
(b)	111 1112 111 1332	113 1132 113 3332	131 1132 131 3332	311 1132 311 3332	$\frac{2(q-8)}{3}$
(c)	211 1111 211 1133 211 3333	213 1113 213 1333	231 1113 231 1333	211 1111 211 1133 211 3333	$\frac{q-8}{3}$
(c)	121 1111 121 1133 121 3333	123 1113 123 1333	121 1111 121 1133 121 3333	321 1113 321 1333	$\frac{q-8}{3}$
(c)	112 1111 112 1133 112 3333	112 1111 112 1133 112 3333	132 1113 132 1333	312 1113 312 1333	$\frac{q-8}{3}$
(d)	111 11111 111 11133 111 13333	113 11113 113 11333 113 33333	131 11113 131 11333 131 33333	311 11113 311 11333 311 33333	?
Total	λ_b	λ_b	λ_b	λ_b	λ_b

4.5 Link between 3-designs with block sizes 7 and 8

There is a considerable similarity between the proofs of Theorems 2.30 and 4.5: the calculations involve similar exponential sums and Kloosterman sum identities, and also λ's are equal. This suggests that there might be a relation between the blocks of these designs. Indeed, a strong structural connection is illustrated in Table 4.3 and explained below. This link makes Theorems 2.30 and 4.5 equivalent and §4.3 gives us a simpler and more uniform proof for Theorem 2.30 as the original one [51].

We assume that we have three fixed coordinates and consider blocks containing them. The corresponding $\mathbf{Z}_4$-symbols in these positions are shown in the Fix-column. Every block of size 8 is viewed as a codeword of cwe-type X^6Z^2 and rank 1 but the blocks of size 7 are viewed as codewords of cwe-types X^6Y, X^4YZ^2, and X^2YZ^4 depending on the situation. The case notations refer to Table 4.1.

The correspondence between the two designs associates a block of size 7 *with a block of size* 8 *if and only if the difference of the corresponding codewords is in the class (i), i.e., the support of the difference is a* 3*-flat.*

We recall a few facts from the affine geometry, see Subsection 1.1.2: Every set of three points defines a unique 2-flat. Furthermore, any 2-flat and a fifth point determine a unique 3-flat. By (iii) in Lemma 2.21 a support of size 7 does not contain a 2-flat and thus any four points within a block of size 7 can be uniquely completed to a 3-flat. The intersection of two 3-flats can have only 0, 1, 2, 4, or 8 points.

Table 4.3: Structural dependence of blocks in Theorems 2.30 and 4.5

Case	Theorem 2.30 → Theorem 4.5				Theorem 4.5 → Theorem 2.30			
	Fix		Comb	Freq	Fix		Comb	Freq
(0a)	111 111	1112 3331311 33111		$\frac{2(q-8)}{3}$	111 111	31113 13333111 2111		$\frac{q-8}{6}$
	111 111	1332 31133113 13113			111 111	31113 13311133 2 133	3	
(1a)	112 3 111	1133 331 1311 31311	2	$\frac{q-8}{3}$	111 1 112	13113 3 331311 3 311		$\frac{2(q-8)}{3}$
	112 3 111	1133 3113311 1 3311	2		111 1 112	13113 1331133 1 133		
(1b)	112 1 113	1111 333 3111 13111	4		113 3 112	13111 1333111 1 111		
	112 1 113	3333 111 1111 31111	4		113 3 112	13111 3 333333 3 333		
(2a)	132 3 131	1113 3311311 1 1311	3	$\frac{q-8}{3}$	131 1 132	11113 3 331311 1 311	2	$\frac{q-8}{2}$
(2b)	312 3 311	1113 3311311 1 1311	3		311 1 312	11113 3 331311 1 311	2	
(3a)	132 1 133	3331 111 1111 11111			133 3 132	11111 3 333333 1 333	2	$\frac{q-8}{6}$
(3b)	312 1 313	3331 111 1111 11111			313 3 312	11111 3 333333 1 333	2	

In Table 4.3 we describe all combinations that need to be considered. All other cases come with the automorphisms as in Section 4.3. Every combination has three rows: original codeword in the first row, the linking codeword with a 3-flat support in the second row, and their sum in the third row. By suitable positioning of 1's and 3's within a 3-flat we get the required connections. However, this is not a 1–1 correspondence as we can sometimes associate a block of one design with several blocks of the other design. This number is indicated in the Comb-column.

For example, in the first case in (1a) we can choose the position with 1 in the 3-flat from the two positions with 3's in the original codeword. One 2-flat within the 3-flat is indicated by underlining its coordinates. As the 3-flat and the sum intersect in 5 points the sum has rank 1 and one of the 2-flats is underlined.

The frequencies in the right side can be taken from Table 4.1 and then the frequencies in the left side can be counted from the relations in the table. For example, in the case (0a) we can construct one block of size 8 from one block of size 7. On the other hand, from one block of size 8 we can construct four blocks of size 7. Hence in this case there must be four times as many blocks in Theorem 2.30 as in Theorem 4.5.

Chapter 5

New 3-designs from codes $\mathscr{G}_2$, $\mathscr{G}_4$, $\mathscr{G}_8$, and $\mathscr{G}_{16}$

In this chapter we generalize all the results from Chapter 4 for codes $\mathscr{G}_k$ with $k \in \{2,4,8,16\}$. The parameters of the 3-designs are the same for every k.

5.1 Main results

The results are presented compactly with the class notation from Section 4.1.

Theorem 5.1. *The class (ii) forms a* 3-$\left(q, 8, \frac{14}{3}(q-8)\right)$ *design for* $k \in \{2,4,8,16\}$.

The proof of this main theorem is postponed to the next section.

Corollary 5.2. *The supports of size* 7*, the class (C), and the class (B) define* 3*-designs when* $k \in \{2,4,8,16\}$.

Proof. The link in Section 4.5 does not depend on k and therefore Theorem 2.30 holds for those values of k for which Theorem 5.1 holds. Also the arguments in the proofs of Corollaries 4.6 and 4.7 are valid for every k. □

Corollary 5.3. *The class (D) and the supports of size* 8 *form* 3*-designs when* $k \in \{2,4,8,16\}$.

Proof. The proofs of Corollaries 4.8 and 4.9 need the knowledge of $\mathrm{cwe}(\mathscr{G}_1)$ or, actually, the number of codewords of hwe-type X^8. We could not find any results about $\mathrm{cwe}(\mathscr{G}_k)$ in the literature but we suspect that it is exactly the same as $\mathrm{cwe}(\mathscr{G}_1)$. Fortunately, we can count below that the number of supports in the class (D) is the same for all k. As the number of other supports of hwe-type X^8 is already known to be the same for the considered values of k, the claim follows.

We know by (iv) and (v) in Lemma 2.21 that the codewords of swe-type X^6Y^2 are of cwe-type X^5Y^2Z, $X^3Y^2Z^3$, and XY^2Z^5, and that there are always two

codewords for one support. Therefore we count only the codewords of cwe-type X^5Y^2Z and half of the codewords of cwe-type $X^3Y^2Z^3$.

Let $\mathbf{c} \in \mathscr{B}_k$ be a codeword with weight 6. If we view $\mathbf{c}$ as a word of cwe-type X^6 in $\mathbf{Z}_4^q$, we see that it satisfies the two equations on the right in (2.2). We can add an odd number, say s, of 2's in arbitrary positions y_i without affecting the validity of these equations, so that the first equation will also hold. When the equation

$$\sigma_2(\chi(\mathbf{c})) = \sum_{i=1}^{s} y_i^2$$

is satisfied we have a codeword in $\mathscr{G}_k$.

Let us count the number of supports of cwe-type X^5Y^2Z, which means that $s = 3$. We can choose a 3-position y_1 in 6 ways from $S = \chi(\mathbf{c})$. Let y_2 get all $q-6$ values outside the support S and this determines the third position y_3 uniquely. If y_3 is in S, we have a codeword of cwe-type X^6Y or X^4YZ^2. Excluding these 6 choices we have $q-6-6$ codewords of cwe-type X^5Y^2Z. Every codeword was counted twice as the roles of the variables y_2 and y_3 can be changed. With the choices of y_1 there are $6(q-12)/2 = 3(q-12)$ codewords $\mathbf{d}$ of cwe-type X^5Y^2Z such that $\mu(\mathbf{d}) = \mathbf{c}$.

The above considerations go similarly with supports of cwe-type $X^3Y^2Z^3$. Now $s = 5$ and we choose 3 positions from S with $\binom{6}{3} = 20$ ways but every two choices correspond to the same support. Hence we consider only 10 different choices. Now y_1, y_2, and y_3 are fixed within S and we let y_4 go through $\mathbf{F} \setminus S$. This determines y_5 and if it is in S we get codewords of cwe-types X^4YZ^2 and X^2YZ^4. Again, the roles of y_4 and y_5 are interchangeable and we have $10(q-12)/2 = 5(q-12)$ different supports.

We can lift $\mathbf{c}$ to a support of swe-type X^6Y^2 with $8(q-12)$ different ways. By Theorem 2.23 and (i) in Example 2.27 there are for every k

$$8(q-12)\frac{q-8}{6}\binom{q}{3}\Big/\binom{6}{3} = \frac{56}{15}(q-8)(q-12)\binom{q}{3}\Big/\binom{8}{3}$$

supports in the class (D) and this corresponds to λ in Corollary 4.8. □

The Lee weight distributions of the codes $\mathscr{G}_k$ are equal [22] and also the coset Lee weight distributions of these codes are the same [27]. In Chapter 3 we introduced a unified decoding algorithm for all these codes. It would be surprising if they would not yield designs with the same parameters.

Conjecture 5.4. *All the results in Chapter 4 hold for every k.*

5.2 Proof of Theorem 5.1

We have the same situation as in Section 4.3 except $k \neq 1$. The case notation refers to Table 4.1.

5.2.1 Syndrome equations

We simplify the equations (2.2) as in Subsection 4.3.1. Assume we have a codeword in the class (ii) with a support $\{x_1,x_2,x_3,x_4,y_1,y_2,y_3,y_4\}$ such that x_i's and y_i's form the two 2-flats, respectively. Assume further that the codeword is of cwe-type X^6Z^2 and the two 3-symbols are in the positions x_4 and y_4. The support should then satisfy

$$\begin{aligned} \sigma_1(x_i) &= \sigma_1(y_i) = 0 \\ \sigma_2'(x_i) &= \sigma_2'(y_i) \\ S_{2^k+1}(x_i) &= S_{2^k+1}(y_i). \end{aligned} \tag{5.1}$$

For the definition of σ_2' see Subsection 4.3.1.

We could use Theorem 1.13 to represent the last equation with σ's. When k is 2 and 3 this equation becomes $\sigma_2(x_i)\sigma_3(x_i) = \sigma_2(y_i)\sigma_3(y_i)$ and $\sigma_2(x_i)^3\sigma_3(x_i) + \sigma_3(x_i)^3 = \sigma_2(y_i)^3\sigma_3(y_i) + \sigma_3(y_i)^3$, respectively. This suggests that it may be simpler to keep the last equation in the power sum form.

5.2.2 Cases (0a) and (0b)

By (i) in Example 2.27 there are $(q-8)/6$ codewords of Hamming weight 6 in $\mathscr{B}_k$ that contain the three fixed coordinates. These codewords can be uniquely lifted to codewords in $\mathscr{G}_k$ of cwe-type X^6Y: the codeword of $\mathscr{B}_k$ satisfies two of the four equations in (2.2) and suitably positioning a single 2 makes the remaining two equations hold, too. This 2-symbol can not be within the original support of size 6 as $d_L(\mathscr{G}_k) = 8$.

As in the case (0a) in Table 4.3 we choose two 3-positions in three different ways outside the three fixed positions and lift the corresponding word uniquely to $\mathscr{G}_k$ as above. We have all in all $(q-8)/6 + 3(q-8)/6 = 2(q-8)/3$ codewords of swe-type X^6Y in the case (0a) in Table 4.3 and therefore $(q-8)/6$ codewords in class (ii). The value in Table 4.1 is valid for all k and the case (0b) comes with automorphisms as in Subsection 4.3.2.

Actually, we could replace Subsection 4.3.2 with the link in Section 4.5 and the above argument.

5.2.3 Cases (1a) and (1b)

Next we study the case (1a). We have the same situation as in the subsection 4.3.3: $x_1 = 0, x_2 = 1, x_3 = x, x_4 = x+1, y_1 = a$. We simplify notations by setting $y_2 = y$, $y_3 = z$, and $y_4 = a+y+z$.

The syndrome equations (5.1) imply that $x = a(y+z) + yz$ and

$$1 + x^{2^k+1} + (x+1)^{2^k+1} = a^{2^k+1} + y^{2^k+1} + z^{2^k+1} + (a+y+z)^{2^k+1}.$$

Substituting the first equation to the second we get

$$W(U+V) = UV$$

where $W = a + a^{2^k}$, $U = y + y^{2^k}$, and $V = z + z^{2^k}$ for any k.

By Lemma 1.5 the mapping $u \mapsto u + u^{2^k}$ is two-to-one and its image is $T_0 = \{u \in \mathbf{F} \mid \mathrm{Tr}(u) = 0\}$. Now we have for all k the following equation

$$W(U+V) = UV \qquad W,U,V \in T_0. \tag{5.2}$$

In Subsection 4.3.3 we noticed that the number of solutions does not depend on a when $k = 1$. Therefore the number of solutions of (5.2) does not depend on W and this holds now for all k. One value of $W = a + a^{2^k}$ corresponds to a and $a+1$ simultaneously but this is not a problem since there are equally many codewords for the values a and $a+1$ as can be seen via the automorphism $x \mapsto x+1$. Hence the number of solutions of (5.2) does not depend on a.

In the case (1b) we have $x_1 = 0$, $x_2 = 1$, $x_3 = x$, $x_4 = x+1$, $y_1 = y$, $y_2 = z$, $y_3 = a + y + z$, and $y_4 = a$. By (5.1) we derive $x = a(y+z) + yz + (y+z)^2$ and

$$W(U+V) = UV + (U+V)^2 \qquad W,U,V \in T_0.$$

With the same argument as above the number of solutions depends neither on k nor on a. Considering U and V as roots of a quadratic equation $T^2 + (U+V)T = UV$ we see also that the value of

$$\mathrm{Tr}\left(\frac{W}{U+V}\right)$$

determines whether the solution (U,V) belongs to the case (1a) or (1b).

5.2.4 Cases (2a) and (2b)

Let us consider the situation as in Subsection 4.3.4: in the case (2a) we have $x_1 = 0$ and $x_4 = 1$, and in the case (2b) $x_1 = 1$ and $x_4 = 0$, and in both cases $y_1 = a$. We denote $x = x_3$, $\sigma_1 = y_2 + y_3$, and $\sigma_2 = y_2 y_3$. One of the equations

$$\begin{aligned} x + x^2 &= a\sigma_1 + \sigma_2 \qquad \text{(2a)} \\ 1 + x + x^2 &= a\sigma_1 + \sigma_2 \qquad \text{(2b)} \end{aligned} \tag{5.3}$$

holds and now the third equation in (5.1) transforms to

$$x + x^{2^k} = a^{2^k+1} + y^{2^k+1} + z^{2^k+1} + (a+\sigma_1)^{2^k+1}. \tag{5.4}$$

Suppose now that k is even. With a telescopic identity

$$x + x^{2^k} = \sum_{i=0}^{k-1} \left(x + x^2\right)^{2^i} = \sum_{i=0}^{k-1} \left(1 + x + x^2\right)^{2^i}$$

we can consider the cases (2a) and (2b) simultaneously and writing (5.4) down with a Dickson polynomial, see Subsection 1.1.3, we derive

$$\sum_{i=0}^{k-1}(a\sigma_1+\sigma_2)^{2^i} = a^{2^k+1} + D_{2^k+1}(\sigma_1,\sigma_2) + (a+\sigma_1)^{2^k+1}.$$

We substitute $\sigma_2 = T + a\sigma_1 + a^2$ and get

$$\sum_{i=0}^{k-1}\left(T+a^2\right)^{2^i} = a^{2^k+1} + D_{2^k+1}\left(\sigma_1, T+a\sigma_1+a^2\right) + (a+\sigma_1)^{2^k+1}. \tag{5.5}$$

By Lemma 1.15 and the identity $a^{2^k+1} + (a+\sigma_1)^{2^k+1} = D_{2^k+1}\left(\sigma_1, a\sigma_1+a^2\right)$ we have

$$\sum_{i=0}^{k-1}\left(T+a^2\right)^{2^i} = D_{2^k+1}(\sigma_1,T) + \sigma_1^{2^k+1}.$$

By regrouping the terms we arrive at the equation

$$P_k(T) := \sum_{i=0}^{k-1}\left(\sigma_1^{2^k+1-2^{i+1}}+1\right)T^{2^i} = \sum_{i=1}^{k} a^{2^i}. \tag{5.6}$$

We try to count the solutions T, and hence σ_2, of the above equation for each $\sigma_1 \in \mathbf{F}^a = \mathbf{F}\setminus\{0,1,a,a+1\}$. This restriction assures that the extra codeword of cwe-type Y^4 is not included to the solutions, as in Subsection 4.3.3.

The polynomial $P_k(T)$ is linearized, see Definition 1.9 and [37, Section 3.4]. Below we seek to give a decomposition of this linearized polynomial into linearized factors of degree 2 and to that end we introduce the following two auxiliary families of polynomials and their properties.

Definition 5.5. $r_i(s) = \sum_{j=0}^{2^i} s^j$ and $w_n(s) = \sum_{i=1}^{n}\binom{n}{i} r_i(s)^{2^{n-i}}$.

Lemma 5.6. *The polynomials $w_n(s)$ have the following properties:*

(i) $w_{n+1}(s) = w_n(s)^2 + \left(s^{2^n}+1\right)w_n(s) + s^{2^{n+1}} + 1$ *with* $w_1(s) = s^2+s+1$;

(ii) $w_n(s) \neq 0$ *for every* $s \in \mathbf{F}$;

(iii) $\mathrm{Tr}\left(w_{n+1}(s)/w_n(s)^2\right) = 1$;

(iv) $w_{2^l-1}(s)^2 \cdot (s+1) = D_{2^{2^l}+1}(s+1,1)$ *is a permutation polynomial.*

Proof. The fact (i) can be seen as follows:

$$\begin{aligned}
w_{n+1}(s) &= \sum_{i=1}^{n+1} \left(\binom{n}{i-1} + \binom{n}{i} \right) r_i(s)^{2^{n+1-i}} \\
&= \sum_{i=0}^{n} \binom{n}{i} r_{i+1}(s)^{2^{n-i}} + \sum_{i=1}^{n} \binom{n}{i} r_i(s)^{2^{n+1-i}} \\
&= \left(s^2+s+1\right)^{2^n} + \sum_{i=1}^{n} \binom{n}{i} (r_i(s) + \sigma_1^{2^i}(r_i(s)+1))^{2^{n-i}} + w_n(s)^2 \\
&= \sigma_1^{2^{n+1}} + s^{2^n} + 1 + w_n(s)\left(s^{2^n}+1\right) + s^{2^n} \sum_{i=1}^{n} \binom{n}{i} + w_n(s)^2 \\
&= s^{2^{n+1}} + 1 + w_n(s)\left(s^{2^n}+1\right) + w_n(s)^2.
\end{aligned}$$

For the fact (ii) suppose that $w_n(s) = 0$ for some $s \in \mathbf{F}$. If $s = 1$, we see by (i) inductively that $w_n(1) = w_{n-1}(1) = \cdots = w_1(1) = 0$ contradicting $w_1(1) = 1$. If $s \neq 1$, we have a root $W = w_{n-1}(s) \in \mathbf{F}$ of the quadratic equation

$$W^2 + \left(s^{2^{n-1}}+1\right) W + s^{2^n} + 1 = 0$$

by the recursion formula (i). Lemma 1.4 then implies a contradiction (recall that m is odd)

$$\mathrm{Tr}\left(\frac{s^{2^n}+1}{\left(s^{2^{n-1}}+1\right)^2} \right) = \mathrm{Tr}(1) = 0.$$

The same argument applies also for the first polynomial $w_1(s) = s^2 + s + 1$.

Now the fact (iii) is an easy consequence of (i) and (ii)

$$\mathrm{Tr}\left(\frac{w_{n+1}(s)}{w_n(s)^2} \right) = \mathrm{Tr}\left(1 + \frac{s^{2^n}+1}{w_n(s)} + \left(\frac{s^{2^n}+1}{w_n(s)} \right)^2 \right) = 1.$$

For the fact (iv) we derive by (1.2)

$$\begin{aligned}
\frac{D_{2^{2^l}+1}(s+1,1)}{s+1} &= (s+1)^{2^{2^l}} + \sum_{i=1}^{2^l} (s+1)^{2^{2^l}-2^i} \\
&= s^{2^{2^l}} + \sum_{i=1}^{2^l-1} \left((s+1)^{2^{2^l-i}-1} \right)^{2^i} \\
&= s^{2^{2^l}} + \sum_{i=1}^{2^l-1} \left(r_{2^l-i}(s) + s^{2^{2^l-i}} \right)^{2^i} \\
&= \sum_{j=1}^{2^l-1} \binom{2^l-1}{j} r_j(s)^{2^{2^l-j}} = w_{2^l-1}(s)^2.
\end{aligned}$$

Since $\gcd\left(2^{2^l}+1, 2^{2m}-1\right) = 1$ the Dickson polynomial is a permutation polynomial by Theorem 1.17. □

Definition 5.7. Let $Q_k(T)$ be a composition (with respect to the variable T and from right to left) of $k-1$ quadratic linearized polynomials

$$Q_k(T) = \left(T^2 + w_{k-1}(\sigma_1)T\right) \circ \left(T^2 + w_{k-2}(\sigma_1)T\right) \circ \cdots \circ \left(T^2 + w_1(\sigma_1)T\right).$$

We will see that the conjecture below implies Theorem 5.1 and hence all designs in Chapter 4 for every $k = 2^l$ which is a power of 2. This would be also a nice result since often almost every k can be represented as a power of 2 modulo m.

Conjecture 5.8 (Special case of Conjecture 5.4). *For every $l \geq 1$ the equation $P_{2^l}(T) = (\sigma_1 + 1)Q_{2^l}(T)$ holds.*

Partial verification. We have verified the claim with *Mathematica* for $l = 1,2,3,4$. This explains why we state Theorem 5.1 only for $\mathscr{G}_2$, $\mathscr{G}_4$, $\mathscr{G}_8$, and $\mathscr{G}_{16}$. □

Example 5.9. The conjecture can be proven easily without a computer in the first two cases:

$$Q_2(T) = T^2 + w_1(\sigma_1)T = T^2 + (\sigma_1^2 + \sigma_1 + 1)T$$

$$\begin{aligned}
Q_4(T) &= \left(T^2 + w_3(\sigma_1)T\right) \circ \left(T^2 + w_2(\sigma_1)T\right) \circ \left(T^2 + w_1(\sigma_1)T\right) \\
&= \left(T^2 + (\sigma_1^8 + \sigma_1^7 + \sigma_1^5 + \sigma_1^4 + \sigma_1^3 + \sigma_1 + 1)T\right) \circ \\
&\quad \left(T^2 + (\sigma_1^4 + \sigma_1^3 + \sigma_1^2 + \sigma_1 + 1)T\right) \circ \left(T^2 + (\sigma_1^2 + \sigma_1 + 1)T\right) \\
&= \left(T^2 + (\sigma_1^8 + \sigma_1^7 + \sigma_1^5 + \sigma_1^4 + \sigma_1^3 + \sigma_1 + 1)T\right) \circ \\
&\quad \left(T^4 + (\sigma_1^3 + \sigma_1)T^2 + (\sigma_1^6 + \sigma_1^4 + \sigma_1^3 + \sigma_1^2 + 1)T\right) \\
&= T^8 + (\sigma_1^8 + \cdots + 1)T^4 + (\sigma_1^{12} + \cdots + 1)T^2 + (\sigma_1^{14} + \cdots + 1)T
\end{aligned}$$

We mention that in the cases $k = 3,5,6$ we do not get a decomposition like $Q_k(T)$ and it may be that this approach is not applicable when $k \neq 2^l$.

The next theorem shows how we can count the number of solutions of (5.6) and complete our proof using the decomposition of $Q_{2^l}(T)$ and Conjecture 5.8.

Theorem 5.10. *For every $l \geq 1$ the equation $(\sigma_1 + 1)Q_{2^l}(T) = \sum_{i=1}^{2^l} a^{2^i}$ has exactly $(q-8)/2$ solutions which satisfy the conditions $\sigma_1 \in \mathbf{F}^a$ and $\mathrm{Tr}\left(\sigma_2/\sigma_1^2\right) = 0$.*

Proof. By the definition of $Q_{2^l}(T)$ the equation splits into a chain of 2^l-1 nested equations

$$\begin{aligned}(\sigma_1+1)\left[U_{2^l-1}^2+w_{2^l-1}(\sigma_1)U_{2^l-1}\right] &= \sum_{i=1}^{2^l} a^{2^i}\\ U_{2^l-2}^2+w_{2^l-2}(\sigma_1)U_{2^l-2} &= U_{2^l-1}\\ &\vdots\\ U_2^2+w_2(\sigma_1)U_2 &= U_3\\ U_1^2+w_1(\sigma_1)U_1 &= U_2.\end{aligned} \tag{5.7}$$

We show that the first equation has two roots for $(q-8)/2$ values of $\sigma_1 \in \mathbf{F}^a$ and that when we substitute these roots to the next equation this second equation has two roots for exactly one of the previous roots. And so on; we can always "drop down" one of the two roots.

We start now by studying the first equation in (5.7). By Lemma 1.4 and (iv) in Lemma 5.6 it has two roots if and only if

$$\mathrm{Tr}\left(\frac{\sum_{i=1}^{2^l} a^{2^i}}{w_{2^l-1}(\sigma_1)^2(\sigma_1+1)}\right) = \mathrm{Tr}\left(\frac{\sum_{i=1}^{2^l} a^{2^i}}{D_{2^{2^l}+1}(\sigma_1+1,1)}\right) = 0. \tag{5.8}$$

The denominator in the trace expression is a permutation polynomial with respect to the variable σ_1 and hence (5.8) has exactly $q/2-4$ solutions $\sigma_1 \in \mathbf{F}^a$ if

(a) the numerator is nonzero and

(b) every $\sigma_1 \in \{0,1,a,a+1\}$ is a solution.

Let us consider first the fact (a). We calculate the kernel of a linear polynomial mapping $p : \mathbf{F} \to \mathbf{F}$, $x \mapsto p(x) = \sum_{i=1}^{2^l} x^{2^i}$. We claim that

$$\ker p = \{x \in \mathbf{F} \mid p(x) = 0\} = \{0,1\}$$

which is equivalent to the identity $\gcd\left(p(x), x+x^{2^m}\right) = x+x^2$. Both polynomials are linearized and let us consider the conventional 2-associates of them (see [37, Section 3.4] for linearized and conventional 2-associates):

$$\begin{aligned}\gcd\left(\sum_{i=1}^{2^l} x^i, 1+x^m\right) = \gcd\left(\sum_{i=0}^{2^l-1} x^i, 1+x^m\right) \quad &\text{divides}\\ \gcd\left(1+x^{2^l}, 1+x^m\right) = 1+x^{\gcd\left(2^l,m\right)} &= 1+x.\end{aligned}$$

Then the linearized 2-associate is the claimed $x+x^2$. On the other hand, it is clear that the kernel contains $\{0,1\}$. So the numerator in (5.8) is nonzero because $a \in \mathbf{F}^{**}$.

In addition, the mapping p is two-to-one and therefore the solutions of the original equation correspond exactly to the cases with a and $a+1$ simultaneously, i.e., the cases (2a) and (2b) are grouped together.

For the fact (b) we consider (5.8) with $\sigma_1 \in \{0,1,a,a+1\}$. When $\sigma_1 = 1$ the denominator in (5.8) is equal to zero and this corresponds to $\mathrm{Tr}(0) = 0$. If $\sigma_1 = 0$, then $D_{2^{2^l}+1}(1,1) = 1$ and the equation holds. In the case $\sigma_1 = a+1$ we show that a quadratic equation

$$V^2 + D_{2^{2^l}+1}(a,1)V = \sum_{i=2}^{2^l+1} a^{2^i}$$

has a solution which implies

$$\mathrm{Tr}\left(\frac{\sum_{i=2}^{2^l+1} a^{2^i}}{D_{2^{2^l}+1}(a,1)^2}\right) = \mathrm{Tr}\left(\frac{\sum_{i=1}^{2^l} a^{2^i}}{D_{2^{2^l}+1}(a,1)}\right) = 0. \tag{5.9}$$

This solution is $V = \sum_{i=0}^{2^l} D_{2^{2^l}+1-2^i}(a,1)$ which is a sum of Dickson polynomials with degrees coming from a Dickson polynomial. We get

$$\begin{aligned} V^2 + D_{2^{2^l}+1}(a,1)V =& \sum_{i=1}^{2^l} D_{2^{2^l+1}+2-2^{i+1}}(a,1) + \sum_{i=1}^{2^l} D_{2^{2^l}+1+2^{2^l}+1-2^i}(a,1) \\ &+ \sum_{i=1}^{2^l} D_{2^{2^l}+1-\left(2^{2^l}+1-2^i\right)}(a,1) \\ =& D_2(a,1) + D_{2^{2^l}+1}(a,1) + \sum_{i=1}^{2^l} D_{2^i}(a,1) = \sum_{i=2}^{2^l+1} a^{2^i}. \end{aligned}$$

By substituting $a \mapsto a+1$ in (5.9) we see that (5.8) holds also when $\sigma_1 = a$ and this completes the proof of the fact (b).

We conclude that the first equation in (5.7) has two solutions U_{2^l-1} and $U_{2^l-1} + w_{2^l-1}(\sigma_1)$ for $(q-8)/2$ values of $\sigma_1 \in \mathbf{F}^a$.

The other equations have two solutions U_i and $U_i + w_i(\sigma_1)$ if and only if $\mathrm{Tr}\left(U_{i+1}/w_i(\sigma_1)^2\right) = 0$. Since

$$\mathrm{Tr}\left(\frac{U_{i+1} + w_{i+1}(\sigma_1)}{w_i(\sigma_1)^2}\right) = \mathrm{Tr}\left(\frac{U_{i+1}}{w_i(\sigma_1)^2}\right) + 1$$

exactly one of the solutions U_{i+1} and $U_{i+1} + w_{i+1}(\sigma_1)$ satisfies the trace condition of the next equation. In the last equation we have solutions $T = U_1$ and $T + w_1(\sigma_1)$ but exactly one of them satisfies the condition $\mathrm{Tr}\left(\sigma_2/\sigma_1^2\right) = 0$:

$$\mathrm{Tr}\left(\frac{T + a\sigma_1 + a^2}{\sigma_1^2}\right) = \mathrm{Tr}\left(\frac{T}{\sigma_1^2}\right) + \mathrm{Tr}\left(\frac{a}{\sigma_1} + \frac{a^2}{\sigma_1^2}\right) = \mathrm{Tr}\left(\frac{T}{\sigma_1^2}\right) \tag{5.10}$$

and

$$\mathrm{Tr}\left(\frac{T+w_1(\sigma_1)}{\sigma_1^2}\right)=\mathrm{Tr}\left(\frac{T}{\sigma_1^2}\right)+\mathrm{Tr}\left(\frac{1+\sigma_1+\sigma_1^2}{\sigma_1^2}\right)=\mathrm{Tr}\left(\frac{T}{\sigma_1^2}\right)+1.$$

□

We have $(q-8)/2$ solutions (σ_1,σ_2) which give us the variables y and z. The variable x can be solved from exactly one of the equations (5.3). The other solution $x+1$ refers to the same codeword and all in all we have $(q-8)/2$ codewords containing the three coordinates 0, 1, and a.

5.2.5 Cases (3a) and (3b)

The setting and the notation are the same as in the Subsection 4.3.5. This differs from the previous subsection such that the equations (5.3) are replaced by

$$\begin{aligned} x+x^2 &= a\sigma_1+\sigma_2+\sigma_1^2 \qquad \text{(3a)} \\ 1+x+x^2 &= a\sigma_1+\sigma_2+\sigma_1^2 \qquad \text{(3b)} \end{aligned} \tag{5.11}$$

so there is one additional term σ_1^2 in both equations. The ideas are exactly the same as above. By substituting $\sigma_2=T+a\sigma_1+a^2+\sigma_1^2$ we replace (5.5) by

$$\sum_{i=0}^{k-1}\left(T+a^2\right)^{2^i}=a^{2^k+1}+D_{2^k+1}\left(\sigma_1,T+a\sigma_1+a^2+\sigma_1^2\right)+(a+\sigma_1)^{2^k+1}$$

and using twice Lemma 1.15 we have

$$\sum_{i=0}^{k-1}\left(T+a^2\right)^{2^i}=D_{2^k+1}(\sigma_1,T)+(k+1)\sigma_1^{2^k+1}.$$

When k is even we get the same equation (5.6) as above and when k is a power of 2 we can also calculate the number of roots.

Theorem 5.10 holds also in the present case and replacing (5.10) by

$$\mathrm{Tr}\left(\frac{T+a\sigma_1+a^2+\sigma_1^2}{\sigma_1^2}\right)=\mathrm{Tr}\left(\frac{T}{\sigma_1^2}\right)+1$$

we see that the solutions in this case are exactly those which were ruled out in the last step of Theorem 5.10. Again the variable x can be solved from one of the equations (5.11) but this time every codeword is counted three times as in Subsection 4.3.5. All in all we have $(q-8)/6$ codewords containing the three coordinates 0, 1, and a.

5.3 Nonequivalence

It is natural to ask whether some of the 3-designs constructed from the codes $\mathscr{G}_k$ are equivalent for some k and k'.

Conjecture 5.11 (BCH). *The minimum weight codewords, i.e. the codewords of Hamming weight* 6*, generate the codes* $\mathscr{B}_k$*.*

Partial proof. We have verified this claim by computer for codelengths $\leq 2^9$. □

By (v) and (iv) in Example 2.8 this conjecture holds for Reed–Muller codes and $RM(m-3,m) \subset \mathscr{B}_k \subset RM(m-2,m)$ and therefore the conjecture seems quite natural.

Theorem 5.12 (Assuming BCH-conjecture). *The designs with block size* 7 *from the codes* $\mathscr{G}_k$*, see Theorem 2.30 and Corollary 5.2, are pairwise nonequivalent for different values of k.*

Proof. Suppose we have two equivalent designs $(\mathbf{F}, B_k)$ and $(\mathbf{F}, B_{k'})$ with block size 7 corresponding to values k and k'. So we have a permutation $p : \mathbf{F} \to \mathbf{F}$ such that $B_{k'} = p(B_k)$. We will deduce below that $\mathscr{B}_{k'} = p(\mathscr{B}_k)$ which implies by Example 2.7 that $k' = k$.

Consider arbitrary block $b \in B_k$. It is a support of swe-type X^6Y in $\mathscr{G}_k$ which can be divide into two parts: a X^6-part which is a support in $\mathscr{B}_k$ and one 2-position. We have all in all 16 blocks in B_k which contain the same X^6-part: one support of cwe-type X^6Y and 15 supports of cwe-type X^4YZ^2, see Subsection 5.2.2 for the lifting procedure.

Let $b' = p(b)$ so $b' \in \mathscr{B}_{k'}$ and b' consists of two parts as above. If the p-image of the X^6-part of b differs from the X^6-part of b', we have two codewords of weight 6 in $\mathscr{B}_{k'}$ which intersect in exactly 5 positions. This contradicts with the minimum distance of $\mathscr{B}_{k'}$. We conclude that p must map a minimum weight codeword of $\mathscr{B}_k$ to a minimum weight codeword of $\mathscr{B}_{k'}$ and assuming BCH-conjecture we see that p is a permutation of the codes $\mathscr{B}_k$ and $\mathscr{B}_{k'}$. □

We suspect that all designs considered are nonequivalent for every k (if they are not equal) but we could not prove it.

Conjecture 5.13. *All designs in Chapters 4 and 5 are pairwise nonequivalent for every k.*

Conclusions and open problems

We have examined the $\mathbf{Z}_4$-Goethals codes and their low-weight codewords. Some systems of equations connected to them were solved by representing the equations with Dickson polynomials and also some results about the Dickson polynomials were obtained in the course of study.

We introduced a unified decoding algorithm for all the codes $\mathscr{G}_k$ which corrects all error patterns up to the error-correcting capability. For the code $\mathscr{G}_1$ Helleseth and Kumar [21] presented even a *complete* decoding algorithm which suggests the following problem.

Problem 1. *Find a* complete *decoding algorithm for all the codes* $\mathscr{G}_k$.

We showed how several new families of 3-designs with block size 8 can be defined with the supports of codewords in $\mathscr{G}_1$. There are still some sets of supports that seem to define 3-designs. We have verified some cases by computer calculations, but have been unable to find general proofs.

Conjecture 4.13. *The class (iii) forms a* 3*-design.*

We generalized all the results in Chapter 4 to some codes $\mathscr{G}_k$ but, unfortunately, we could not do this for other values of k than $2, 4, 8$, and 16.

Conjecture 5.4. *All the results in Chapter 4 hold for every k.*

We could not find any results about $\mathrm{cwe}(\mathscr{G}_k)$ in the literature. Fortunately, we could prove Corollary 5.3 without this knowledge.

Problem 2. *Is* $\mathrm{cwe}(\mathscr{G}_k)$ *the same for all values of k?*

The study of the nonequivalence of the 3-designs in Chapter 5 aroused a claim concerning the structure of two-error-correcting BCH codes.

Conjecture 5.11. *The minimum weight codewords, i.e. the codewords of Hamming weight* 6*, generate the codes* $\mathscr{B}_k$.

This conjecture was used to obtain a partial result of the following general conjecture.

Conjecture 5.13. *All designs in Chapters 4 and 5 are pairwise nonequivalent for every k.*

The study of this thesis can be expanded to many directions. As suggestions for further research we conclude with two problems which were completely sidestepped in this thesis.

Problem 3. *Can one define* 3*-designs from larger supports of the codes* $\mathscr{G}_k$*?*

There are probably many designs definable from the supports of codewords in the codes $\mathscr{G}_k$ but the methods in this thesis may be inadequate and cumbersome for larger supports.

Problem 4. *What is the most general adaption of the Assmus–Mattson theorem in the* $\mathbf{Z}_4$*-domain? Can one use the notion of lifting rank in this setting?*

Bibliography

[1] E. F. Assmus, Jr. and H. F. Mattson, Jr. New 5-designs. *J. Combin. Theory*, 6:122–151, 1969.

[2] R. D. Baker, J. H. van Lint, and R. M. Wilson. On the Preparata and Goethals codes. *IEEE Trans. Inform. Theory*, 29(3):342–345, 1983.

[3] L. A. Bassalygo and V. A. Zinoviev. A remark on uniformly packed codes. *Problems Inform. Transmission*, 13(3):178–180, 1977.

[4] T. P. Berger. Automorphism groups and permutation groups of affine-invariant codes. In S. Cohen and H. Niederreiter, editors, *Finite Fields and Applications*, volume 233 of *London Mathematical Society Lecture Note Series*, pages 31–45, Glasgow, 1996. Cambridge University Press.

[5] E. R. Berlekamp, H. Rumsey, and G. Solomon. On the solution of algebraic equations over finite fields. *Information and Control*, 10(6):553–564, 1967.

[6] A. Bonnecaze, E. Rains, and P. Solé. 3-Colored 5-designs and $\mathbf{Z}_4$-codes. *J. Statist. Plann. Inference*, 86(2):349–368, 2000.

[7] A. R. Calderbank and G. McGuire. Construction of a $(64, 2^{37}, 12)$ code via Galois rings. *Des. Codes Cryptogr.*, 10(2):157–165, 1997.

[8] A. R. Calderbank, G. McGuire, P. V. Kumar, and T. Helleseth. Cyclic codes over $\mathbb{Z}_4$, locator polynomials, and Newton's identities. *IEEE Trans. Inform. Theory*, 42(1):217–226, 1996.

[9] P. Charpin. Open problems on cyclic codes. In V. S. Pless and W. C. Huffman, editors, *Handbook of Coding Theory*, volume I, chapter 11, pages 963–1063. Elsevier, 1998.

[10] W.-S. Chou, J. Gomez-Calderon, and G. L. Mullen. Value sets of Dickson polynomials over finite fields. *J. Number Theory*, 30(3):334–344, 1988.

[11] P. Delsarte and J. M. Goethals. Alternating bilinear forms over $GF(q)$. *J. Combin. Theory Ser. A*, 19(1):26–50, 1975.

[12] L. E. Dickson. The analytic representations of substitutions on a power of a prime number of letters with a discussion of the linear group. *Ann. of Math.*, 11:65–120, 161–183, 1896–1897.

[13] L. E. Dickson. *Linear Groups with an exposition of the Galois field theory*. Dover Publications, Inc., New York, 1958.

[14] I. I. Dumer. Some new uniformly packed codes. In *Proceedings of Moscow Institute of Physics and Technology*, pages 72–78, Moscow, 1976.

[15] I. Duursma, T. Helleseth, C. Rong, and K. Yang. Split weight enumerators for the Preparata codes with applications to designs. *Des. Codes Cryptogr.*, 18:103–124, 1999.

[16] J.-M. Goethals. Two dual families of nonlinear binary codes. *Electron. Lett.*, 10:471–472, 1974.

[17] J.-M. Goethals. Nonlinear codes defined by quadratic forms over GF(2). *Information and Control*, 31(1):43–74, 1976.

[18] T. A. Gulliver and M. Harada. Extremal double ciculant Type II codes over $\mathbb{Z}_4$ and construction of 5-$(24, 10, 36)$ designs. *Discrete Math.*, 194:129–137, 1999.

[19] 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*, 40(2):301–319, 1994.

[20] M. Harada. New 5-designs constructed from the lifted Golay code over Z_4. *J. Combin. Des.*, 6(3):225–229, 1998.

[21] T. Helleseth and P. V. Kumar. The algebraic decoding of the Z_4-linear Goethals code. *IEEE Trans. Inform. Theory*, 41(6):2040–2048, 1995.

[22] T. Helleseth, P. V. Kumar, and A. Shanbhag. Codes with the same weight distributions as the Goethals codes and the Delsarte-Goethals codes. *Des. Codes Cryptogr.*, 9(3):257–266, 1996.

[23] T. Helleseth, P. V. Kumar, and K. Yang. An infinite family of 3-designs from Preparata codes over Z_4. *Des. Codes Cryptogr.*, 15(2):175–181, 1998.

[24] T. Helleseth, C. Rong, and K. Yang. On t-designs from codes over $\mathbf{Z}_4$. *Discrete Math.*, 238:67–80, 2001.

[25] T. Helleseth and V. Zinoviev. New Kloosterman sums identities over F_{2^m} for all m. To appear in Finite Fields Appl.

[26] T. Helleseth and V. Zinoviev. On Z_4-linear Goethals codes and Kloosterman sums. *Des. Codes Cryptogr.*, 17:269–288, 1999.

[27] T. Helleseth and V. Zinoviev. Codes with the same coset weight distributions as the Z_4-linear Goethals codes. *IEEE Trans. Inform. Theory*, 47(4):1589–1595, 2001.

[28] T. Helleseth and V. Zinoviev. On coset weight distributions of the Z_4-linear Goethals codes. *IEEE Trans. Inform. Theory*, 47(5):1758–1772, 2001.

[29] N. Jacobson. *Basic Algebra I*. W. H. Freeman and Company, San Francisco, 1974.

[30] N. Jacobson. *Basic Algebra II*. W. H. Freeman and Company, San Francisco, 1980.

[31] F. M. Johnsen. *Cyclic Codes over* $\mathbf{Z}_4$*: A Computer Search*. Master's thesis, University of Bergen, Nov. 1995.

[32] A. M. Kerdock. A class of low-rate nonlinear binary codes. *Information and Control*, 20(2):182–187, 1972.

[33] D. L. Kreher. t-Designs, $t \geq 3$. In C. J. Colbourn and J. H. Dinitz, editors, *The CRC Handbook of Combinatorial Designs*, Discrete Mathematics and Its Applications, chapter I.3, pages 47–66. CRC Press, 1996.

[34] P. V. Kumar, T. Helleseth, A. R. Calderbank, and A. R. Hammons. Large families of quaternary sequences with low correlation. *IEEE Trans. Inform. Theory*, 42(2):579–592, 1996.

[35] J. Lahtonen. Decoding the 6-error-correcting $\mathbf{Z}_4$-linear Calderbank–McGuire code. In *2000 IEEE International Symposium on Information Theory: Sorrento, Italy, 25-30 June*, page 446, 2000.

[36] R. Lidl, G. L. Mullen, and G. Turnwald. *Dickson Polynomials*, volume 65 of *Pitman Monographs and Surveys in Pure and Applied Mathematics*. Longman Scientific & Technical, Harlow, 1993.

[37] R. Lidl and H. Niederreiter. *Finite Fields*, volume 20 of *Encyclopedia of Mathematics and Its Applications*. Addison-Wesley, 1983.

[38] F. J. MacWilliams and N. J. A. Sloane. *The Theory of Error-Correcting Codes*, volume 16 of *North-Holland Mathematical Library*. North-Holland, ninth edition, 1996.

[39] B. R. McDonald. *Finite Rings with Identity*. Marcel Dekker Inc., New York, 1974.

[40] W. Nöbauer. Über eine Klasse von Permutationspolynomen und die dadurch dargestellten Gruppen. *J. Reine Angew. Math.*, 231:215–219, 1968.

[41] A. A. Nechaev. Kerdock code in a cyclic form. *Discrete Math. Appl.*, 1(4):365–384, 1991.

[42] A. W. Nordstrom and J. P. Robinson. An optimum nonlinear code. *Information and Control*, 11(5/6):613–616, 1967.

[43] L. Ojala. *Elliptiset käyrät yli äärellisten kuntien*. Master's thesis, University of Turku, Nov. 2001.

[44] V. S. Pless, W. C. Huffman, and R. A. Brualdi. An introduction to algebraic codes. In V. S. Pless and W. C. Huffman, editors, *Handbook of Coding Theory*, volume I, chapter 1, pages 3–139. Elsevier, 1998.

[45] F. P. Preparata. A class of optimum nonlinear double-error-correcting codes. *Information and Control*, 13(4):378–400, 1968.

[46] K. Ranto. On algebraic decoding of the $\mathbf{Z}_4$-linear Goethals-like codes. *IEEE Trans. Inform. Theory*, 46(6):2193–2197, 2000.

[47] K. Ranto. Infinite families of 3-designs from $\mathbf{Z}_4$-Goethals codes with block size 8. *SIAM J. Discrete Math.*, 15(3):289–304, 2002.

[48] C. Rong, T. Helleseth, and J. Lahtonen. On algebraic decoding of the $\mathbb{Z}_4$-linear Calderbank–McGuire code. *IEEE Trans. Inform. Theory*, 45(5):1423–1434, 1999.

[49] N. V. Semakov, V. A. Zinoviev, and G. V. Zaitsev. Uniformly close-packed codes. *Problems Inform. Transmission*, 7(1):30–39, 1971.

[50] N. V. Semakov, V. A. Zinoviev, and G. V. Zaitsev. Interrelation of Preparata and Hamming codes and extension of Hamming codes to new double-error-correcting codes. In B. N. Petrov and F. Csáki, editors, *2nd International Symposium on Information Theory: Tsahkadsor, Armenia, USSR, Sept. 2–8, 1971*, pages 257–263, Akadémiai Kiadó, Budapest, 1973.

[51] D.-J. Shin, P. V. Kumar, and T. Helleseth. 3-Designs from the Z_4-Goethals codes via a new Kloosterman sum identity. To appear in Des. Codes Cryptogr.

[52] D.-J. Shin, P. V. Kumar, and T. Helleseth. An Assmus–Mattson-type approach for identifying 3-designs from linear codes over Z_4. To appear in Des. Codes Cryptogr.

[53] D.-J. Shin, P. V. Kumar, and T. Helleseth. 5-Designs from the lifted Golay code over Z_4 via an Assmus–Mattson type approach. *Discrete Math.*, 241:479–487, 2001.

[54] K. Tanabe. An Assmus–Mattson theorem for $\mathbf{Z}_4$-codes. *IEEE Trans. Inform. Theory*, 46(1):48–53, 2000.

[55] K. Yang and T. Helleseth. Two new infinite families of 3-designs from Kerdock codes over Z_4. *Des. Codes Cryptogr.*, 15(2):201–214, 1998.