New infinite families of 3-designs from the $\mathbb{Z}_4$-Goethals Codes

Kalle Ranto

Turku Centre for Computer Science TUCS
FIN-20520 Turku, Finland
e-mail: kara@utu.fi

Turku Centre for Computer Science
TUCS Technical Report No 394
February 2001
ISBN 952-12-0785-X
ISSN 1239-1891

Abstract

We construct several new families of simple 3-designs from codewords of the $\mathbf{Z}_4$-Goethals codes. These designs have parameters $3-(2^m, 8, \lambda)$ with odd $m \geq 5$. The smallest design has $\lambda = 14(2^m - 8)/3$ and the others are corollaries of this and some previously known designs.

Keywords: t-designs, Goethals codes, quaternary codes, Kloosterman sums

TUCS Research Group
Coding Theory Group

1 Introduction

Let D be a set of v elements. Then a collection of k-subsets (or blocks) of D is called a $t-(v,k,\lambda)$ *design* if any t elements of D are contained in exactly λ k-subsets (or blocks). A design is called *simple* if all the blocks are distinct, otherwise the design is said to have *repeated blocks*. In this paper all designs considered are simple unless otherwise stated.

Research on constructing t-designs from $\mathbf{Z}_4$-codes started with Harada [7]. He showed by computer search that the supports of codewords of Hamming weight 10 and 12 in the $\mathbf{Z}_4$-Golay code yield 5-(24,10,36), 5-(24,12,1584), and 5-(24,12,1632) designs. This result was later proved analytically by Bonnecaze, Rains, and Solé [4] and Shin, Kumar, and Helleseth [12].

In addition to the above interesting but restricted designs, Helleseth, Kumar, and Yang [9] have constructed an infinite family of 3-designs from the $\mathbf{Z}_4$-Preparata codes. The supports of codewords of Hamming weight 5 form a $3-(2^m,5,10)$ design for all odd $m \geq 3$.

From the $\mathbf{Z}_4$-Goethals code Shin, Kumar, and Helleseth [11] constructed a $3-(2^m,7,14(2^m-8)/3)$ design for odd $m \geq 5$ by taking the supports of codewords of Hamming weight 7. In this paper we introduce the notion of a *lifting rank* and classify the supports of codewords of Hamming weight 8 by their lifting rank and symmetrized weight. The supports in one class define a $3-(2^m,8,14(2^m-8)/3)$ design. It is interesting that this design has exactly the same parameters as the design mentioned above except the block size which is equal to 8. This relation is explained in Section 6.

There have also been attempts to give some general theorems to decide whether the supports of some codewords would form a t-design. The results are usually more complicated than the celebrated Assmus-Mattson theorem [1] in the case of linear codes over finite fields. Our new design can not be derived from the theorem by Shin, Kumar, and Helleseth [13] but this theorem is used to derive Corollary 3. We also think that the theorem by Tanabe [14] does not give any designs from the $\mathbf{Z}_4$-Goethals code. The required calculations are messy and not included in this paper.

In Section 2 we recall some notions and results from coding theory and the theory of finite fields. Section 3 is devoted to the $\mathbf{Z}_4$-Goethals codes and their structure. In Section 4 we list the known 3-designs related to our discussion. Section 5 gives the main theorem and the corollaries and in Section 6 we describe the relation between the main theorem and Theorem 6. In Section 7 we come to conclusions and describe some further research. Finally, in Appendix A we prove the main theorem and in Appendix B we prove Corollary 1.

2 Preliminaries

Let $m \geq 5$ be an odd integer and let $\mathbf{Z}_l$ denote the ring of integers modulo l.

We consider linear $\mathbf{Z}_4$-codes of length 2^m which are subgroups of $\mathbf{Z}_4^{2^m}$ with componentwise addition. Let $\mathbf{c} = (c_1, \ldots, c_{2^m})$ be a codeword.

Definition 1. The *support* of $\mathbf{c}$ is $\chi(\mathbf{c}) = \{k \mid c_k \neq 0\}$ and the *multiplicity* of $i \in \mathbf{Z}_4$ in $\mathbf{c}$ is $n_i(\mathbf{c}) = |\{k \mid c_k = i\}|$.

cwe The *complete weight enumerator* of $\mathbf{c}$ is $W^{n_0(\mathbf{c})}X^{n_1(\mathbf{c})}Y^{n_2(\mathbf{c})}Z^{n_3(\mathbf{c})}$.

swe The *symmetrized weight enumerator* of $\mathbf{c}$ is $W^{n_0(\mathbf{c})}X^{n_1(\mathbf{c})+n_3(\mathbf{c})}Y^{n_2(\mathbf{c})}$.

hwe The *Hamming weight enumerator* of $\mathbf{c}$ is $W^{n_0(\mathbf{c})}X^{n_1(\mathbf{c})+n_2(\mathbf{c})+n_3(\mathbf{c})}$.

lwe The *Lee weight enumerator* of $\mathbf{c}$ is $W^{n_0(\mathbf{c})}X^{n_1(\mathbf{c})+2n_2(\mathbf{c})+n_3(\mathbf{c})}$.

The *weight enumerator* of a code is the sum of the enumerators of the codewords.

If there is no ambiguity, the variable W can be excluded. Clearly, supports of binary codewords can be identified with the codewords and this is usually done without mentioning.

Now we consider some properties of the finite field $\mathbf{F}$ of 2^m elements. Let $\mathrm{Tr}(x)$ denote the trace function from $\mathbf{F}$ to the binary field $\mathbf{F}_2$. The following lemma is well-known.

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

Equation $x^2 + bx + a = 0$ where $b \neq 0$ can be transformed to $(x/b)^2 + x/b + a/b^2 = 0$ and the condition in the previous lemma changes to $\mathrm{Tr}(a/b^2) = 0$.

We denote sets $\mathbf{F} \setminus \{0\}$ and $\mathbf{F} \setminus \{0, 1\}$ by $\mathbf{F}^*$ and $\mathbf{F}^{**}$, respectively. Berlekamp, Rumsey, and Solomon [3] have proved the following result.

Lemma 2. *The cubic equation $x^3 + x = a$ with $a \in \mathbf{F}^*$ has a unique solution in $\mathbf{F}$ iff $\mathrm{Tr}(1/a) \neq \mathrm{Tr}(1)$. For $a = 0$ the equation has two roots, namely 0 and 1, for $(2^m - 2)/2$ values of a the equation has a unique root, and for $(2^m - 2)/6$ values of a the equation has three roots.*

In the proof of the main theorem we use the Kloosterman sums and the identity of the next theorem.

Definition 2. The *Kloosterman sum* $K(a)$ for $a \in \mathbf{F}^*$ is defined as

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

Theorem 1. *For every $a \in \mathbf{F}^{**}$*

$$K\left(a^3(a+1)\right) = K\left(a(a+1)^3\right).$$

Proof. Shin, Kumar, and Helleseth [11] have proved the identity

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

for every $a \in \mathbf{F}^{**}$. By substituting $a \mapsto a/(1+a)$ in this identity we get the claim. It is obvious that this substitution is a permutation $\mathbf{F}^{**} \to \mathbf{F}^{**}$. $\square$

3 $\mathbf{Z}_4$-Goethals Codes

Let $R = \mathrm{GR}(4, m)$ be a Galois ring of characteristic 4 with 4^m elements. The multiplicative group of units R^* contains a unique cyclic subgroup $\langle \beta \rangle$ of order $2^m - 1$. Every element of R can be expressed uniquely as $A + 2B$ where $A, B \in \mathcal{T}$ and

$$\mathcal{T} = \{0, 1, \beta, \dots, \beta^{2^m - 2}\}.$$

Let $\mu : \mathbf{Z}_4 \to \mathbf{Z}_2$ denote the modulo 2 reduction map. We extend μ to R in a natural way and thus $\mu(\mathcal{T}) = \mathbf{F}$.

The $\mathbf{Z}_4$-Goethals code $\mathcal{G}$ is defined by the parity-check matrix

$$H_{\mathcal{G}} = \begin{bmatrix} 1 & 1 & 1 & 1 & \dots & 1 \\ 0 & 1 & \beta & \beta^2 & \dots & \beta^{2^m-2} \\ 0 & 2 & 2\beta^3 & 2\beta^6 & \dots & 2\beta^{3(2^m-2)} \end{bmatrix},$$

that is, $\mathbf{c} \in \mathcal{G}$ iff $\mathbf{c}H_{\mathcal{G}}^T = \mathbf{0}$. It is natural to index the codewords with the elements of $\mathcal{T}$ and then $\mathbf{c} \in \mathcal{G}$ iff

$$\begin{aligned} \sum_{X \in \mathcal{T}} c_X &= 0 \\ \sum_{X \in \mathcal{T}} c_X X &= 0 \\ 2 \sum_{X \in \mathcal{T}} c_X X^3 &= 0. \end{aligned} \tag{1}$$

3.1 From Ring Equations to Field Equations

Helleseth and Kumar [8] have proved the following lemma which we use to transform the above equations to equations over the finite field.

Lemma 3. *Let $(c_X)_{X \in \mathcal{T}} \in \mathbf{Z}_4^{2^m}$ and $C_j = \{\mu(X) \mid c_X = j\}$ for $j = 0, 1, 2, 3$. The equation*

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

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

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

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

We transform the last two equations from (1) to the following set of equations over $\mathbf{F}$:

$$\begin{aligned}\sum_{x\in C_1\cup C_3} x &= 0\\ \sum_{x\in C_2\cup C_3} x^2 &= \sum_{\substack{x,y\in C_1\cup C_3\\ x<y}} xy \\ \sum_{x\in C_1\cup C_3} x^3 &= 0.\end{aligned} \tag{2}$$

As we have equations over $\mathbf{F}$ it is natural to think that the codewords are indexed with the elements of $\mathbf{F}$. With the next lemma by Hammons et al. [6] we can decrease the needed case-by-case analysis in the proof of the main theorem.

Lemma 4. *The automorphism group of $\mathcal{G}$ contains the doubly transitive group of affine permutations*

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

3.2 Low-Weight Codewords and Supports

Some of the following facts are well-known and others can be easily deduced from (2). For more information the reader is referred to [6]. The $\{0, 2\}$-subcode of $\mathcal{G}$ is denoted by $\mathcal{G}_{[0,2]} = \{\mathbf{c} \in \mathcal{G} \mid n_0(\mathbf{c}) + n_2(\mathbf{c}) = 2^m\}$.

Lemma 5.

(i) *The minimum Lee distance of $\mathcal{G}$ is 8.*

(ii) $\mu(\mathcal{G}) = \mathrm{eBCH}$ *the extended double-error-correcting BCH code.*

(iii) $\mathcal{G}_{[0,2]} = 2\,\mathrm{eHamming}$ *the extended Hamming code.*

(iv) *All cwe-types of codewords of Hamming weight ≤ 6 are: Y^4 and Y^6.*

(v) *All cwe-types of codewords of Hamming weight 7 are:* X^6Y, X^4YZ^2, X^2YZ^4, *and* YZ^6.

(vi) *Any two distinct codewords $\mathbf{c}$ and $\mathbf{d}$ of Hamming weight 7 have the same support iff $\mathbf{c} = -\mathbf{d}$.*

(vii) *All cwe-types of codewords of Hamming weight 8 are:* X^8, X^6Z^2, X^4Z^4, X^2Z^6, Z^8, X^5Y^2Z, $X^3Y^2Z^3$, XY^2Z^5, *and* Y^8.

(viii) *Any two distinct codewords $\mathbf{c}$ and $\mathbf{d}$ of swe-type X^6Y^2 have the same support iff $\mathbf{c} = -\mathbf{d}$.*

The supports of codewords of swe-type X^8 are distributed in a more complicated manner. For example, there are codewords like 11111111 and 11113333 which have the same support. Below we shorten sentences by using phrase "support of swe-type X^8" instead of "support of codeword of swe-type X^8".

Definition 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 the generator matrix of $\mathcal{G}|_S = \{\mathbf{c} \in \mathcal{G} \mid \chi(\mathbf{c}) \subseteq S\}$ is permutation-equivalent to a matrix of the form

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

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 the rank is a non-negative integer at most 3. The supports of rank 3 are special: they are 3-flats in affine geometry, or equivalently, minimum weight codewords in the Reed-Muller code $RM(m, m-3)$, see for example [10, Chapter 13]. In the next lemma we analyze the possible ranks and the corresponding subcodes.

Lemma 6. *Let S be a support of swe-type X^8. Then S belongs to one of the following classes:*

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

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

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

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

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

Proof. If S has rank 3, then there is a codeword with this support and of cwe-type X^8 in $\mathcal{G}$ 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 $\{x_1, x_2, x_3, x_4, x_5, y_1, y_2, y_3\}$, $y_i \notin S$. Again the codeword with this support and of cwe-type X^8 belongs to $\mathcal{G}$. Considering case-by-case we see that only the combination (ii) can exist and in this case codewords 11111133 and 11133313 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 the Lee minimum distance of $\mathcal{G}$.

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

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

The main theorem says that the supports of the class (ii) define a 3-design.

4 Known 3-designs

In this section we describe some known 3-designs which are connected to our new results. All designs have $v = 2^m$.

The Assmus-Mattson theorem [1] gives a sufficient condition for the codewords of a constant Hamming weight in a linear code over a finite field to form a t-design. This theorem is applicable to the codes $\mathrm{eHamming}$ and eBCH, that is, $\mathcal{G}_{[0,2]}$ and $\mu(\mathcal{G})$. The weight distributions of these codes are well-known and λ's can be calculated from the identity

$$\binom{v}{t}\,\lambda = \binom{k}{t}\,b$$

where b denotes the number of blocks.

Theorem 2. *The Assmus-Mattson theorem implies the existence of the following designs:*

(i) The supports of cwe-type Y^4 *in* $\mathcal{G}$ *form a* $3-(v,4,1)$ *design.*

(ii) The supports of cwe-type Y^6 *in* $\mathcal{G}$ *form a* $3-(v,6,\frac{(v-4)(v-8)}{6})$ *design.*

(iii) The supports of cwe-type Y^8 *in* $\mathcal{G}$ *form a* $3-(v,8,\frac{(v-4)(v-6)(v^2-15v+71)}{120})$ *design.*

(iv) The supports of hwe-type X^6 *in* eBCH *form a* $3-(v,6,\frac{v-8}{6})$ *design.*

(v) The supports of hwe-type X^8 *in* eBCH *form a* $3-(v,8,\frac{v^3-25v^2+246v-760}{120})$ *design.*

The following theorem can be proved simply by counting the 3-flats which contain some fixed three points.

Theorem 3. *The supports of swe-type* X^8 *and rank 3 in* $\mathcal{G}$ *form a* $3-(v,8,\frac{v-4}{4})$ *design.*

To derive Corollary 1 from our main theorem we need one design with a different size of a base set. Let ϕ be the Gray map which maps $\mathbf{Z}_4$-codewords componentwise to binary words by the rules: $\phi(0) = 00$, $\phi(1) = 01$, $\phi(2) = 11$ and $\phi(3) = 10$. The binary code $\phi(\mathcal{G})$ has the same weight distribution as the binary Goethals code [6] and the following theorem is derived from the results of Bassalygo and Zinoviev [2].

Theorem 4. *The supports of hwe-type* X^8 *in* $\phi(\mathcal{G})$ *form a* $3-(2v,8,\frac{(2v-4)(4v-17)}{60})$ *design.*

For Corollary 3 we need the following theorem from [13].

Theorem 5. *The supports of any fixed Hamming weight in* $\mathcal{G}$ *form a 3-design possibly with repeated blocks.*

The next result by Shin, Kumar, and Helleseth [11] is the starting point for this paper.

Theorem 6. *The supports of hwe-type* X^7 *in* $\mathcal{G}$ *form a* $3-(v, 7, \frac{14}{3}(v-8))$ *design.*

5 New 3-designs

We now state our main theorem and deduce some corollaries. The proof of the main theorem is postponed to Appendix A.

Theorem 7 (Main Theorem). *The supports of cwe-type* X^6Z^2 *and rank 1 in* $\mathcal{G}$ *form a* $3-(v, 8, \frac{14}{3}(v-8))$ *design.*

By Lemma 6 we could use in the main theorem supports of cwe-type X^2Z^6 and rank 1, supports of cwe-type X^4Z^4 and rank 1, or supports of swe-type X^8 and rank 1. The supports would be the same.

Corollary 1. *The supports of swe-type* X^8 *in* $\mathcal{G}$ *form a* $3-(v, 8, \frac{32v^2-985v+5892}{60})$ *design.*

The proof of Corollary 1 can be found from Appendix B.

Clearly, the supports of swe-type X^8 and rank $\neq 3$ in $\mathcal{G}$ define a $3-(v, 8, 2(v-8)(4v-93)/15)$ design, the supports of swe-type X^8 and rank $\neq 1$ in $\mathcal{G}$ define a $3-(v, 8, (32v^2-1265v+8132)/60)$ design, and the supports of swe-type X^8 and rank 0 in $\mathcal{G}$ define a $3-(v, 8, 8(v-8)(v-32)/15)$ design.

Corollary 2. *The supports of hwe-type* X^8 *in* eBCH *which can not be lifted to codewords of swe-type* X^8 *in* $\mathcal{G}$ *form a* $3-(v, 8, \frac{(v-8)(v-32)(v-49)}{120})$ *design.*

Proof. The result is straigtforward consequence of the design (v) in Theorem 2 and Corollary 1, and we get

$$\lambda = \frac{v^3-25v^2+246v-760}{120} - \frac{32v^2-985v+5892}{60} = \frac{(v-8)(v-32)(v-49)}{120}.$$

□

Corollary 3. *The supports of swe-type* X^6Y^2 *in* $\mathcal{G}$ *form a* $3-(v, 8, \frac{56(v-8)(v-12)}{15})$ *design.*

Proof. The supports of hwe-type X^8 define a 3-design possibly with repeated blocks by Theorem 5. We can calculate λ from $\mathrm{cwe}(\mathcal{G}^{\perp})$ (counted in [13]) and it is equal to

$$\lambda^* = \frac{v^4-25v^3+1269v^2-21390v+100648}{120}.$$

The blocks of this design are of swe-types Y^8, X^8, and X^6Y^2 by Lemma 5. We drop out all codewords of swe-types Y^8 and X^8 and we substract the corresponding λ's, that is, by Theorem 2 and (11) we have

$$\begin{aligned}\lambda &= \lambda^* - \frac{(v-4)(v-6)(v^2-15v+71)}{120} - \frac{4(4v^2-75v+404)}{15}\\ &= \frac{112}{15}(v-8)(v-12).\end{aligned}$$

We take the supports of the remaining codewords and by item (viii) in Lemma 5 we get a simple 3-design with a parameter $\lambda/2$. □

5.1 Examples with $v = 32$

The designs from the $\mathbf{Z}_4$-Goethals code of length 32 are quite different from the longer ones. Duursma et al. [5] noticed that for the length 32 the automorphism group of $\mathcal{G}$ is 3-homogenous (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.

The code $\mathcal{G}$ of length 32 has no codewords of swe-type X^8 and rank 0. This means that the main theorem accounts for all the codewords of cwe-type X^6Z^2. In addition, all codewords of Hamming weight 8 in eBCH can be lifted to codewords of swe-type X^8 in $\mathcal{G}$. Therefore the design of Corollary 1 is equal to the design (v) in Theorem 2 and the design in Corollary 2 is empty. All in all we get only two new designs:

- $3-(32,8,112)$ design (Main Theorem)
- $3-(32,8,1792)$ design (Corollary 3)

By the above mentioned result of Duursma et al., we can split the second design to two simple $3-(32,8,672)$ and $3-(32,8,1120)$ designs corresponding to the supports of cwe-types X^5Y^2Z and $X^3Y^2Z^3$, respectively.

Interestingly, for length 32 we have $3-(32,6,112)$, $3-(32,7,112)$, and $3-(32,8,112)$ designs by (ii) in Theorem 2, Theorem 6, and Theorem 7, respectively.

5.2 Examples with $v = 128$

In the $\mathbf{Z}_4$-Goethals code of length 128 all classes of Lemma 6 are nonempty. We get the following new designs:

- $3-(128,8,560)$ design (Main Theorem)
- $3-(128,8,6735)$ design (Corollary 1)
- $3-(128,8,7584)$ design (Corollary 2)
- $3-(128,8,51968)$ design (Corollary 3)

By computer we can verify also the existence of the following designs:

- $3-(128, 8, 2688)$ design (supports (iii) from Lemma 6)
- $3-(128, 8, 3456)$ design (supports (iv) and (v) from Lemma 6)

5.3 Remark in the case $v = 512$

Again, by computer we can verify the existence of the following designs:

- $3-(512, 8, 56448)$ design (supports (iii) from Lemma 6)
- $3-(512, 8, 72576)$ design (supports (iv) and (v) from Lemma 6)

6 Link between Theorems 6 and 7

There is a considerable similarity between the proofs of Theorems 6 and 7. There are similar exponential sums and Kloosterman sum identities in these proofs. Also the equality of λ's in the corresponding designs suggests that there might be some structural dependence between the blocks of these designs.

After completing the proof in Appendix A the author discovered a connection between the two designs. This connection is shown in Table 1 and it is explained below. This link makes the main theorem as a corollary of Theorem 6, or conversely, Appendix A gives us an shorter and more uniform proof for Theorem 6 as the original one.

The case notations refer to cases in Appendix A and Table 2. We assume that we have three fixed coordinates 0, 1, and $a \in \mathbf{F}^{**}$ and we consider blocks containing them. The corresponding $\mathbf{Z}_4$-symbols in these positions are shown in the column below $01a$-entry. Actually, in this proof the three positions could be arbitrary.

The correspondence relating the two designs associates a word of Hamming weight 7 with a word of Hamming weight 8 and rank 1 iff their difference is a codeword of Hamming weight 8 and rank 3 (i.e. the support of the difference is a 3-flat).

There is a unique way of completing a set of three points into a 2-flat. Similarly any 2-flat and a fifth point outside it determine a unique 3-flat. By item (vi) in Lemma 5 the support of Hamming weight 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. On the other hand, one of the two 2-flats in the word of Hamming weight 8 and rank 1 and one extra point can be uniquely completed to a 3-flat.

Table 1 shows that we can form a block of the other design starting with a block of the other by suitable positioning 3's and 1's within a 3-flat. 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 in this manner. This number is indicated in the Comb-column.

Table 1: Structural Dependence of Blocks in Theorems 6 and 7

Case	Theorem 6 → Theorem 7				Theorem 7 → Theorem 6			
	$01a$		Comb	Freq	$01a$		Comb	Freq
(0a)	111	1112			$\underline{111}$	$\underline{3}1113$		
		$\underline{333}1\underline{3}111$				$1\underline{3333}111$		
	$\underline{111}$	$3\underline{3}111$		$\frac{2(v-8)}{3}$	111	2111		$\frac{v-8}{6}$
	111	1332			$\underline{111}$	$\underline{3}1113$		
		$\underline{311}3\underline{3}113$				$1\underline{3311}133$	3	
	$\underline{111}$	$1\underline{3}113$			111	2 133		
(0b)	113	3332			$\underline{113}$	$\underline{1}1113$		
		$\underline{111}1\underline{1}111$				$3\underline{3333}333$		
	$\underline{113}$	$3\underline{1}111$		$\frac{2(v-8)}{3}$	113	2333		$\frac{v-8}{6}$
	113	3112			$\underline{113}$	$\underline{1}1113$		
		$\underline{133}3\underline{1}113$				$3\underline{3311}311$	3	
	$\underline{113}$	$1\underline{1}113$			113	2 311		
(1a)	112	1133			$\underline{111}$	$\underline{13}113$		
	3	$\underline{331}$ $\underline{1}311$	2		$\underline{1}$	3 $\underline{331}311$		
	$\underline{11}1$	$\underline{31}311$			112	3 311		
	112	1133			$\underline{111}$	$\underline{13}113$		
	3	$\underline{3113}311$	2		$\underline{1}$	$1\underline{331}133$		
	$\underline{11}1$	$\underline{1}$ $\underline{3}311$		$\frac{v-8}{3}$	112	1 133		$\frac{2(v-8)}{3}$
(1b)	112	1111			$\underline{11}3$	$\underline{13}111$		
	1	$\underline{333}$ $\underline{3}111$	4		$\underline{3}$	$1\underline{333}111$		
	$\underline{11}3$	$\underline{13}111$			112	1 111		
	112	3333			$\underline{11}3$	$\underline{13}111$		
	1	$\underline{111}$ $\underline{1}111$	4		$\underline{3}$	3 $\underline{333}333$		
	$\underline{11}3$	$\underline{31}111$			112	3 333		
(2a)	132	1113			$\underline{13}1$	$\underline{11}113$		
	3	$\underline{3311}311$	3		$\underline{1}$	3 $\underline{331}311$	2	
	$\underline{13}1$	$\underline{1}$ $\underline{1}311$			132	1 311		$\frac{v-8}{2}$
(2b)	312	1113			$\underline{31}1$	$\underline{11}113$		
	3	$\underline{3311}311$	3		$\underline{1}$	3 $\underline{331}311$	2	
	$\underline{31}1$	$\underline{1}$ $\underline{1}311$		$\frac{v-8}{3}$	312	1 311		
(3a)	132	3331			$\underline{13}3$	$\underline{11}111$		
	1	$\underline{111}$ $\underline{1}111$			$\underline{3}$	3 $\underline{333}333$	2	
	$\underline{13}3$	$\underline{11}111$			132	1 333		$\frac{v-8}{6}$
(3b)	312	3331			$\underline{31}3$	$\underline{11}111$		
	1	$\underline{111}$ $\underline{1}111$			$\underline{3}$	3 $\underline{333}333$	2	
	$\underline{31}3$	$\underline{11}111$			312	1 333		

For example in the first case in (1a) we can choose the position of 1 from the two positions of 3 in the original codeword. One of the 2-flats inside the 3-flat is indicated by underlining its positions. The resulting codeword has rank 1 since rank 3 would contradict the minimum distance of $RM(m, m-3)$. In this word one of the two 2-flats is again underlined.

The frequencies in the right side can be taken from Table 2 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 codeword of cwe-type X^6Z^2 and rank 1 from one codeword of Hamming weight 7. On the other hand, from one codeword of cwe-type X^6Z^2 and rank 1 we can construct four codewords of Hamming weight 7. This means that in this case the number of blocks in Theorem 6 must be four times the number of blocks in Theorem 7. This gives us an alternative proof for Theorem 6.

On the other hand, if we take the frequencies in the left side from [11] we can count the frequencies in the right side and get another proof for the main theorem.

7 Conclusions and Further Research

We have constructed several new infinite families of simple 3-designs from the codewords of Hamming weight 8 in the $\mathbf{Z}_4$-Goethals codes. This was done by analyzing the low-weight codewords and counting the number of solutions to certain systems of equations over finite fields. In addition, we described the correspondence between the designs in Theorems 6 and 7.

There are many open problems in this area and we state a few of them. Can one find the designs mentioned in Section 5.3 also for other lengths? Can one generalize the results in this paper to the $\mathbf{Z}_4$-Goethals-like codes? Can one find simple designs from codewords of a larger Hamming weight? Last but not least: What is the most general adaptation of the Assmus-Mattson theorem in the $\mathbf{Z}_4$-domain? This work suggests that lifting rank may play a key role.

Appendices

A Proof of the Main Theorem

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 Lemma 4 we can assume that the 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 6 shows that supports and codewords (of this considered type) can be identified and we know that the support is a union of two 2-flats and both of them contain one position with a 3. In other words, codeword is split in the two 2-flats like: 1113 and 1113. This leads to a total of 22 combinations of postitions 0, 1, and a among the two 2-flats and 1's and 3's as shown in Table 2. 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 $14(v-8)/3$ and the supports, indeed, form a 3-design.

Table 2: 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						$(v-8)/6$
(0b)	0	1		a					$(v-8)/6$
(0c)	0	a		1					$(v-8)/6$
(0d)	1	a		0					$(v-8)/6$
(1a)	0	1			a				$\frac{2(v-8)}{3}$
(1b)	0	1						a	
(2a)	0			1	a				$\frac{v-8}{2}$
(2b)	1			0	a				
(3a)	0			1				a	$\frac{v-8}{6}$
(3b)	1			0				a	
(4)	0	a			1				$\frac{2(v-8)}{3}$
	0	a						1	
(5)	0			a	1				$\frac{v-8}{2}$
	a			0	1				
(6)	0			a				1	$\frac{v-8}{6}$
	a			0				1	
(7)	1	a			0				$\frac{2(v-8)}{3}$
	1	a						0	
(8)	1			a	0				$\frac{v-8}{2}$
	a			1	0				
(9)	1			a				0	$\frac{v-8}{6}$
	a			1				0	

A.1 Cases (0c), (0d), and (4)-(9)

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 Lemma 4 we get a codeword which includes the positions 0, $1/a$ and 1. This permuted codeword is counted in the case (0c) with a parameter $1/a \in \mathbf{F}^{**}$. Conversely, the codewords counted in (0b) are permuted versions of codewords in (0c) 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 (4)-(6). Another permutation $x \mapsto x+1$ links the case (0c) with (0d) and cases (4)-(6) with (7)-(9). All in all we conclude that it suffices to prove only the cases (0a), (0b) and (1a)-(3b).

A.2 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 2 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) and the 2-flat structure the following equations should hold for the support:

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

where $\sigma_k(a_1, \ldots, a_n) = \sum_{1 \le i_1 < \cdots < i_k \le n} a_{i_1} \ldots a_{i_k}$ is the kth elementary symmetric polynomial and $S_k(a_1, \ldots, a_n) = \sum_{i=1}^{n} a_i^k$ is the sum of kth powers.

We abbreviate the often used terms $\sigma(x_1, x_2, x_3, x_4)$ and $\sigma(x_1, x_2, x_3)$ to $\sigma(x_i)$ and $\sigma'(x_i)$, respectively. Similar notation holds for S_3's and y_i's.

We simplify the third equation in the following manner:

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

With Newton's identity $S_3 = \sigma_1^3 + \sigma_1\sigma_2 + \sigma_3$ the fourth equation can be written in the form

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

All in all the considered support should satisfy

$$\begin{aligned} \sigma_1(x_i) &= \sigma_1(y_i) = 0 \\ \sigma_2'(x_i) &= \sigma_2'(y_i) \\ \sigma_3(x_i) &= \sigma_3(y_i). \end{aligned} \tag{3}$$

If the variables x_i and y_i are distinct, the corresponding codeword is of the desired type and rank. The item (iv) from Lemma 5 and the fact that the supports of Hamming weight 7 do not include any 2-flats imply easily that the only possible overlapping of the variables x_i and y_i satisfying (3) is the case where the 2-flats are equal and $x_4 = y_4$, that is, together they form the support $\{0, 1, a, a+1\}$ of cwe-type Y^4. So the solutions of (3) have one extra codeword which must be excluded.

A.3 Cases (0a) and (0b)

In the case (0a) we set $x_1 = 0$, $x_2 = 1$, and $x_3 = a$. By (3) 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 (3)

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

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

$$T^3 + \sigma T^2 + aT + a\sigma + a^2 + a. \tag{4}$$

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 polynomial (4) that has three distinct zeros corresponds exactly to the codeword that is counted in the case (0a).

Next we calculate the number of values of σ for which (4) has three distinct zeros. The derivative of this polynomial is $T^2 + a$ which has only one zero $\sqrt{a}$. This is the only candidate for a multiple zero but

$$\sqrt{a}^3 + \sigma a + a\sqrt{a} + a\sigma + a^2 + a = a^2 + a \neq 0.$$

and therefore (4) has distinct zeros in its splitting field.

We substitute $T = U + \sigma$ and the polynomial (4) transforms to $U^3 + (\sigma^2 + a)U + a^2 + a$. For $\sigma = \sqrt{a}$ the polynomial clearly has only one zero and we can ignore that case. We substitute now $U = (\sigma + \sqrt{a})V$ and divide by $(\sigma + \sqrt{a})^3$ and get

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

By Lemma 2 the above polynomial has three zeros for $(v - 2)/6$ values of σ. Our substitutions preserve the number of zeros and hence we can conclude that (4) has three distinct zeros for $(v - 2)/6$ values of σ.

The codeword of cwe-type Y^4 would have $\{y_1, y_2, y_3\} = \{0, 1, a\}$ and the corresponding polynomial would be $T^3 + (a+1)T^2 + aT$. This is clearly included in the above calculations and hence we have all in all $(v - 8)/6$ codewords in the case (0a) as claimed in Table 2.

The case (0b) can be proved almost along the same lines. We have $x_1 = 0$, $x_2 = 1$, $x_4 = a$, and $x_3 = a + 1$. Now $\sigma_3(x_i) = a^2 + a$ is the same as above but $\sigma_2'(x_i) = a + 1$ differs by 1. Therefore the polynomial comparable to (4) is

$$T^3 + \sigma T^2 + (a + 1)T + (a + 1)\sigma + a^2 + a$$

and the transforms are $U^3 + (\sigma^2 + a + 1)U + a^2 + a$ and

$$V^3 + V + \frac{a^2 + a}{(\sigma + \sqrt{a+1})^3}.$$

As above we can count that there are $(v-8)/6$ codewords in the case (0b).

A.4 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 the condition $\mathrm{Tr}(\sigma_2/\sigma_1^2) = 0$ must hold.

The extra codeword of cwe-type Y^4 in (3) 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 (3), 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 the same restriction also in the forthcoming subsections.

By (3) we know that $x_4 = x + 1$, $y_4 = a + \sigma_1$, $x = a\sigma_1 + \sigma_2$ and

$$x^2 + x = a\sigma_2 + a\sigma_1(a + \sigma_1) + \sigma_2(a + \sigma_1) = \sigma_1\sigma_2 + a^2\sigma_1 + a\sigma_1^2. \qquad (5)$$

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

$$\sigma_2^2 + (\sigma_1 + 1)\sigma_2 = (a^2 + a)\sigma_1(\sigma_1 + 1). \qquad (6)$$

As σ_2 is an element of $\mathbf{F}$, again by Lemma 1 the condition

$$\mathrm{Tr}\left(\frac{(a^2+a)\sigma_1}{\sigma_1 + 1}\right) = \mathrm{Tr}\left(\frac{(a^2+a)\sigma_1}{\sigma_1 + 1} + a^2 + a\right) = \mathrm{Tr}\left(\frac{a^2+a}{\sigma_1 + 1}\right) = 0 \qquad (7)$$

must hold. We simplified the condition using the well-known fact $\mathrm{Tr}(a^2 + a) = 0$.

By dividing (6) 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 (6). 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 other trace condition $\mathrm{Tr}((\sigma_2 + \sigma_1 + 1)/\sigma_1^2) = \mathrm{Tr}(\sigma_2/\sigma_1^2) = 0$ by the fact that $\mathrm{Tr}((a+1)/a^2) = 0$.

Clearly, $N_{0,0} = v - 4$. 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

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

As in (7) we drop z from the last numerator and substitute $u = z + 1$ and $w = (a^2 + a)u$.

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

since clearly $K(a^2) = K(a)$. By combining the above results we have

$$N_a = \frac{1}{4}\big(v - 7 + K(a^2 + a)\big).$$

The case (1b) goes almost as above. Now $y_4 = a$, $y_1 = \sigma_1 + a$, $x = \sigma_1^2 + a\sigma_1 + \sigma_2$, the equation (5) still holds, but instead of (6) we get

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

Therefore the task is to calculate the number

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

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 $N'_{0,0} = v - 4$. With the substitution $z = \sigma_1 + 1$ we have

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

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

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

Then $N'_a = (v - 11 - 3K(a^2+a))/4$ and the total number of codewords in the cases (1a) and (1b) together is

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

as claimed in Table 2.

A.5 Cases (2a) and (2b)

The situation in the case (2a) is the following: $x_1 = 0$, $x_4 = 1$, and $y_1 = a$. As in the previous subsection we denote $x = x_3$, $\sigma_1 = y_2 + y_3$, and $\sigma_2 = y_2 y_3$. We have by (3) that $x_2 = x + 1$, $y_4 = a + \sigma_1$, and (5) holds, but this time the equation for σ'_2 gives

$$x^2 + x = a\sigma_1 + \sigma_2. \tag{8}$$

By combining the above equation with (5) we get

$$\sigma_2 = \frac{\sigma_1(a\sigma_1 + a^2 + a)}{\sigma_1 + 1}.$$

Since the roots of (8) should be in $\mathbf{F}$ the variable σ_1 should satisfy

$$\mathrm{Tr}\left(a\sigma_1 + \frac{\sigma_1(a\sigma_1 + a^2 + a)}{\sigma_1 + 1}\right) = \mathrm{Tr}\left(\frac{a^2\sigma_1}{\sigma_1 + 1}\right) = \mathrm{Tr}\left(\frac{a^2}{\sigma_1 + 1} + a^2\right) = 0 \tag{9}$$

by Lemma 1. On the other hand σ_1 should also satisfy

$$\begin{aligned} \mathrm{Tr}\left(\frac{\sigma_2}{\sigma_1^2}\right) &= \mathrm{Tr}\left(\frac{a\sigma_1 + a^2 + a}{\sigma_1(\sigma_1 + 1)}\right) + \mathrm{Tr}\left(\frac{a^2\sigma_1}{\sigma_1 + 1}\right) \\ &= \mathrm{Tr}\left(\frac{(a^2 + a)(\sigma_1 + 1)}{\sigma_1(\sigma_1 + 1)} + \frac{a^2\sigma_1(\sigma_1 + 1)}{\sigma_1(\sigma_1 + 1)}\right) \\ &= \mathrm{Tr}\left(\frac{a^2 + a}{\sigma_1} + a^2\right) = 0. \end{aligned} \tag{10}$$

In the first line we added a term which is equal to zero by (9).

This time we are interested in the number

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

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 (5), but they correspond to the same codeword.

We count the number M_a with the same tricks as N_a and N'_a. Clearly $M_{0,0} = v - 4$ and

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

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

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

We conclude that

$$M_a = \frac{1}{4}\Big(v - 8 - 3(-1)^{\mathrm{Tr}(a)} + (-1)^{\mathrm{Tr}(a)} K\big(a^3(a+1)\big)\Big).$$

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

$$M_a + M_{a+1} = \frac{2v - 16 + (-1)^{\mathrm{Tr}(a)}\Big(K\big(a^3(a+1)\big) - K\big((a+1)^3 a\big)\Big)}{4} = \frac{v-8}{2}$$

by Theorem 1. This is exactly the frequency given in Table 2.

A.6 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 (3) we know that $x_2 = x + 1$, $y_1 = a + \sigma_1$, (5) holds, and

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

As in the previous cases we can solve

$$\sigma_2 = \frac{(a+1)\sigma_1(\sigma_1 + a)}{\sigma_1 + 1}$$

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

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

We claim that the number of solutions to these two trace equations is equal to M_{a+1}. If we substitute $a \mapsto a+1$ to the middle trace expression in (9), we get equation

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

and by the same substitution the middle term from (10) transforms to

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

and these two equations are exactly the same as the ones in the present case. 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 so 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

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

as claimed in Table 2. This concludes our proof for the main theorem.

B Proof of Corollary 1

As in the proof of the main theorem we can assume by Lemma 4 that our three coordinates are 0, 1, and $a \in \mathbf{F}^{**}$ and we prove that the number of supports of swe-type X^8 that include these positions does not depend on a.

Let us consider the consequences of Theorem 4. We fix the Gray map as follows: for $\mathbf{c} = (c_1, \ldots, c_v) \in \mathcal{G}$ and $\phi(c_i) = (c_{i0}, c_{i1})$ we set

$$\phi(\mathbf{c}) = (c_{00}, c_{10}, \ldots, c_{v0} \mid c_{01}, c_{11}, \ldots, c_{v1}) = (\mathbf{c}_L, \mathbf{c}_R).$$

For every coordinate 0, 1, and a of $\mathbf{c}$ we can choose the corresponding coordinate of $\phi(\mathbf{c})$ either from $\mathbf{c}_L$ or $\mathbf{c}_R$. These eight combinations of "binary" coordinates give sets of codewords which we can count.

Take for example all three coordinates from the left side. The codewords of $\phi(\mathcal{G})$ that include these positions are images of $\mathbf{Z}_4$-codewords that have either 1 or 2 in the positions 0, 1, and a. If some coordinate is taken from the right side then the corresponding $\mathbf{Z}_4$-codeword should have either 2 or 3 in this position. We illustrate half of the combinations in Table 3.

By Theorem 4 the codewords of the binary Goethals code $\phi(\mathcal{G})$ of Hamming weight 8 form a 3-design with $\lambda_b = (2v-4)(4v-17)/60$. These codewords correspond to the $\mathbf{Z}_4$-codewords of Lee weight 8. For every three "binary" coordinates the number of codewords $\phi(\mathbf{c})$ containing them is equal to λ_b. In the Table 3 we show all possible cwe-types of the corresponding $\mathbf{Z}_4$-codewords $\mathbf{c}$ and the number of them. The frequency column gives the number of codewords in ONE column. By multiplying the whole table by -1 we get the remaining four combinations.

The frequency in the case (a) comes directly from (i) in Theorem 2. The frequency in the case (b) can be seen as follows: by (iv) in Theorem 2 there are $(v-8)/6$ codewords of Hamming weight 6 in eBCH containing three fixed positions. Set 3's to those coordinates that require it and then in the remaining three positions we can choose from 4 combinations of 1's and 3's. Every such codeword can be lifted uniquely to a codeword of swe-type X^6Y in $\mathcal{G}$ and therefore we have $4(v-8)/6$ codewords in the case (b).

Table 3: 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	$\frac{2(v-8)}{3}$
(c)	211 1111 211 1133 211 3333	213 1113 213 1333	231 1113 231 1333	211 1111 211 1133 211 3333	$\frac{v-8}{3}$
(c)	121 1111 121 1133 121 3333	123 1113 123 1333	121 1111 121 1133 121 3333	321 1113 321 1333	$\frac{v-8}{3}$
(c)	112 1111 112 1133 112 3333	112 1111 112 1133 112 3333	132 1113 132 1333	312 1113 312 1333	$\frac{v-8}{3}$
(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

The frequency in the case (c) can be found from Table 1. Hence we conclude that the codewords in the case (d) in all combinations, that is, the codewords of swe-type X^8, form a 3-design with repeated blocks and

$$\lambda' = 8? = 8\left(\frac{(2v-4)(4v-17)}{60} - \frac{5(v-8)}{3} - 1\right) = \frac{4(4v^2-75v+404)}{15}. \tag{11}$$

We know that there are repeated blocks by Lemma 6, but we can exclude them and make the design simple. This follows from the fact that the codewords of rank 1 and the codewords of rank 3 both form simple 3-designs and we can count them. For every codeword **c** of swe-type X^8 there is a codeword $-\mathbf{c}$ with the same support and it can be dropped out. By Lemma 6 this settles the supports of rank 0. For every codeword of rank 3 there are still 7 extra words and for codewords of rank 1 there is one extra codeword with the same support and therefore the simple design has

$$\begin{aligned}\lambda = \frac{1}{2}\lambda' - 7\lambda_3 - \lambda_1 &= \frac{2(4v^2-75v+404)}{15} - \frac{7(v-4)}{4} - \frac{14(v-8)}{3} \\ &= \frac{32v^2-985v+5892}{60}.\end{aligned}$$

Acknowledgment

This paper and the proof of the main theorem were inspired by the article by Shin, Kumar, and Helleseth [11]. Thanks are also due to J. Lahtonen for several useful discussions.

References

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

[2] L. A. Bassalygo and V. A. Zinoviev, *Remark on uniformly packed codes*, Problems Inform. Transmiss. **13** (1977), no. 3, 22–25.

[3] E. R. Berlekamp, H. Rumsey, and G. Solomon, *On the solution of algebraic equations over finite fields*, Information and Control **10** (1967), no. 6, 553–564.

[4] A. Bonnecaze, E. Rains, and P. Solé, *3-colored 5-designs and Z_4-codes*, Research report no. 4, Royal Melbourne Institute of Technology, April 1998.

[5] Iwan Duursma, Tor Helleseth, Chunming Rong, and Kyeongcheol Yang, *Split weight enumerators for the Preparata codes with applications to designs*, Designs, Codes and Cryptography **18** (1999), 103–124.

[6] A. Roger Hammons, Jr., P. Vijay Kumar, A. R. Calderbank, N. J. A. Sloane, and Patrick Solé, *The $\mathbb{Z}_4$-linearity of Kerdock, Preparata, Goethals, and related codes*, IEEE Trans. Inform. Theory **40** (1994), no. 2, 301–319.

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

[8] Tor Helleseth and P. Vijay Kumar, *The algebraic decoding of the Z_4-linear Goethals code*, IEEE Trans. Inform. Theory **41** (1995), no. 6, 2040–2048.

[9] Tor Helleseth, P. Vijay Kumar, and Kyeongcheol Yang, *An infinite family of 3-designs from Preparata codes over Z_4*, Designs, Codes and Cryptography **15** (1998), 175–181.

[10] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error–Correcting Codes*, North–Holland Mathematical Library, vol. 16, North–Holland, Amsterdam, 1977.

[11] Dong-Joon Shin, P. Vijay Kumar, and Tor Helleseth, *3-designs from the Z_4-Goethals codes via a new Kloosterman sum identity*, submitted to Designs, Codes and Cryptography.

[12] ______, *5-designs from the lifted Golay code over Z_4 via an Assmus-Mattson type approach*, to appear in Discrete Mathematics.

[13] ______, *An Assmus-Mattson-type approach for identifying 3-designs from linear codes over Z_4*, submitted to Designs, Codes and Cryptography.

[14] Kenichiro Tanabe, *An Assmus-Mattson theorem for $\mathbf{Z}_4$-codes*, IEEE Trans. Inform. Theory **46** (2000), no. 1, 48–53.

Turku Centre for Computer Science
Lemminkäisenkatu 14
FIN-20520 Turku
Finland

http://www.tucs.fi

University of Turku
- **Department of Mathematical Sciences**

Åbo Akademi University
- **Department of Computer Science**
- **Institute for Advanced Management Systems Research**

Turku School of Economics and Business Administration
- **Institute of Information Systems Science**