Symmetric Designs and Self-Dual Codes over Rings

Steven T. Dougherty
Department of Mathematics
University of Scranton
Scranton, PA 18510, USA

T. Aaron Gulliver
Department of Electrical and Computer Engineering
University of Victoria
Victoria, BC V8W 3P6, Canada

and

Reshma Ramadurai *
Department of Mathematics
University of Illinois at Chicago
Chicago, IL 60607, USA

July 25, 2007

Abstract

We describe a technique for producing self-dual codes over rings and fields from symmetric designs. We give special attention to biplanes and determine the minimum weights of the codes formed from these designs. We give numerous examples of self-dual codes constructed including an optimal code of length 22 over $\mathbb{Z}_4$ with respect to the Hamming metric from the biplane of order 3.

*The author is grateful for the hospitality of the University of Scranton where she stayed while this paper was written.

1 Introduction

Numerous constructions of self-dual codes over fields from designs exist. However, these constructions do not generally apply to codes over rings. This is because usually the construction requires that a prime p sharply divides the order to make the code formed from the design the right dimension to make a self-dual code. There do exist constructions of self-dual codes over rings from symmetric designs, see [8], where self-dual codes over $\mathbb{Z}_4$ are constructed but again in that construction 4 sharply divides the order of the symmetric design. In this work we shall give a construction of self-dual codes over rings, specifically the ring $\mathbb{Z}_m$. It will not require m to sharply divide the order of the design. The construction was inspired by a construction given by Glynn [6] in which he produced binary self-dual codes from projective planes of odd order. The construction by Glynn requires the codes to be binary. In [4], his construction was generalized to any projective plane and for codes over non-binary fields. However, all of these constructions were only for codes over fields. In this work the construction is generalized to any symmetric design and is extended to codes over rings. We begin with the necessary definitions of designs and codes.

1.1 Symmetric Designs

A $t-(v,k,\lambda)$ design is a set of v points, with blocks of size k such that through any t points there are λ blocks. Let D be a $2-(v,k,\lambda)$ symmetric design. We know by definition that the number of points is equal to the number of blocks. The number of points on a block is $n+\lambda$ and the number of blocks through a point is $n+\lambda$. Let L be a block, through each point there are $(n+\lambda-1)$ blocks other than L. In this count each block is counted λ times. A symmetric design with $\lambda=1$ is a projective plane and a symmetric design with $\lambda=2$ is a biplane. Hence in a symmetric design we have $v=\frac{(n+\lambda-1)(n+\lambda)}{\lambda}+1$ and $k=n+\lambda$ where n is the order of the design.

Let $D=(\mathcal{P},\mathcal{B},\mathcal{I})$ be a (v,k,λ) symmetric design. If $\mathcal{B}'=\{b' \mid b'$ is the complement of a block in $\mathcal{B}\}$ then $D^c=(\mathcal{P},\mathcal{B}',\mathcal{I})$ is a $(v,v-k,b-2r-\lambda)$ symmetric design, where b is the size of the blocks. We refer to this design as the complementary design.

1.2 Codes

A code of length N over the ring $\mathbb{Z}_m$ is a subset of $\mathbb{Z}_m^N$. If the code is a submodule then we say that the code is linear. We attach the usual innerproduct to the space, i.e. $[v, w] = \sum v_i w_i$ and $C^\perp = \{v \mid [v, w] = 0\}$ for all $w \in C$. The code $C^\perp$ is linear and we have $|C||C^\perp| = m^N$. If a code C has $C \subseteq C^\perp$ then C is said to be a self-orthogonal code. If $C = C^\perp$ then C is said to be a self-dual code. Two codes are said to be equivalent if one can be obtained from the other by permuting the rows or multiplying a column by a unit.

A code over $\mathbb{Z}_m$ has a generator matrix that is equivalent to a matrix of the following form

$$\begin{pmatrix} a_1 I_{k_1} & A_{1,2} & A_{1,3} & A_{1,4} & \cdots & \cdots & A_{1,s+1} \\ 0 & a_2 I_{k_2} & a_2 A_{2,3} & a_2 A_{2,4} & \cdots & \cdots & a_2 A_{2,s+1} \\ 0 & 0 & a_3 I_{k_3} & a_3 A_{3,4} & \cdots & \cdots & a_3 A_{3,s+1} \\ \vdots & \vdots & 0 & \ddots & \ddots & & \vdots \\ \vdots & \vdots & \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 0 & a_s I_{k_s} & a_s A_{s,s+1} \end{pmatrix}, \tag{1}$$

where $A_{i,j}$ are binary matrices for $i > 1$. It can be arranged so that $a_1 = 1$ and $a_i < a_j$ and a_i divides m for all i. A code of this form is said to be of *type* $\{1^{k_1}, a_2^{k_2}, a_3^{k_3}, \ldots, a_s^{k_s}\}$ and has $\prod_{i=1}^{s} (\frac{m}{a_i})^{k_i}$ elements.

The Hamming weight of a vector is the number of non-zero coordinates in the vector and the minimum Hamming weight of a code is the smallest of all non-zero weights in the code. The Hamming weight enumerator of a code C is defined by $W_C(x, y) = \sum_{c \in C} y^{wt(c)}$ where $wt(c)$ is the Hamming weight of the vector c.

2 Construction of self-dual codes

Throughout this section we assume that m is an integer dividing $n + 1$ where n is the order of the design.

Let D be a symmetric $2-(v, k, \lambda)$ design with $\mathcal{P}$ the points set and $\mathcal{B}$ the blocks set. We denote the points by $\mathcal{P} = \{q_1, q_2, \ldots, q_{|\mathcal{P}|}\}$ and the blocks by $\mathcal{B} = \{\ell_1, \ell_2, \ldots, \ell_{|\mathcal{P}|}\}$. The ambient space for the codes we consider is $\mathbb{Z}_m^{\mathcal{P} \cup \mathcal{B}}$.

For a point q let χ_q be the vector that is 1 at the coordinate corresponding to q and 0 elsewhere. We let ψ_q be the vector that is 1 at the coordinate corresponding to ℓ if q is incident with ℓ and 0 elsewhere.

We define

$$\Delta(q_i, q_j) = (\chi_i - \chi_j, \psi_i - \psi_j). \tag{2}$$

The weight of $\Delta(q_i, q_j)$ is $2n + 2$ where n is the order of the design.

Lemma 2.1 *For a symmetric design D of order n and m dividing $n + 1$*

$$[\Delta(q_i, q_j), \Delta(q_{i'}, q_{j'})] = 0. \tag{3}$$

Proof. It is enough to consider the following three cases.

Case 1: If the q_i are 4 distinct points then the supports of the $\chi(q_i)$ are distinct. Then

$$\begin{aligned}[(\psi_{q_i} - \psi_{q_j}), (\psi_{q_{i'}} - \psi_{q_{j'}})] &= [\psi_{q_i}, \psi_{q_{i'}}] - [\psi_{q_i}, \psi_{q_{j'}}] - [\psi_{q_j}, \psi_{q_{i'}}] + [\psi_{q_j}, \psi_{q_{j'}}] \\ &= \lambda - \lambda - \lambda + \lambda = 0.\end{aligned}$$

Case 2: If $q_i = q_{i'}$ and $q_j \neq q_{j'}$ then

$$[(\chi_{q_i} - \chi_{q_j}), (\chi_{q_{i'}} - \chi_{q_{j'}})] = 1, \tag{4}$$

since the support of $\chi(q_i)$ is the support of $\chi(q_{i'})$ and the others are disjoint. Then

$$\begin{aligned}[(\psi_{q_i} - \psi_{q_j}), (\psi_{q_{i'}} - \psi_{q_{j'}})] &= [\psi_{q_i}, \psi_{q_i}] - [\psi_{q_i}, \psi_{q_{j'}}] - [\psi_{q_j}, \psi_{q_i}] + [\psi_{q_j}, \psi_{q_{j'}}] \\ &= (n + \lambda) - \lambda - \lambda + \lambda = n.\end{aligned}$$

This gives that

$$[((\chi_{q_i} - \chi_{q_j}), (\psi_{q_i} - \psi_{q_j})), ((\chi_{q_{i'}} - \chi_{q_{j'}}), (\psi_{q_{i'}} - \psi_{q_{j'}}))] = 1 + n = 0. \tag{5}$$

Case 3: If $q_i = q_{j'}$ and $q_j \neq q_{i'}$ then in an argument similar to Case 2 we get

$$[((\chi_{q_i} - \chi_{q_j}), (\psi_{q_i} - \psi_{q_j})), ((\chi_{q_{i'}} - \chi_{q_{j'}}), (\psi_{q_{i'}} - \psi_{q_{j'}}))] = -(1 + n) = 0. \tag{6}$$

□

Next we construct a self-orthogonal code. Let

$$C_m(D) = \langle \Delta(q_i, q_j) \mid q_i, q_j \in \mathcal{P} \rangle. \tag{7}$$

We shall construct self-dual codes from this code in a variety of ways depending on the structure of $\mathbb{Z}_m$. Let M be the $|\mathcal{P}|-1$ by $2|\mathcal{P}|$ matrix where the i-th row of M is $\Delta(q_1, q_{i+1})$. It is clear that the rows of M are orthogonal over $\mathbb{Z}_m$ and that M generates $C_m(D)$. Further, it is apparent from the structure of M that the type of $C_m(D)$ is $1^{|\mathcal{P}|-1}$. We summarize these results in the following.

Lemma 2.2 *Let D be a symmetric design of order n with m an integer dividing $n+1$, then $C_m(D)$ is a self-orthogonal, linear code with $m^{|\mathcal{P}|-1}$ elements.*

Let P be the vector that is 1 on the coordinates corresponding to the points and 0 on the coordinates corresponding to the blocks and let L be the vector that is 0 on the coordinates corresponding to the points and 1 on the coordinates corresponding to the blocks. We note that $P \in C_m(D)^{\perp}$ since $[\Delta(q_i, q_j)], P] = 1-1 = 0$ and $L \in C_m(D)^{\perp}$ since $[\Delta(q_i, q_j), L] = n-n = 0$. To make $\alpha P + \beta L$ self-orthogonal we need $[\alpha P + \beta L, \alpha P + \beta L] = 0$ which means that $(\alpha^2 + \beta^2)|\mathcal{P}| = 0$. If $|\mathcal{P}| \not\equiv 0 \pmod{m}$, this means that $\alpha^2 = -\beta^2$ so that the ring must have $\sqrt{-1}$.

If the ring $\mathbb{Z}_m$ has $\sqrt{-1}$, and m does not divide v then let

$$E_m(D) = \langle C_m(D), P + \sqrt{-1}L \rangle. \tag{8}$$

The reason that we cannot use this description of $E_m(D)$ when m divides v and $\lambda - 1$ is the square root of -1, is that the vector will already be in $C_m(D)$. This will be explained in the following.

In a symmetric design we have

$$\begin{aligned} \sum_{i=2}^{v} \Delta(q_1, q_i) &= \sum_{i=2}^{v}((\chi_{q_i} - \chi_{q_j}), (\psi_{q_i} - \psi_{q_j})) \\ &= (v-1, -1, -1, \ldots, -1, \alpha(1), \alpha(2), \ldots, \alpha(v)), \end{aligned}$$

where

$$\alpha(i) = \begin{cases} -n-\lambda & \text{if } \ell_i \text{ is not incident with } q_1 \\ v-n-\lambda & \text{if } \ell_i \text{ is incident with } q_1 \end{cases}.$$

Lemma 2.3 *If m divides v then* $(-1, -1, \ldots, -1, -n-\lambda, -n-\lambda, \ldots, -n-\lambda) \in C_m(D)$.

Proof. By the previous computation when m divides v we have

$$\sum_{i=2}^{v} \Delta(q_1, q_i) = (-1, -1, \dots, -1, -n - \lambda, -n - \lambda, \dots, -n - \lambda).$$

□

Multiplying the above vector by -1 we have $(1, 1, \dots, 1, n + \lambda, n + \lambda, \dots, n + \lambda)$. Now $(n + \lambda)^2 = (\lambda - 1)^2$.

Lemma 2.4 *If m divides v and $(\lambda - 1) = \sqrt{-1}$ then $P + \sqrt{-1}L \in C_m(D)$.*

Proof. Follows from the previous discussion. □

In this case we can define

$$E'_m(D) = \langle C_m(D), P + L \rangle. \tag{9}$$

We know that $P + L$ is in $C_m(D)^\perp$. Then $[P + L, P + L] = 2v = 0$, and this gives the following.

Theorem 2.5 *Let D be a symmetric design of order n with m an integer dividing $n+1$. If m does not divide v or $(\lambda - 1)$ is not $\sqrt{-1}$ and $\sqrt{-1} \in \mathbb{Z}_m$ then $E_m(D)$ is a self-dual code over $\mathbb{Z}_m$ of length $2|\mathcal{P}|$. If m does divide v and $(\lambda - 1) = \sqrt{-1}$ then $E'_m(D)$ is a self-dual code over $\mathbb{Z}_m$ of length $2|\mathcal{P}|$.*

Proof. The code is self-orthogonal by construction and its cardinality is $m|C_m(D)| = m^{|\mathcal{P}|}$. □

Corollary 2.6 *Let D be a symmetric design of order n with p a prime dividing $n + 1$. If $p \equiv 1 \pmod 4$ then $E_m(D)$ is a self-dual code over $\mathbb{F}_p$.*

Proof. It is well known that $\mathbb{F}_p$ contains a $\sqrt{-1}$ if and only if $p \equiv 1 \pmod 4$ and $|\mathcal{P}| = n^2 + n + 1 \equiv 1 \not\equiv 0 \pmod m$. Then the result follows from the previous theorem. □

Next we shall consider a construction of self-dual codes when the ring does not necessarily have $\sqrt{-1}$ but is a square.

If $m = q^2$ take $F_m(D) = \langle C_m(D), qP, qL \rangle$.

Theorem 2.7 *Let D be a symmetric design of order n with $m = q^2$ and integer dividing $n+1$. The code $F_m(D)$ is a self-dual code over $\mathbb{Z}_m$ of length* $2|\mathcal{P}|$.

Proof. We have that $[qP, qP] = q^2 = 0$ and $[qL, qL] = q^2 = 0$. Then we have that $|F_m(D)| = q(q(|C_m(D))) = m|C_m(D)| = m^{|\mathcal{P}|}$, so $F_m(D)$ is a self-dual code. □

In the case where $\mathbb{Z}_m$ does not contain a $\sqrt{-1}$ and m is not a square we can proceed as follows. We shall construct a self-dual code in this case of length $2v + 2$. To each vector in $C_{i,j} = (C_m(D) + iP + jL)$ adjoin a vector of length 2, $w_{i,j}$. For linearity we need $w_{i,j} = iw_{1,0} + jw_{0,1}$. To make this new code self-dual we need these new vectors to satisfy the following: $[w_{i,j}, w_{i'j'}] = -[C_{i,j}, C_{i',j'}]$. Hence we need to find $w_{1,0}$ and $w_{0,1}$ such that

$$(10) \qquad [w_{1,0}, w_{1,0}] = [w_{0,1}, w_{0,1}] = -v,$$

since $[P, P] = [L, L] = v$, and

$$(11) \qquad [w_{1,0}, w_{0,1}] = 0,$$

since $[P, L] = 0$.

If there exist α, β with $\alpha^2 + \beta^2 = -v$, let $w_{1,0} = (\alpha, \beta)$ and $w_{0,1} = (-\beta, \alpha)$. These vectors satisfy (10) and (11). Then define

$$(12) \qquad G_m(D) = \cup_{i,j}(C_{i,j}, w_{i,j}).$$

The length of this code is $2v + 2$ and has dimension $\frac{2v+2}{2}$. This gives the following theorem.

Theorem 2.8 *Let D be a symmetric design of order n with q a prime dividing $n + 1$ with $\alpha^2 + \beta^2 = v$ in $\mathbb{F}_q$. Then $G_m(D)$ is a self-dual code of length $2v + 2$.*

If $\mathbb{Z}_m$ has $\alpha = \sqrt{-v - 1}$ then we proceed as follows. Let $w_{1,0} = (\alpha, 1)$ and $w_{0,1} = (1, -\alpha)$. These vectors satisfy (10) and (11). Then define

$$(13) \qquad H_m(D) = \cup_{i,j}(C_{i,j}, w_{i,j}).$$

The length of this code is $2v+2$ and has $|H_m(D)| = m^2 C_m(D) = m^2(m^{v-1}) = m^{v+1}$, so the code is self-dual. This gives the following.

Theorem 2.9 *Let D be a symmetric design of order n with m dividing $n+1$ where $\mathbb{Z}_m$ contains $\sqrt{-v-1}$. Then $H_m(D)$ is a self-dual code of length $2v+2$.*

In [4], the minimum weights of the codes formed from projective planes were given. These result have a natural generalization to the ring $\mathbb{Z}_m$. The proof is a straightforward generalization, but lengthy, and so we omit the proof of the following.

Theorem 2.10 *Let Π be a projective plane of order n, then the minimum weight of $C_m(D)$ is $2n+2$, the minimum weight of $E_m(D)$ is $2n$ if $m=2$ and $2n+2$ otherwise, and the minimum weight of $G_m(D)$ and $H_m(D)$ is $n+4$.*

3 Minimum Weights

We shall provide some new definitions of vectors which are needed to determine the minimum weights of the codes. For a given block ℓ in $\mathcal{L}$, let η_ℓ be the vector of length v that has a 1 at the coordinate corresponding to ℓ and a 0 elsewhere. Let μ_ℓ be the vector of length v with a 1 at the coordinate for a point p if ℓ is incident with p and a 0 elsewhere. These are similar to χ and λ but their roles are reversed. We shall show that we could also have generated the codes using these vectors. The reason for our choice of vectors is so that they can be used in the proofs to determine some of the minimum weights of the self-dual codes constructed.

Define

$$\Gamma(\ell_1,\ell_2) = (\mu_{\ell_1} - \mu_{\ell_2}, \eta_{\ell_2} - \eta_{\ell_1}). \tag{14}$$

Notice that the order is reversed in the second part. Let ℓ_1 and ℓ_2 be two blocks in the design with $\{q_1,q_2,\dots,q_n\}$ the points on ℓ_1 not on ℓ_2 and $\{q_1',q_2',\dots,q_n'\}$ the points on ℓ_2 not on ℓ_1. It is easy to see that $\sum_{i=1}^n(\chi_{q_i} - \chi_{q_i'}) = \mu_{\ell_1} - \mu_{\ell_2}$ on the first v coordinates. On the second v coordinates consider $\sum_{i=1}^n(\lambda_{q_i} - \lambda_{q_i'})$. For the coordinate corresponding to ℓ_1, the vector λ_{q_i} is 1 and the vector $\lambda_{p_i'}$ is 0. In the sum there is an n which is -1. On the coordinate for ℓ_2 there a 1 for each $\lambda_{q_i'}$ and a 0 for each λ_{q_i}. In the sum there is a $-n$ which is 1, since p divides $n+1$. On any other block there are two coordinates with a 1 and two with a -1 since any block intersects ℓ_1 and ℓ_2 exactly twice. Thus on the second set of coordinates the vector is $\eta_{\ell_2} - \eta_{\ell_1}$. This gives

$$(15) \qquad \sum_{i=1}^{n} \Delta(q_i, q_i') = \Gamma(\ell_1, \ell_2),$$

where the points incident with ℓ_1 and not incident with ℓ_2 are $\{q_1, q_2, \ldots, q_n\}$ and the points incident with ℓ_2 and not incident with ℓ_1 are $\{q_1', q_2', \ldots, q_n'\}$.

It is a simple matter to see the following.

Theorem 3.1 *The code $C_m(D) = \langle \Delta(\ell_1, \ell_2) \mid \ell_1, \ell_2 \in \mathcal{L} \rangle$.*

Lemma 3.2 *Let D be a symmetric design of order n. Vectors of the form (χ_p, λ_p) are in $C_m(D)^{\perp}$ and vectors of the form $(\mu_\ell, -\eta_\ell)$ are in $C_m(D)^{\perp}$.*

Proof. We shall show this vector is orthogonal to each generator. If $q \neq q'$ then

$$(16) \qquad [(\chi_q, \lambda_q), (\chi_q - \chi_{q'}, \lambda_q - \lambda_{q'})] = 1 + n = 0.$$

If $q \neq q_1, q_2$ then

$$(17) \qquad [(\chi_q, \lambda_q), (\chi_{q_1} - \chi_{q_2}, \lambda_{q_1} - \lambda_{q_2})] = 0 + 2 - 2 = 0.$$

The second computation is similar. For any block $\ell \in L$, we have

$$(18) \qquad [(\mu_\ell, -\eta_\ell), (\mu_{\ell_1} - \mu_{\ell_2}, \eta_{\ell_2} - \eta_{\ell_1})] = \lambda - \lambda = 0,$$

if $\ell \neq \ell_1, \ell_2$,

$$(19) \qquad [(\mu_\ell, -\eta_\ell), (\mu_{\ell_1} - \mu_{\ell_2}, \eta_{\ell_2} - \eta_{\ell_1})] = n + 1 = 0,$$

if $\ell = \ell_1$, and

$$(20) \qquad [(\mu_\ell, -\eta_\ell), (\mu_{\ell_1} - \mu_{\ell_2}, \eta_{\ell_2} - \eta_{\ell_1})] = -n - 1 = 0,$$

if $\ell = \ell_2$. □

Lemma 3.3 *If $w \in C_m(D)$ and ℓ is tangent to $Supp_{\mathcal{P}}(w)$ then $w_\ell \neq 0$.*

Proof. We know $(\mu_\ell, -\eta_\ell) \in C_m(\Pi)^{\perp}$. Thus

$$[(\mu_\ell, -\eta_\ell), w] = 1 - w_\ell = 0,$$

and then $w_\ell = 1$. □

3.1 Minimum Weights for Codes from Biplanes

We shall use these results to find the minimum weights of codes formed from biplanes. Throughout this section Π is a biplane of order n.

We shall now find the codes $C_m(\Pi), G_m(\Pi)$ and $H_m(\Pi)$ and $C_m(\Pi)^\perp$ when Π is a biplane.

Theorem 3.4 *For $n > 2$ the minimum weight of $C_m(\Pi)$ is at least $n+5$.*

Proof. Let $w \in C_m(\Pi)$ and assume $wt(w) < n+5$. Without loss of generality assume $a = |Supp(w)| \leq \frac{n}{2}+2$. It is easy to see that we can take $a > 1$. By Lemma 3.3 we know that $w_\ell \neq 0$ if ℓ is tangent to $Supp_{\mathcal{P}}(w)$. Through any point in $Supp_{\mathcal{P}}(w)$ there are at least $n+4-2a$ tangents so

$$wt(w) \geq a(n+4-2a)+a, \tag{21}$$

which implies $a(n+5-2a) \leq n+4$, which for all $a > 1$ and $n > 2$ is a contradiction.

For $n = 2$ the generators have weight $2n+2 = 6 < 2+5$, so the theorem does not apply. For $n = 1$ the generators have weight $4 < 5$, so the theorem does not apply. □

Lemma 3.5 *Given a set containing a points with $0 \leq a \leq n+2$, the maximum number of lines in a biplane that can meet these points is $a(n+2-a)+\frac{a(a-1)}{2}+1$.*

Proof. The maximum occurs when the points are collinear. In this case there are $a(n+2-a)$ tangents and $(a-1)+(a-2)+\ldots+2+1$ secants. Then the number of lines meeting these points is

$$\begin{aligned} 1+a(n+2-a)+1 &+ (a-1)+(a-2)+\ldots+1 \\ &= a(n+2-a)+1+(a-1)a-\frac{a(a-1)}{2} \\ &= a(n+2-a)+\frac{a(a-1)}{2}+1. \end{aligned}$$

□

Theorem 3.6 *The minimum weight of $C_m(\Pi)^\perp$ is $n+3$.*

Proof. We note that $(\chi_p, \lambda_p) \in C_m(\Pi)^\perp$ and this vector has weight $n+3$. Hence the minimum weight is at most $n+3$. Assume $w \in C_m(\Pi)^\perp$ with $wt(w) \leq n+2$. Without loss of generality we can assume $|Supp_{\mathcal{P}}(w)| \leq \frac{n+2}{2}$. If ℓ and ℓ' are exterior to $Supp_{\mathcal{P}}(w)$ then $[w, (\mu_\ell - \mu_{\ell'}, \eta_{\ell'} - \eta_\ell)] = 0$ which implies that $[w, \eta_\ell] = [w, \eta_{\ell'}] = 0$. If m and m' are tangent to $Supp_{\mathcal{P}}(w)$ then $[w, (\mu_m - \mu_{m'}, \eta_{m'} - \eta_m)] = 0$ which implies that $[w, \eta_m] = [w, \eta_{m'}] = 0$. Hence w has the same innerproduct for all η_ℓ exterior lines ℓ and the same innerproduct with η_m for all tangent lines m.

Since $|Supp_{\mathcal{P}}(w)| \leq \frac{n+2}{2}$, we know that there must be lines exterior by using Lemma 3.5, and that there must be tangent lines as well. Let m be a tangent block and ℓ be an exterior block for $Supp_{\mathcal{P}}(w)$. Then we have

$$\begin{aligned}
[w, (\mu_\ell - \mu_m, \eta_m - \eta_\ell)] &= 0 \\
[w, \mu_\ell] - [w, \mu_m] + [w, \eta_m] - [w, \eta_\ell] &= 0 \\
-1 + [w, \eta_m] - [w, \eta_\ell] &= 0 \\
[w, \eta_m] - [w, \eta_\ell] &= 1.
\end{aligned}$$

This gives that w has non-zero innerproduct with η_ℓ all tangent lines or all exterior lines. In either case, this implies that w must be non-zero on the coordinate corresponding to ℓ.

If it is the exterior lines that have non-zero innerproduct then

$$\begin{aligned}
wt(w) &\geq a + v - (a(n+2-a) + \frac{a(a-1)}{2} + 1) \\
&\geq a + \frac{n^2+3n+2}{2} - a(n+2-a) - \frac{a(a-1)}{2}.
\end{aligned}$$

Then we have

$$\begin{aligned}
n+3 &> a + \frac{n^2+3n+2}{2} - a(n+2-a) - \frac{a(a-1)}{2} \\
0 &> a + \frac{n^2}{2} + \frac{n}{2} - 2 - an - 2a + a^2 - \frac{a(a-1)}{2} \\
0 &> \frac{n^2}{2} + (\frac{1}{2} - a)n + (a - 2 - 2a + a^2 - \frac{a(a-1)}{2} \\
0 &> \frac{n^2}{2} + (\frac{1}{2} - a)n + (\frac{a^2}{2} - \frac{a}{2} - 2) \\
0 &> n^2 + (1-a)n + (a^2 - a - 4)
\end{aligned}$$

which is a contradiction for all a with $0 \leq a < n+3$.

If it is the tangent lines that have non-zero innerproduct, then the proof in Theorem 3.4 shows the weight must be at least $n+5$. Hence the minimum weight of $C_m(\Pi)^\perp$ is $n+3$. □

We note that there are codes which exceed this bound as given in the next section.

Theorem 3.7 *If Π is a biplane of order n with p a prime dividing n, then the minimum weight of $G_m(D)$ and $H_m(\Pi)$ is $n+5$.*

Proof. We have that

$$Q = \cup(C_{\alpha,\beta}, w_{\alpha,\beta}),$$

and $wt(w_{\alpha,\beta}) = 2$ if α and β are not both 0. Also we know the minimum weight of $C_{0,0} = C_m(\Pi)$ is $n+5$ and the minimum weight of $C_{\alpha,\beta} \geq n+3$. It is known that there are vectors of weight $n+3$ in some $C_{\alpha,\beta}$. Hence the minimum weight is $n+5$. □

4 Self-dual codes constructed from symmetric designs

4.1 Biplane Computations

- For the biplane of order 1, the code $E_2(\Pi)$ is the $[8,4,4]$ Hamming code.

- For the biplane of order 2, the code $G_3(\Pi)$ is an optimal $[16,8,6]$ ternary self-dual code.

- The code $E_2(\Pi)$ is the optimal $[22,11,6]$ baby Golay code.

- There are three biplanes of order 4.

  For all three $E_5(\Pi)$ is a self-dual $[32,16,8]$ code over $\mathbb{F}_5$.

- There are three biplanes of order 7.

  For all three, $E_2(\Pi)$ is a $[74,37,10]$ Type I code.

- There are five biplanes of order 9.

  For all five, $E_2(\Pi)$ is a $[112, 56, \geq 12]$ Type I code, and $E_5(\Pi)$ is a $[112, 56, \geq 12]$ self-dual code over $\mathbb{F}_5$.

- There is one known biplane of order 11.

  The code $E_2(\Pi)$ is a $[158, 79, \geq 14]$ Type I code, and the code $G_3(\Pi)$ is a $[160, 80, 14]$ ternary self-dual code. The codes $E_4(\Pi)$ and $E_6(\Pi)$ are length 158 self-dual codes with minimum weight at least 14.

4.2 Symmetric Designs

The following lemma will reduce the number of cases we must consider.

Lemma 4.1 *If there exists a symmetric design of order n then λ divides $n(n-1)$.*

Proof. The number of points is $\frac{(n+\lambda-1)(n+\lambda)}{\lambda}+1$. If this number is an integer then $(n+\lambda-1)(n+\lambda)$ must be divisible by λ. Taking $(n+\lambda-1)(n+\lambda)$ (mod λ) gives $n(n-1)$. □

Lemma 4.2 *If D and D' are complimentary designs then $C_m(D)$ and $C_m(D')$ are equivalent codes.*

Proof. Consider the generator matrix of $C_m(D)$. Multiplying the columns corresponding to the blocks by -1 produces the generator matrix of $C_m(D')$. Hence the codes are equivalent. □

This means that we only need to consider one of the designs, as the code formed from the other is equivalent.

4.3 Symmetric designs of order 1

We know that there exists a $2-(v, \lambda+1, \lambda)$ design for all $\lambda \geq 1$. Specifically, take $\lambda+2$ points and let the blocks be any possible $\lambda+1$ subset. Then any two blocks meet in λ places. Let D_λ be this design of order 1. Moreover, this represents all symmetric designs of order 1, since a symmetric design of order 1 must have $\lambda+2$ points and block size $\lambda+1$. We have that 2 is the only integer greater than 1 that divides the $n+1$.

The following is easy to see.

Proposition 4.3 *The code $E_2(D_\lambda)$ is a $[2\lambda+4, \lambda+2, 4]$ self-dual binary code, for $\lambda > 1$. If $\lambda = 1$ then $E_2(D_1)$ is a $[6,3,2]$ self-dual code. If $2|\mathcal{P}| \equiv 0 \pmod 4$ then $F_2(D)$ is a Type II code.*

Proof. The fact that the code is Type II when $2|\mathcal{P}| \equiv 0 \pmod 4$ follows from the fact that each of the generators has weight congruent to $0 \pmod 4$. □

Proposition 4.4 *The code $E_2(D_\lambda) = E_2(D_\lambda^c)$ for all λ.*

Proof. Let Δ^c be Δ defined on the complementary design. Then $\Delta(q_i, q_j) = \Delta^c(q_i, q_j)$, which gives the result. □

4.4 Symmetric designs of order 2

The only possible symmetric designs of order 2 have $\lambda = 1$ or 2. That is the unique projective plane of order 2, and the unique biplane of order 2 which is the complement of the projective plane of order 2. The only integer that divides $n+1$ is 3. The result for the plane is given in [4], and the result for the biplane is given in the previous section.

- If D is the projective plane of order 2 then $E_3(D)$ is the optimal $[16,8,6]$ ternary self-dual code.
- If D is the biplane of order 2 then $E_3(D)$ is the $[16,8,6]$ ternary self-dual code as above.

4.5 Symmetric designs of order 3

For $n = 3$, the possible λ are $1, 2, 3, 6$. These correspond to the projective plane of order 3, the biplane of order 3 and their complements. Here both 2 and 4 divide $n+1$.

- If D is the projective plane of order 3 then the code $F_4(D)$ over $\mathbb{Z}_4$ is a length 26 self-dual code with minimum weight 5 and weight enumerator given in Table 1. The code $E_2(D)$ is a $[26,13,6]$ binary code.

- If D is the biplane of order 3 then the code $F_4(D)$ over $\mathbb{Z}_4$ is a length 22 self-dual code with minimum weight 6 and weight enumerator given in Table 1. This code is an optimal self-dual code. The code $E_2(D)$ is the $[22, 11, 6]$ binary baby Golay code.

4.6 Symmetric designs of order 4

For $n = 4$ the possible λ are $1, 2, 3, 4, 6, 12$. These correspond to the projective plane of order 4, the three biplanes of order 4, the design formed from the codewords of the simplex code, and their complements. Here only 5 divides $n + 1$.

- If D is the projective plane of order 4 then $E_5(D)$ is a $[42, 21, 10]$ self-dual code over $\mathbb{F}_5$ [4].

- If D is any of the 3 biplanes of order 4 then $E_5(D)$ is a $[32, 16, 8]$ self-dual code over $\mathbb{F}_5$, as in the previous section.

- If D is the design formed from the simplex code then $E_5(D)$ is a $[30, 15, 8]$ self-dual code over $\mathbb{F}_5$, with weight enumerator given in Table 1.

References

[1] E.F. Assmus, Jr., and J.D. Key, *Designs and their Codes*. Cambridge University Press:Cambridge, 1992.

[2] A.E. Brouwer, Block Designs, in *Handbook of Combinatorics*, R.L. Graham. M Grötschel, L. Lovász, eds., 693–745, Elsevier:Amsterdam, 1995.

[3] D. Burton, *Elementary Number Theory*, McGraw-Hill:New York, 2002.

[4] S.T. Dougherty, A New Construction of Self-Dual Codes from Projective Planes, *Australasian J. Comb.*, **31**, 337–348, 2005.

[5] S.T. Dougherty, M. Harada and P. Solé, Self-dual Codes over the Chinese Remainder Theorem, *Hokkaido Math Journal*, **28**, 253–283, 1999.

[6] D. Glynn, The Construction of Self-dual Binary Codes from Projective Planes of Odd Order, *Australasian J. Comb.*, 4, 277–284, 1991.

[7] J.D. Key and V.D. Tonchev, Computational Results for the Known Biplanes of Order 9, in *Geometry, Combinatorial Designs and Related Structures*, London Math. Soc. Lecture Notes Ser. 245, Cambridge University Press:Cambridge 1997.

[8] M. Klemm, Selbstduale Code über dem Ring der ganzen Zahlen modulo 4., *Arch. Math. (Basel)*, **53**, 201-207, 1989.

[9] M. Klemm, Über den p-Rang von Inzidenzmatrizen. *J. Combin. Theory Ser. A* **51**, 138–139, 1986.

[10] W.C. Huffman and V.S. Pless, *Fundamentals of Error-correcting Codes*, Cambridge: Cambridge University Press, 2003.

[11] E. Rains and N.J.A. Sloane, Self-dual Codes, in *Handbook of Coding Theory*, V.S. Pless and W.C. Huffman, eds., 177–294, Elsevier:Amsterdam, 1998.

[12] G. Royle, Known Biplanes, http://www.csse.uwa.edu.au/ gordon/remote/biplanes/.

Table 1: Weight Enumerators

Plane-3	Biplane-3	Simplex	Weight
1	1	1	0
26	0	0	5
52	77	0	6
0	352	0	7
702	550	1260	8
1872	880	0	9
4433	7436	4872	10
18096	33024	3360	11
79404	86900	87220	12
257116	185680	159600	13
665340	358270	1482180	14
1609296	584672	4502912	15
3440905	769505	22110720	16
6086600	811536	65096640	17
9029358	675180	202580140	18
11348688	425920	473746560	19
11902124	191620	1116132192	20
10238618	55088	2004097480	21
7039656	7613		22
3673904			23
1354080			24
320216			25
38377			26