AUSTRALASIAN JOURNAL OF COMBINATORICS
Volume **31** (2005), Pages 337–348

A new construction of self-dual codes from projective planes

Steven T. Dougherty

Department of Mathematics
University of Scranton
Scranton, PA 18510
U.S.A.

Abstract

From any projective plane of order n we construct a self-dual code over $\mathbb{F}_q$ of length $2n^2 + 2n + 2$ if either $q = 2$ or q is a prime congruent to 1 $\pmod 4$ that divides $n + 1$ and of length $2n^2 + 2n + 4$ if there is a prime q congruent to 3 $\pmod 4$ dividing $n + 1$.

1 Introduction

There have been many interesting results concerning the connection between codes over finite fields and finite designs. Usually, a code is formed from a design by generating it with the characteristic functions of the blocks. For a full account of this connection see [1]. The codes constructed in this work shall be constructed in a different manner than the usual construction.

In [4], Glynn gives a construction of self-dual binary codes from projective planes of odd order. In this work we shall generalize this construction to produce self-dual codes over various primes from projective planes. The constructions are equivalent for the case given in [4] but there the setting is different and is done in a very different way. His technique relies on the binary code corresponding to boolean characteristic functions and uses the geometry heavily. We simply give generators for the code and so we can generalize to non-binary fields and to other planes.

1.1 Planes

A finite projective plane Π with points $\mathcal{P}$, lines $\mathcal{L}$, and incidence relation $\mathcal{I} \subset \mathcal{P} \cup \mathcal{L}$ satisfies the following:
(1) any two points are incident with a unique line;
(2) any two lines are incident with a unique point;
and
(3) there exist at least four points no three of which are collinear.

It follows that $|\mathcal{P}| = |\mathcal{L}| = n^2 + n + 1$ for some n, which is the order of the plane. Finite projective planes exists for all prime power orders. It is not known if there exist planes for non-prime power orders. For a complete description of finite projective planes see Chapter 6 of [1] and the references therein.

1.2 Codes

A code is a subset of the space $\mathbb{F}_q^m$ where $\mathbb{F}_q$ is the finite field of order q. A linear code is a vector subspace of the ambient space. In general, we let q be a prime. Attached to the ambient space is the usual innerproduct, i.e.

$$[v,w] = \sum v_i w_i.$$

The orthogonal to the code is given by

$$C^\perp = \{w \mid [v,w] = 0 \ \forall v \in C\}.$$

A code is self-orthogonal if $C \subseteq C^\perp$ and is self-dual if $C = C^\perp$. Self-dual codes exist for all even lengths for $q = 2$ and $q \equiv 1 \pmod 4$ and for all lengths divisible by 4 for $q \equiv 3 \pmod 4$. For a complete description of self-dual codes and all undefined terms see [5].

The Hamming weight of a vector is the number of non-zero elements in the vector. The minimum weight of a code C is denoted by d_C and is the smallest of all non-zero Hamming weights in the code.

The Hamming weight enumerator of a code C is given by

$$W_C(x,y) = \sum_{c \in C} x^{n-wt(c)} y^{wt(c)} \tag{1}$$

where $wt(c)$ is the number of non-zero elements in c. Usually, when displaying the weight enumerator we set $y = 1$.

2 Constructing the codes

Let Π be a plane of order n and q a prime that divides $n+1$. For a given point p in $\mathcal{P}$, let χ_p be the vector of length n^2+n+1 that has a 1 at the coordinate corresponding to p and a 0 elsewhere. Let λ_p be the vector of length n^2+n+1 with a 1 at the coordinate for a line L if L is incident with p and a 0 elsewhere.

List the points of Π by $\mathcal{P} = \{p_1, \dots, p_{n^2+n+1}\}$ and the lines of Π by $\mathcal{L} = \{\ell_1, \dots, \ell_{n^2+n+1}\}$ and use the points as coordinates of the first n^2+n+1 places and the lines as the coordinates of the second n^2+n+1 places in $\mathbb{F}_q^{2(n^2+n+1)}$.

For $p_1 \neq p_2$, let $\Delta(p_1,p_2) = (\chi_{p_1} - \chi_{p_2}, \lambda_{p_1} - \lambda_{p_2})$. Specifically, this vector has a 1 at the coordinate corresponding to p_1, a -1 on the coordinate corresponding to p_2 and a 0 elsewhere on the first n^2+n+1 coordinates. On the second set of n^2+n+1 coordinates, there is a 1 on the coordinates corresponding to the lines through p_1 but not through p_2, a -1 on the lines corresponding to the lines through p_2 and not through p_1 and a 0 elsewhere. The Hamming weight of $\Delta(p_1,p_2)$ is $2n+2$.

Lemma 2.1 *For a plane Π of order n and q a prime dividing $n+1$, with $p_i \in \mathcal{P}$,*

$$[\Delta(p_1,p_2),\Delta(p_3,p_4)] = 0. \tag{2}$$

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

Case 1: If the p_i are distinct then there are no non-zero coordinates matching up on the first n^2+n+1 coordinates. On the second n^2+n+1 coordinates

$$\begin{aligned}[(\lambda_{p_1}-\lambda_{p_2}),(\lambda_{p_3}-\lambda_{p_4})] &= [\lambda_{p_1},\lambda_{p_3}]-[\lambda_{p_1},\lambda_{p_4}]-[\lambda_{p_2},\lambda_{p_3}]+[\lambda_{p_2},\lambda_{p_4}] \\ &= 1-1-1+1=0.\end{aligned}$$

Case 2: If $p_1 = p_3$ and $p_2 \neq p_4$ then

$$[(\chi_{p_1}-\chi_{p_2}),(\chi_{p_3}-\chi_{p_4})] = 1 \tag{3}$$

since p_1 matches p_3 and p_2 is distinct from p_4. Then

$$\begin{aligned}[(\lambda_{p_1}-\lambda_{p_2}),(\lambda_{p_3}-\lambda_{p_4})] &= [\lambda_{p_1},\lambda_{p_1}]-[\lambda_{p_1},\lambda_{p_4}]-[\lambda_{p_2},\lambda_{p_1}]+[\lambda_{p_2},\lambda_{p_4}] \\ &= (n+1)-1-1+1=n.\end{aligned}$$

This gives that

$$[((\chi_{p_1}-\chi_{p_2}),(\lambda_{p_1}-\lambda_{p_2})),((\chi_{p_3}-\chi_{p_4}),(\lambda_{p_3}-\lambda_{p_4}))] = 1+n=0. \tag{4}$$

Case 3: If $p_1 = p_4$ and $p_2 \neq p_3$ then

$$[(\chi_{p_1}-\chi_{p_2}),(\chi_{p_3}-\chi_{p_4})] = -1 \tag{5}$$

since p_1 matches p_4 (which has a -1 at this coordinate) and p_2 is distinct from p_3. Then

$$\begin{aligned}[(\lambda_{p_1}-\lambda_{p_2}),(\lambda_{p_3}-\lambda_{p_4})] &= [\lambda_{p_1},\lambda_{p_3}]-[\lambda_{p_1},\lambda_{p_1}]-[\lambda_{p_2},\lambda_{p_1}]+[\lambda_{p_2},\lambda_{p_1}] \\ &= 1-(n+1)-1+1=-n.\end{aligned}$$

This gives that

$$[((\chi_{p_1}-\chi_{p_2}),(\lambda_{p_1}-\lambda_{p_2})),((\chi_{p_3}-\chi_{p_4}),(\lambda_{p_3}-\lambda_{p_4}))] = -1-n=0. \tag{6}$$

□

Define the following code. Let

$$C(\Pi) = \langle \Delta(p_1,p_2) \mid p_1,p_2 \in \mathcal{P}\rangle. \tag{7}$$

Lemma 2.2 *If Π is a projective plane of order n with q a prime dividing $n+1$ then $C(\Pi)$ is a self-orthogonal code of length $2n^2+2n+2$ and dimension n^2+n.*

Proof. The dimension follows from the fact that a basis can be made by fixing p_1 and then taking $\Delta(p_1, p_i)$ for the other n^2+n values of i. It is easy to see that these n^2+n vectors are linearly independent and span the space. The fact that it is self-orthogonal follows from Lemma 2.1. □

Let P be the vector that is 1 on the coordinates of $\mathcal{P}$ and 0 elsewhere and let L be the vector that is 1 on the coordinates of $\mathcal{L}$ and 0 elsewhere. Notice that $P, L \in C(\Pi)^{\perp}$. The codimension of $C(\Pi)$ in $C(\Pi)^{\perp}$ is 2. In fact, the cosets of C are

$$C_{i,j} = C + iP + jL. \tag{8}$$

It is easy to determine the orthogonality relations between the cosets. Any vector in $C_{i,j}$ is of the form $c+iP+jL$ for some $c \in C$ and any vector in $C_{i',j'}$ is of the form $c' + i'P + j'L$ for some $c' \in C$. We shall denote the inner-product of any vector in $C_{i,j}$ with any vector in $C_{i',j'}$ by $[C_{i,j}, C_{i',j'}]$. We notice that since $n+1 \equiv 0 \pmod{q}$, we have $n \equiv -1 \pmod{q}$ and $n^2 \equiv 1 \pmod{q}$. Then

$$\begin{aligned}[c+iP+jL, c'+i'P+j'L] &= ii'[P,P] + ij'[P,L] + ji'[L,P] + jj'[L,L] \\ &= ii'(n^2+n+1) + jj'(n^2+n+1) \\ &= ii' + jj'.\end{aligned}$$

Hence

$$[C_{i,j}, C_{i',j'}] = ii' + jj'. \tag{9}$$

What is needed to form a self-dual code is a self-orthogonal vector in $C(\Pi)^{\perp}$. Since P and L are in the orthogonal, so are iP and jL for i, j in $\mathbb{F}_q$. Consider the vector $(iP+jL)$, that is the vector with an i in the first n^2+n+1 coordinates and a j in the second n^2+n+1 coordinates. Then

$$\begin{aligned}[(iP+jL),(iP+jL)] &= (n^2+n+1)i^2 + (n^2+n+1)j^2 \\ &= n^2(i^2+j^2) = i^2+j^2.\end{aligned} \tag{10}$$

We need $i^2+j^2 = 0$, which has a solution $i = \sqrt{-1}j$ in $\mathbb{F}_q$ whenever $q \equiv 1 \pmod{4}$.

Define $D(\Pi) = \langle C, iP+jL \rangle$, where $i = \sqrt{-1}j$ for some $j \in \mathbb{F}_q$.

Theorem 2.3 *Let Π be a plane of order n with $q \equiv 1 \pmod{4}$ a prime dividing $n+1$, then $D(\Pi)$ is a self-dual code.*

Proof. Lemma 2.2 gives that the code is self-orthogonal of dimension 1 less than a self-dual code. Adjoining a self-orthogonal vector from the dual code $C(\Pi)^{\perp}$ will give a self-dual code. We have shown that $iP+jL$, with $i = \sqrt{-1}j$, is self-orthogonal and hence the code is self-dual. □

Any automorphism of the projective plane Π induces an automorphism of the codes $C(\Pi)$ and $D(\Pi)$ by simply allowing it to act on the coordinates as it acts on the points and lines of the plane. It is clear that if two planes are isomorphic then their associated codes are also isomorphic. Therefore, the codes associated with desarguesian planes have non-trivial automorphism groups.

In [4], Glynn gives this construction (in a very different form) only for odd planes and binary codes. Hence 2 always divides $n+1$ and does not divide n^2+n+1 but does divide $2(n^2+n+1)$. Thus, he constructs the code $\langle C, P+L\rangle$. He also notes that $C(\Pi)$ is doubly-even, that is, the Hamming weight of each vector is a multiple of 4. The construction employed there is intimately related to the theory of shadows. Specifically, $C(\Pi)$ is the doubly-even subcode of codimension 1 in $D(\Pi)$ and $C(\Pi)^\perp - D(\Pi)$ is the shadow of the code $D(\Pi)$. Glynn shows that the minimum weight of the self-dual code is $2n$ for a plane of order n and the minimum weight of the shadow is $n+2$. Moreover, he shows that the number of vectors of minimum weight in the shadow is $2(n^2+n+1)$. Using these facts and applying the theory of shadows gives that the weight enumerator of the $[26,13,6]$ self-dual code with $d_S=5$ formed from the plane of order 3 and the $[62,31,10]$ self-dual code with $d_S=7$ formed from the plane of order 5 have unique weight enumerators. This simplifies the proofs given in [4].

Additionally, in the binary case there is another interesting relationship for the weight enumerators given in the following theorem.

Theorem 2.4 *Let Π be a projective plane of odd order n, and let $q=2$. Then*

$$W_{D(\Pi)}(x,y) = W_{C(\Pi)}(x,y) + W_{C(\Pi)}(y,x). \tag{11}$$

Proof. The code $D(\Pi) = C(\Pi) \cup (C(\Pi)+(P+L))$. The vector $P+L$ is the all one vector and hence adding the all one vector to any vector in $C(\Pi)$ changes each 1 to a 0 and each 0 to a 1. □

Theorem 2.5 *Let Π be a plane of order n, $q \equiv 3 \pmod 4$ a prime dividing $n+1$ then $C(\Pi)$ is a maximal self-orthogonal code.*

Proof. We need to show that there is no self-orthogonal vector in $C(\Pi)^\perp$. Assume to the contrary, then there exists a vector of the form $c+iP+jL$ for some vector c in $C(\Pi)$, that is self-orthogonal. This follows from the fact that $C(\Pi)^\perp = \cup_{i,j\in\mathbb{F}_q} C_{i,j}$. Then $[c+iP+jL, c+iP+jL]=0$. Noticing $[c,iP]=0=[c,jL]$ since iP, jL are in $C(\Pi)^\perp$, we have that $i^2+j^2=0$ and then that $\sqrt{-1}\in\mathbb{F}_q$ with $q\equiv 3 \pmod 4$ which is a contradiction. Therefore the code is a maximal self-orthogonal code. □

Example 2.6 *Consider the projective plane of order 2. Here 3 divides $n+1$. Hence $C(\Pi)$ is a maximal self-orthogonal code of length 14 over $\mathbb{F}_3$ with minimum weight 6. Its weight enumerator is*

$$W_{C(\Pi)}(1,y) = 1 + 84y^6 + 476y^9 + 168y^{12}. \tag{12}$$

We shall show how to construct a self-dual code in the case where $q \equiv 3 \pmod 4$. To each vector in $C_{i,j} = (C + iP + jL)$ adjoin a vector of length 2, $w_{i,j}$. To insure linearity we want $w_{i,j} = iw_{1,0} + jw_{0,1}$. For the new code to be self-dual we need, $[w_{i,j}, w_{i'j'}] = -[C_{i,j}, C_{i',j'}]$. It is enough to find $w_{1,0}$ and $w_{0,1}$ with the property that

$$[w_{1,0}, w_{1,0}] = [w_{0,1}, w_{0,1}] = -1 \tag{13}$$

since $[P, P] = [L, L] = n^2 + n + 1 = 1$, and

$$[w_{1,0}, w_{0,1}] = 0 \tag{14}$$

since $[P, L] = 0$.

Since $q \equiv 3 \pmod 4$ it is well known that there exist α, β with $\alpha^2 + \beta^2 = -1$. Let $w_{1,0} = (\alpha, \beta)$ and $w_{0,1} = (-\beta, \alpha)$. These vectors satisfy equations (13) and (14).

Define

$$E(C) = \cup_{i,j}(C_{i,j}, w_{i,j}). \tag{15}$$

The length of this code is $2(n^2 + n + 1) + 2 = 2n^2 + 2n + 4$ and has dimension $n^2 + n + 2$.

This gives the following theorem.

Theorem 2.7 *Let Π be a projective plane of order n with $q \equiv 3 \pmod 4$ a prime dividing $n + 1$. Then $E(\Pi)$ is a self-dual code of length $2n^2 + 2n + 4$.*

To continue Example 2.6, if Π is the plane of order 2 then $E(C)$ is a self-dual code of length 16 with weight enumerator

$$W_{E(\Pi)}(1, y) = 1 + 224y^6 + 2720y^9 + 3360y^{12} + 256y^{15}. \tag{16}$$

This code is optimal for ternary self-dual codes of length 16.

The construction of $E(\Pi)$ is similar to the techniques of shadow construction given in [2] and [3] for self-dual codes.

For a given point ℓ in $\mathcal{L}$, let η_ℓ be the vector of length $n^2 + n + 1$ that has a 1 at the coordinate corresponding to ℓ and a 0 elsewhere. Let μ_ℓ be the vector of length $n^2 + n + 1$ with a 1 at the coordinate for a point p if ℓ is incident with p and a 0 elsewhere.

We shall consider vectors of the form

$$\Gamma(\ell_1, \ell_2) = (\mu_{\ell_1} - \mu_{\ell_2}, \eta_{\ell_2} - \eta_{\ell_1}). \tag{17}$$

Notice that the order is switched in the second part. For binary codes, as in [4], the order is not switched in the second part since subtraction is addition.

Essentially, the lines and points play the opposite role in this construction. We shall show that the code generated by these vectors is in fact $C(\Pi)$.

Let ℓ_1 and ℓ_2 be two lines in Π with $\{p_1, p_2, \ldots, p_n\}$ the points on ℓ_1 not on ℓ_2 and $\{p'_1, p'_2, \ldots, p'_n\}$ the points on ℓ_2 not on ℓ_1. It is easy to see that $\sum_{i=1}^{n}(\chi_{p_i} - \chi_{p'_i}) = \mu_{\ell_1} - \mu_{\ell_2}$ on the first $n^2 + n + 1$ coordinates. On the second $n^2 + n + 1$ coordinates consider $\sum_{i=1}^{n}(\lambda_{p_i} - \lambda_{p'_i})$. For the coordinate corresponding to ℓ_1 the vector λ_{p_i} is 1 there and the vector $\lambda_{p_i'}$ is 0 there. Hence in the sum there is an n which is -1. On the coordinate for ℓ_2 there a 1 for each $\lambda_{p_i'}$ and a 0 for each λ_{p_i}. Hence in the sum there is a $-n$ which is 1. On any other line there is one coordinate with a 1 and one with a -1 since any line intersects ℓ_1 and ℓ_2 exactly once. So on the second set of coordinates the vector is $\eta_{\ell_2} - \eta_{\ell_1}$.

Hence we have

$$\sum_{i=1}^{n} \Delta(p_i, p_i') = \Gamma(\ell_1, \ell_2), \tag{18}$$

where the points incident with ℓ_1 not incident with ℓ_2 are $\{p_1, p_2, \ldots, p_n\}$ and the points incident with ℓ_2 not incident with ℓ_1 are $\{p_1', p_2', \ldots, p_n'\}$.

Theorem 2.8 *The code* $C(\Pi) = \langle \Delta(\ell_1, \ell_2) \mid \ell_1, \ell_2 \in \mathcal{L} \rangle$.

Proof. The previous discussion shows that it is a subset and then noticing that the dimension is again $n^2 + n$ we see that the two codes are equal. □

3 Minimum Weights

In this section we shall determine the minimum weights of the codes $C(\Pi)$, $D(\Pi)$, $E(\Pi)$ and $C(\Pi)^{\perp}$. We begin with a few necessary lemmas.

Lemma 3.1 *Vectors of the form* (χ_p, λ_p) *are in* $C(\Pi)^{\perp}$.

Proof. We only need to show it is orthogonal to each generator. If $p \neq p'$ then

$$[(\chi_p, \lambda_p), (\chi_p - \chi_{p'}, \lambda_p - \lambda_{p'})] = 1 + n = 0. \tag{19}$$

If $p \neq p_1, p_2$ then

$$[(\chi_p, \lambda_p), (\chi_{p_1} - \chi_{p_2}, \lambda_{p_1} - \lambda_{p_2})] = 0 + 1 - 1 = 0. \tag{20}$$

□

Lemma 3.2 *Vectors of the form* $(\mu_\ell, -\eta_\ell)$ *are in* $C(\Pi)^{\perp}$.

For any line $\ell \in L$, we have

$$[(\mu_\ell, -\eta_\ell), (\mu_{\ell_1} - \mu_{\ell_2}, \eta_{\ell_2} - \eta_{\ell_1})] = 1 - 1 = 0, \tag{21}$$

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

$$[(\mu_\ell, -\eta_\ell), (\mu_{\ell_1} - \mu_{\ell_2}, \eta_{\ell_2} - \eta_{\ell_1})] = n + 1 = 0 \tag{22}$$

if $\ell = \ell_1$ and

$$[(\mu_\ell, -\eta_\ell), (\mu_{\ell_1} - \mu_{\ell_2}, \eta_{\ell_2} - \eta_{\ell_1})] = -n - 1 = 0 \tag{23}$$

if $\ell = \ell_2$. □

Lemma 3.3 *If v is a vector in $C(\Pi)$ and ℓ is exterior to $Supp_{\mathcal{P}}(v)$ then $v_\ell = 0$.*

Proof. We know $[(\mu_\ell, -\eta_\ell), v] = 0$ but $[(\mu_\ell, -\eta_\ell), v] = v_\ell$ and therefore $v_\ell = 0$.

Theorem 3.4 *Let Π be a projective plane of order n, then the minimum weight of $C(\Pi)$ is $2n + 2$.*

Proof. The generators have weight $2n+2$ so the minimum weight is at most $2n+2$.

Assume there exists a vector with weight less than $2n+2$, i.e. $|Supp(v)| < 2n+2$. Denote by $Supp_{\mathcal{P}}(v)$ and $Supp_{\mathcal{L}}(v)$ the supports on the coordinates corresponding to points and lines respectively. For any line $\ell \in L$, we have $(\mu_\ell, -\eta_\ell) \in C(\Pi)^\perp$ by Lemma 3.2.

Assume $v_p \neq 0$ for $p \in \mathcal{P}$, i.e. $p \in Supp_{\mathcal{P}}(v)$ and assume l is tangent to $Supp_{\mathcal{P}}(v)$ at p. Then we have

$$[v, \mu_\ell - \eta_\ell] = v_p - v_\ell = 0.$$

Hence $v_p = v_\ell$. Therefore if ℓ is tangent to $Supp_{\mathcal{P}}(v)$ then $v_\ell \neq 0$. At this point the proof is similar to the binary case given in [4]. Specifically, assume $|Supp_{\mathcal{P}}(v)| = a$ then at each point in $Supp_{\mathcal{P}}(v)$ there are at least $n + 2 - a$ lines tangent. Hence $|Supp_{\mathcal{L}}(v)| \geq a(n + 2 - a)$ and therefore $|Supp(v)| \geq a(n + 3 - a)$ giving that $2(n + 1) - a(n + 3 - a) = (a - 2)(a - (n + 1)) \leq 0$.

Thus the minimum weight of $C(\Pi) = 2n + 2$. □

Lemma 3.5 *Let Π be a projective plane of order n, then the minimum weight of $D(\Pi)$ is greater than or equal to $2n$.*

Proof. Assume the weight of $(v + iP + jL) \in D(\Pi)$ is less than $2n$. Let $b = |Supp_{\mathcal{P}}(v+iP)|$. Without loss of generality assume $b < n$. If ℓ is exterior to $Supp_{\mathcal{P}}(v+iP)$ then $v_p = -i$ for all p incident with ℓ, since $v_p + i$ must be 0.

We know $[v, (\mu_\ell, -\eta_\ell)] = 0$ since $v \in C(\Pi)$. Also we have $[v, (\mu_\ell, -\eta_\ell)] = -(n + 1)i - v_\ell = -v_\ell$, therefore $v_\ell = (v + P)_\ell = 0$. We have $(v + iP)_\ell = 0$ for lines exterior to $Supp_{\mathcal{P}}(v + iP)$.

There are at most $n + 1 + (b - 1)n$ lines through $Supp_{\mathcal{P}}(v + iP)$, and so there are at least $n^2 + n + 1 - (n + 1 + (b - 1)n) = n(n + 1 - b)$ lines exterior. Therefore $(v + iP + jL)_\ell \neq 0$ for all exterior lines ℓ.

Then $Supp(v + iP + jL) \geq b + n^2 + n - bn = n^2 + n - b(n - 1)$. When $n > b$ we have $n^2 + n - b(n - 1) > 2n$. Therefore the minimum weight of $D(\Pi)$ is at least $2n$. □

Theorem 3.6 *Let Π be a projective plane of order n, then the minimum weight of $D(\Pi)$ is $2n$ if $q = 2$.*

Proof. The vector $(\chi_p, \lambda_p) + (\mu_\ell, -\eta_\ell)$ with p incident with ℓ has weight $2n$ if $q = 2$. Moreover, we have that $[(\chi_p, \lambda_p), (\mu_\ell, -\eta_\ell)] = 1 - 1 = 0$ when p is incident with ℓ. Since there is only one self-orthogonal coset for the binary case we know this vector is in $D(\Pi)$. □

Theorem 3.7 *Let* Π *be a projective plane of order* n*, then the minimum weight of* $D(\Pi)$ *is* $2n+2$ *if* $q \equiv 1 \pmod 4$.

Proof. For $p \equiv 1 \pmod 4$ the self-orthogonal vector corresponding to the weight $2n$ vectors in the binary case would be of the form $i(\chi_p, \lambda_p) + j(\mu_\ell, -\eta_\ell)$, where $i = \sqrt{-1}j$, which has weight $2n+2$.

All that remains is to show that there are no vectors of weight $2n$ or $2n+1$ in $D(\Pi)$ when $q \equiv 1 \pmod 4$. Assume there was a vector v of weight $2n$, then by the previous discussion its support would have to be n points on a line ℓ and the n lines through the $n+1$-st point on the line ℓ. Let w be such a vector. Since $[w, (\chi_p - \chi_{p'}, \lambda_p - \lambda_{p'})] = w_p - w_{p'} = 0$ for p, p' in $Supp_{\mathcal{P}}(w)$ we have that $w_p = w_{p'}$ on $Supp_{\mathcal{P}}(w)$. A similar argument shows the vector is constant on $Supp_{\mathcal{L}}(w)$. Let $w_p = \alpha$ for $p \in Supp_{\mathcal{P}}(w)$ and $w_\ell = \beta$ for $\ell \in Supp_{\mathcal{P}}(w)$. Since the vector is self-orthogonal we have that $\alpha^2 = -\beta^2$ and $\alpha = \sqrt{-1}\beta$ which gives that $\beta \neq \pm\alpha$ since $q \neq 2$. Let p a point in $Supp_{\mathcal{P}}(w)$ and p' be a point not in $Supp_{\mathcal{P}}(w)$. We have that $[w, (\chi_p - \chi_{p'}, \lambda_p - \lambda_{p'})] = \alpha - \beta$ since exactly one line through p' is exterior to $Supp_{\mathcal{P}}(w)$ in this situation. But $\alpha - \beta \neq 0$ giving a contradiction. Hence for $p \equiv 1 \pmod 4$ there are no weight $2n$ vectors.

Assume there is a weight $2n+1$ vector w in $D(\Pi)$, then without loss of generality we have that $|Supp_{\mathcal{L}}(w)| \geq n+1$. This implies that there is a b with $b = |Supp_{\mathcal{P}}(w)| \leq n$ and as before there are at least $n^2 + n - b(n-1)$ exterior lines which must be non-zero. This shows that the only case we need to consider is when $|Supp_{\mathcal{P}}(w)| = n$ and n exterior lines are non-zero and an additional line ℓ has w_ℓ non-zero. Let $\{p_1, p_2, \ldots, p_n\}$ be $Supp_{\mathcal{P}}(w)$. The innerproduct is

$$[w, (\chi_{p_i} - \chi_{p_j}, \lambda_{p_i} - \lambda_{p_j})] = w_{p_i} - w_{p_j} + (w_\ell - w_\ell) = 0.$$

If p_i and p_j are incident with ℓ then $w_{p_i} = w_{p_j}$ for all p_i on ℓ. Notice that some p_i must be incident with ℓ since it is not exterior to $Supp_{\mathcal{P}}(w)$.

Let p_i be incident with ℓ and p_j be not incident with ℓ then

$$[w, (\chi_{p_i} - \chi_{p_j}, \lambda_{p_i} - \lambda_{p_j})] = w_{p_i} - w_{p_j} + w_\ell = 0.$$

Thus for all p_j not incident with ℓ, w is constant on those coordinates and $w_{p_j} = w_{p_i} + w_\ell$. As before we can show that for all m, m' in $Supp_{\mathcal{L}} - \{\ell\}$ we have $w_m = w_{m'} = \delta$ for some δ. Since $[w, L] = n\delta + w_\ell = -\delta + w_\ell = 0$ we have that $w_L = -\delta$. It can be shown that if $\gamma = \sqrt{-1}$ then either $\alpha(\chi_p, \lambda_p) + \gamma\alpha(\mu_\ell, -\eta_\ell))$ or $\alpha(\chi_p, \lambda_p) + (-\gamma)\alpha(\mu_\ell, -\eta_\ell))$ are in $D(\Pi)$. Let v be the vector that is in $D(\Pi)$. Then by the construction given above there is a suitable choice of ϵ_1 and ϵ_2 so that $\epsilon_1 v + \epsilon_2 w$ is a vector of weight less than $2n$ which is a contradiction. Hence there are no vectors of weight $2n+1$. □

Theorem 3.8 *Let* Π *be a projective plane of order* n*, then the minimum weight of* $C(\Pi)^\perp$ *is* $n+2$.

Proof. The vector (χ_p, λ_p) is in $C(\Pi)^\perp$ by Lemma 3.1. The weight of (χ_p, λ_p) is $n+2$ and thus the minimum weight is at most $n+2$.

We shall now show the weight cannot be less than $n+2$. Let $a = |Supp_{\mathcal{P}}(v)|$. The largest number of lines that intersect $Supp_{\mathcal{P}}$ is $(n+1)+n(a-1)$ which obviously occurs when the points are collinear. There are at least $n^2+n+1-((n+1)+n(a-1)) = n(n+1-a)$ lines exterior to $Supp_{\mathcal{P}}(v)$. We have shown that vectors of the form $v+iP+jL$, $i,j \neq 0$ have weight greater than or equal to $2n$ in the previous lemma so we need only to consider vectors of the form $v+jL$, $j \neq 0$ and $v+iP$, $i \neq 0$. We shall show the case $v+jL$, the other case follows similarly.

If $a \geq n+2$ the weight of $v+jL$ is greater than or equal to $n+2$. If $a \leq n+2$ then the weight of $v+jL$ is at least $a+n(n+1-a)$. If $a < n+1$ then this weight is greater than or equal to $2n$. If $a = n+1$ then the only way for the vector to have weight $n+1+(n(n+1-(n+1)) = n+1$ is if the points are collinear and $v_\ell = 0$ for $\ell \in \mathcal{L}$. In this case, $v = \mu_\ell$. Then

$$[\mu_\ell, (\mu_\ell - \mu_m, \eta_m - \eta_\ell)] = n \neq 0$$

which contradicts that $v \in C(\Pi)^\perp$.

If $a = n+1$ and $Supp_{\mathcal{P}}(v)$ is not a line then there are at most

$$(n+1)+n(a-2)+n-1$$

lines intersecting $Supp_{\mathcal{P}}(v)$ with

$$n^2+n+1-((n+1)+n(n+1-2)+n-1) = 1$$

line exterior. Then the weight of v is $n+2$.

Therefore the weight of any vector in $C(\Pi)^\perp$ is at least $n+2$. □

Corollary 3.9 *The minimum weight vectors in $C(\Pi)^\perp$ are scalar multiples of (χ_p, λ_p) or $(\mu_\ell, -\eta_\ell)$ for some point p or some line ℓ.*

Proof. We showed that the sizes of the two supports ($Supp_{\mathcal{P}}$ and $Supp_{\mathcal{L}}$) of a minimum weight vector must be n and 1, and that the supports are either n points on a line and a line with which they are collinear or n lines and a point with which they are copunctual. If there were another vector v with the same support but not a multiple of the vectors w described above then $\alpha v + \beta w$ would have weight less than $n+2$ for proper choice of α, β. □

Theorem 3.10 *Let Π be a projective plane of order n, $q \equiv 3 \pmod 4$ a prime dividing $n+1$ then the minimum weight of $E(\Pi)$ is $n+4$.*

Proof. The vectors in $E(\Pi)$ consist of the vectors in $C(\Pi)^\perp$ with a length 2 vector adjoined. The minimum weight vectors given in Corollary 3.9 all have a weight 2 vector adjoined. Each other vector has at least a weight 1 vector adjoined except for the vectors in $C(\Pi)$ whose vectors have minimum weight $2n+2$. □

4 Conclusion

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

Theorem 4.1 *Let* Π *be a projective plane of order* n. *If* $q \equiv 1 \pmod 4$ *divides* $n+1$ *then the code* $D(\Pi)$ *is an* $[2(n^2+n+1), n^2+n+1, 2n+2]$ *self-dual code over* $\mathbb{F}_q$. *If* 2 *divides* $n+1$ *then the code* $D(\Pi)$ *is an* $[2(n^2+n+1), n^2+n+1, 2n]$ *self-dual code over* $\mathbb{F}_2$. *If* $q \equiv 3 \pmod 4$ *is a prime dividing* $n+1$ *then the code* $C(\Pi)$ *is a maximal self-orthogonal* $[2(n^2+n+1), n^2+n+1, 2n+2]$ *code over* $\mathbb{F}_q$ *and* $E(\Pi)$ *is an* $[2(n^2+n+2), n^2+n+2, n+4]$ *self-dual code over* $\mathbb{F}_q$.

This theorem guarantees that every finite projective plane produces a self-dual code.

Examples:

- The projective plane of order 4 produces a $[42, 21, 10]$ self-dual code over $\mathbb{F}_5$.
- The projective plane of order 5 produces a $[62, 31, 10]$ self-dual code over $\mathbb{F}_2$.
- The projective plane of order 5 produces a $[64, 32, 9]$ self-dual code over $\mathbb{F}_3$.
- The projective plane of order 7 produces a $[114, 57, 14]$ self-dual code over $\mathbb{F}_2$.
- The projective plane of order 8 produces a $[148, 74, 12]$ self-dual code over $\mathbb{F}_3$.
- The projective plane of order 9 produces a $[182, 91, 18]$ self-dual code over $\mathbb{F}_2$.
- The projective plane of order 9 produces a $[182, 91, 20]$ self-dual code over $\mathbb{F}_5$.
- A putative projective plane of order 36 produces a $[2666, 1333, 74]$ self-dual code over $\mathbb{F}_{37}$. Notice that this putative plane would not produce a self-dual code under the usual coding constructing from planes for any prime.

References

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

[2] S.T. Dougherty, *Shadow Codes and their Weight Enumerators*, IEEE Trans. Inform. Theory **41** No. 3 (1995), 762–768.

[3] S.T. Dougherty and P. Solé, *Shadows of codes and lattices*, Proc. Third Asian Math. Conf., 2000 (Diliman), 139–152, World Sci. Publishing, River Edge, NJ, 2002.

[4] D. Glynn, *The construction of self-dual binary codes from projective planes of odd order*, Australas. J. Combin. **4** (1991), 277–284.

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

(Received 19 July 2003)