Mathematical Journal of Okayama University

Volume 40, *Issue* 1 1998 *Article* 8

JANUARY 1998

Self-Dual Codes and Finite Projective Planes

Steven T. Dougherty*

*University of Scranton

Self-Dual Codes and Finite Projective Planes

Steven T. Dougherty

Abstract

We investigate self-dual codes from symmetric designs, specifically for the case when these designs are finite projective planes. We give a proof of the Bruck-Ryser-Chowla theorem in the case where a prime sharply divides the order in a coding-theoretic setting. We give constructions of self-dual codes arising from finite projective planes and also sudy the weight enumerators of the codes formed from projective planes.

Math. J. Okayama Univ. **40** (1998), 45-54 [2000]

SELF-DUAL CODES AND FINITE PROJECTIVE PLANES

STEVEN T. DOUGHERTY

ABSTRACT. We investigate self-dual codes from symmetric designs, specifically for the case when these designs are finite projective planes. We give a proof of the Bruck-Ryser-Chowla theorem in the case where a prime sharply divides the order in a coding-theoretic setting. We give constructions of self-dual codes arising from finite projective planes and also study the weight enumerators of the codes formed from projective planes.

1. INTRODUCTION

There have been many interesting and productive results from the application of coding theory to the study of finite designs. See [1] for many examples. In this paper, we consider self-dual codes formed from symmetric designs and the weight enumerators formed by the codes of these designs.

In section 2 we give a coding-theory proof of a specific case of the Bruck-Ryser-Chowla theorem when there exists a prime which sharply divides the order of the design. In section 3 we give constructions for self-dual codes from projective planes. In section 4 we investigate the complete weight enumerator of the codes formed from projective planes, and we place restrictions on these weight enumerators.

A linear $[n,k]$ code C over F_p is a k-dimensional vector subspace of F_p^n, where F_p is the field with p elements, p prime. The elements of C are called codewords and the Hamming weight $wt(x)$ of a codeword x is the number of its non-zero coordinates. Let C be a code over F_p, p a prime, then the **complete weight enumerator** is

$$W_C(x_0, x_1, \ldots, x_{p-1}) = \sum A_{(a_0,a_1,\ldots,a_{p-1})} x_0^{a_0} x_1^{a_1} \cdots x_{p-1}^{a_{p-1}},$$

where there are $A_{(a_0,a_1,\ldots,a_{p-1})}$ vectors in C with a_i coordinates with i in them, where $i \in F_q$. The **Hamming weight enumerator** is

$$W_C(x,y) = \sum c_i x^{n-i} y^i,$$

where there are c_i vectors in C of weight i. The minimum weight of C is defined by $\min\{wt(x) \mid 0 \neq x \in C\}$. When the minimum weight d is known the code is referred to as an $[n,k,d]$ code.

We attach the standard innerproduct to the ambient space, i.e.

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

The author is grateful to Masaaki Harada for helpful conversations and to the referee for useful suggestions.

and define the dual as $C^{\perp} = \{x \in F_p^n | \ x \cdot y = 0 \text{ for all } y \in C\}$. C is *self-dual* if $C = C^{\perp}$ and C is *self-orthogonal* if $C \subseteq C^{\perp}$.

An incidence structure $D = (P, B)$ is a t-(v, k, λ) *design* where t, v, k, λ are non-negative integers, $|P| = v$, with P the set of points; every block $b \in B$ is incident with precisely k points; and every t distinct points are together incident with precisely λ blocks. Let $C_p(D)$ denote the code generated by characteristic function of blocks in D over the finite field F_p.

A finite *projective plane* Π of order n is a set of points P, a set of lines L, and an incidence relation I between them, where $|P| = |L| = n^2+n+1$. Any two points are incident with a unique line, and any two lines are incident with a unique point. Two planes are said to be isomorphic if there exists a bijection between them preserving incidence. Let $C_p(\Pi)$ denote the code generated by the characteristic functions of lines over F_p. We have that $C_p(\Pi) \subseteq F_p^{n^2+n+1}$. The Hull $Hull_p(\Pi)$ of Π is the code $C_p(\Pi) \cap C_p(\Pi)^{\perp}$. See [1] for many applications of the Hull.

2. Self-Dual Codes Constructed from Symmetric Designs

The following lemma is by Klemm [7] and appears as Theorem 2.4.2 in [1].

Lemma 2.1. *Let $D = (P, B)$ be a 2-(v, k, λ) design of order n and p a prime dividing n. Then the rank of an incidence matrix of D over F_p is bounded by*

$$rank_p(D) \leq \frac{|B|+1}{2},$$

moreover, if p does not divide λ and p^2 does not divide n, then

$$C_p(D)^{\perp} \subseteq C_p(D),$$

and $rank_p(D) \geq \frac{v}{2}$.

Lemma 2.2. *Let $D = (P, B)$ be a symmetric 2-(v, k, λ) design of order n with v odd and p a prime sharply dividing n and which does not divide λ . Then*

$$rank_p(D) = \lfloor \frac{v}{2} \rfloor + 1$$

and $C_p(D)^{\perp}$ is codimension 1 in $C_p(D)$.

Proof. Since the design is symmetric we have that $|B| = |P|$. The previous lemma gives that

$$\frac{v}{2} \leq rank_p(D) \leq \frac{v+1}{2}.$$

Given that v is odd we have that $rank_p(D) = \frac{v+1}{2}$. Then

$$\dim C_p(D)^{\perp} = v - \dim C_p(D) = v - \frac{v+1}{2} = \frac{v-1}{2} = \dim C_p(D) - 1,$$

giving the result, where $\dim C_p(D)$ denotes the dimension of $C_p(D)$. □

Remark. A similar result is listed in Theorem 17.3.1 of Hall [6].

Let D be a symmetric 2-(v,k,λ) design of order n (where $n = k-\lambda$) with p a prime not dividing λ and p sharply dividing n. We also assume v is odd. Set $H = C_p(D)^{\perp}$ and $C = C_p(D)$. The code H is a self-orthogonal code of length v of codimension 1 in $C = H^{\perp}$. Hence $C = \langle H, w\rangle$ for some codeword w. Let H_i denote the coset $H + iw$ in C for $i \in F_p$. Since $n = k - \lambda$ for a symmetric design and p divides n but does not divide λ then p does not divide k. Hence we can take w to be the characteristic function of a block since no block will be self-orthogonal over F_p and so not in $C_p(D)^{\perp}$. Set $\alpha = [w,w]$, i.e. $\alpha \equiv k \pmod p$.

We set $C' = \cup(w_i, H_i)$ where a vector in (w_i, H_i) is of the form (w_i, h_i) with h_i any vector in H_i. To insure that the code C' is linear once w_1 is chosen then $w_i = iw_1$. We also want the new code to be self-orthogonal so we need $w_1^2 = -\alpha$. Then

$$[(w_i,h_i),(w_j,h_j)] = [w_i,w_j] + [h+iw, h'+jw] = ij[w_1,w_1] + ij\alpha = 0.$$

If $-\alpha$ is a square in F_p, i.e. $-\alpha = \beta^2$ for some $\beta \in F_p$, then set $w_1 = \beta$. Then C' is a self-orthogonal linear code of length $v+1$ with $\dim C' = \dim H + 1 = \frac{v+1}{2}$, and therefore C' is a self-dual code.

If $-\alpha$ is not a square in F_p then it is the sum of squares, say $-\alpha = \gamma^2 + \delta^2$. Then set $w_1 = (\gamma, \delta, 0)$. Let $u = (a, b, c, 0, \ldots, 0)$. We want $[u, (w_i, h_i)] = 0$ and $[u,u] = 0$. That is we need $a\gamma + b\delta = 0$ and $a^2 + b^2 + c^2 = 0$. To solve the first choose a non-zero a and then $b = \frac{a\gamma}{-\delta}$. Then

$$\begin{aligned} a^2 + b^2 + c^2 &= 0, \\ a^2 + \frac{a^2\gamma^2}{\delta^2} + c^2 &= 0, \\ \frac{a^2(\gamma^2+\delta^2)}{\delta^2} + c^2 &= 0, \end{aligned}$$

making $c = \sqrt{\alpha}\frac{a}{\delta}$.

When $p \equiv 3 \pmod 4$, if $-\alpha$ is not a square then α is a square and hence a solution for c, but when $p \equiv 1 \pmod 4$ then if $-\alpha$ is not a square then neither is α. We have that $E = \langle u, C'\rangle$ is a self-orthogonal linear code of length $v+3$ with $\dim E = \dim C + 1 = \frac{v+1}{2} + 1 = \frac{v+3}{2}$ and so E is a self-dual code. This gives the following theorem.

Theorem 2.3. *Let D be a symmetric 2-(v,k,λ) design with p a prime sharply dividing n but not dividing λ. Then if $-k$ is a square in F_p the code C' is a self-dual code of length $v+1$. If $-k$ is not a square in F_p and $p \equiv 3 \pmod 4$ then the code E is a self-dual code of length $v+3$.*

Theorem 2.3 is a generalization of a result in [2]. It is well known that if $p \equiv 3 \pmod 4$ then a self-dual code of length m exists if and only if $m \equiv 0 \pmod 4$, giving the following:

Corollary 2.4. *Let D be a symmetric 2-(v,k,λ) design with $p \equiv 3 \pmod 4$ a prime sharply dividing n but not dividing λ. If $-k$ is not a square in F_p then $v \equiv 1 \pmod 4$ and if $-k$ is a square in F_p then $v \equiv 3 \pmod 4$.*

Notice that the Bruck-Ryser-Chowla theorem says that if a symmetric 2-(v,k,λ) design exists then either v is even and n is a square or v is odd and $z^2 = nx^2 + (-1)^{\frac{v-1}{2}}\lambda y^2$ has a non-trivial solution in integers x, y, z. The first case requires n to be a square which means no prime sharply divides it. If v is odd, assuming the conditions of Corollary 2.4, and if the above equation has integer solutions then replacing λ with $k - n$ and reading the equation $(\mathrm{mod}\ p)$ gives:

$$z^2 \equiv (-1)^{\frac{v-1}{2}} k \pmod{p}.$$

This implies the conclusion of the corollary. See [10] and [11] for similar arguments.

3. Self-Dual Codes Constructed from Projective Planes

For the specific case of a projective plane, using the results in previous section we have the following:

Corollary 3.1. *Let Π be a projective plane of order n with p a prime sharply dividing n. If $p \equiv 3 \pmod 4$, then the code $E = \langle C', w\rangle$ described above is a self-dual code of length $n^2 + n + 4$. If either $p = 2$ or $p \equiv 1 \pmod 4$, then the code $C' = \cup(w_i, H_i)$ is a self-dual code of length $n^2 + n + 2$.*

Thus the above corollary implies that $n^2 + n + 4$ must be divisible by 4 when $p \equiv 3 \pmod 4$, which implies $n^2 + n + 1 \equiv 1 \pmod 4$. If $n \equiv 1$ or $2 \pmod 4$ then $n^2 + n + 1$ is not $1 \pmod 4$ giving a special case of the Bruck-Ryser theorem first shown in [3]:

Corollary 3.2. *If $n \equiv 1$ or $2 \pmod 4$ and p is a prime sharply dividing n with p a prime and $p \equiv 3 \pmod 4$, then there does not exist a projective plane of order n.*

If $p = 2$ and n necessarily congruent to $2 \pmod 4$ this code must be doubly-even since the generators are self-orthogonal and have weight $n + 2$ which is divisible by 4 in this case. A binary self-dual code is doubly-even if all codewords have weight divisible by four. This construction was discovered very early in the study of codes and planes and was used in the study of the possible plane of order 10 (cf. [5] and [8]). In [2], this is used to prove the following:

Corollary 3.3. *If $n \equiv 6 \pmod 8$ then there exists no plane of order n.*

Proof. Follows from the previous corollary. Note that if a doubly-even code of length n exists then n must be divisible by eight. □

Theorem 3.4. *Let Π be a projective plane of order n with p a prime sharply dividing n, and $W(x_0, x_1, \ldots, x_{p-1})$ the complete weight enumerator of $Hull_p(\Pi)$. If $p \not\equiv 3 \pmod 4$ then the code C' is a self-dual code of length $n^2 + n + 2$ with complete weight enumerator*

$$\sum_{i=0}^{p-1} x_i W\left(x_{(0+(p-i))}, x_{(1+(p-i))}, \ldots, x_{(p-1+(p-i))}\right),$$

where the variable subscripts are read mod p. If $p \equiv 3 \pmod 4$ *then the code E described above is a self-dual code of length* n^2+n+4 *with complete weight enumerator*

$$\sum_{k=0}^{p-1} w_{0,k}(x_0, x_1, \ldots, x_{p-1}) W(x_0, x_1, \ldots, x_{p-1}) + \sum_{k=0}^{p-1} w_{1,k}(x_0, x_1, \ldots, x_{p-1}) W(x_{p-1}, x_0, \ldots, x_{p-2}) + \cdots + \sum_{k=0}^{p-1} w_{p-1,k}(x_0, x_1, \ldots, x_{p-1}) W(x_1, x_2, \ldots, x_0),$$

where $w_{i,k}(x_0, \ldots, x_{p-1})$ *is the weight enumerator of the vector* $kw + w_i$.

Proof. The weight enumerator for $p \not\equiv 3 \pmod 4$ is simply the sum of the weight enumerators of (w_i, H_i). For $p \equiv 3 \pmod 4$, it is the sum of the weight enumerators of $\sum_{\alpha=0}^{p-1} \alpha w + (w_i, H_i)$, with w and w_i as given above. □

Example 1. Let Π be the projective plane of order 3, i.e. $\Pi = PG_2(F_3)$. Let $W(x,y,z)$ be the complete weight enumerator of $Hull_3(\Pi)$. Using Theorem 4.4 we find that $W(x,y,z) = x^{13} + 78xy^6z^6 + 13x^4z^9 + 234x^4y^3z^6 + 234x^4y^6z^3 + 13x^4y^9 + 156x^7y^3z^3$. Let C' be the code as given in Corollary 3.1, with $v_1 = (1,1,0)$ and then $E = \langle C', w\rangle$ with $w = (1,2,1)$. Then E is a self-dual code of length 16 and $W_E(x,y,z) = (x^3 + y^2z + yz^2)W(x,y,z) + (xy^2 + xyz + xz^2)W(z,x,y) + (xz^2 + xy^2 + xyz)W(y,z,x)$.

We shall show how to construct other self-dual codes from the codes of a plane and how they are related to the self-dual codes already produced. We take Π to be a projective plane with p a prime sharply dividing n. Let α be any point in Π; let K_α be the code that is formed from $Hull_p(\Pi)$ by taking codewords that are 0 on the coordinate corresponding to α, and let G_α be K_α with the coordinate corresponding to α removed. That is, take the subcode of $Hull_p(\Pi)$ that is orthogonal to the vector $(0,0,\ldots,1,\ldots,0)$ where the 1 is in the coordinate corresponding to α to form K_α, and then disregard that coordinate to form G_α. The code G_α is the shortened code at α. Notice that G_α has length n^2+n, is self-orthogonal, and $\dim G_\alpha = \dim Hull_p(\Pi) - 1$. Denote the all one vector of length n^2+n by $\mathbf{j}$. Let $w = (1,1,\ldots,1,0,1,1,\ldots,1)$, i.e. w is $\mathbf{j}$ with a 0 in the coordinate corresponding to α. If $\mathbf{j} \in G_\alpha$ then $w \in Hull_p(\Pi)$. Take a line L of Π not incident with α, then $[w, L] = 1 \neq 0$ and so $w \notin Hull_p(\Pi)$ and then $\mathbf{j} \notin G_\alpha$. Let $G'_\alpha = \langle G_\alpha, \mathbf{j}\rangle$.

Theorem 3.5. *If* α *is any point in a projective plane* Π *of order n with p a prime sharply dividing n, then* G'_α *is a self-dual code of length* n^2+n.

Proof. G_α is a self-orthogonal code, and $[\mathbf{j},\mathbf{j}] = n^2+n = 0$ and the all one vector of length n^2+n+1 is in $Hull_p(\Pi)^\perp$ and so if a codeword in $Hull_p(\Pi)$

is 0 on the coordinate corresponding to α then it is orthogonal to $\mathbf{j}$. Hence G'_α is self-orthogonal and $\dim G'_\alpha = \dim G_\alpha + 1 = \dim Hull_p(\Pi) = \frac{n^2+n}{2}$, giving that G'_α is a self-dual code. □

For $p \equiv 1 \pmod 4$ or $p = 2$, with a the element of the field with $a^2 = -1$, then the matrix

$$\begin{pmatrix} 0 & 0 & M_{1,i} \\ 0 & 0 & M_{2,i} \\ 0 & 0 & M_{3,i} \\ \vdots & \vdots & \vdots \\ 0 & 0 & M_{\frac{n}{2}-1,i} \\ a & 1 & \mathbf{j} \\ 0 & 1 & v \end{pmatrix},$$

is the generator for the self-dual code C'. Note also that C' is the self-dual code formed from the shadows of the code G'_α. In the notation of [4], we have $C' = \Phi(G'_\alpha, v)$. Note that the second coordinate is the coordinate that was deleted from $Hull_p(\Pi)$ to form G_α.

For $p \equiv 3 \pmod 4$, if x, y are the elements of the field with $x^2 + y^2 = -1$ and a, b, c are the elements with $ax + by = 0$ and $a^2 + b^2 + c^2 = 0$ as in the proof of Corollary 3.1, then matrix

$$\begin{pmatrix} 0 & 0 & 0 & 0 & M_{1,i} \\ 0 & 0 & 0 & 0 & M_{2,i} \\ 0 & 0 & 0 & 0 & M_{3,i} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & M_{\frac{n}{2}-1,i} \\ x & y & 0 & 1 & \mathbf{j} \\ 0 & 0 & 0 & 1 & v \\ a & b & c & 0 & \mathbf{0} \end{pmatrix},$$

is the generator of E. Set $w = (a, b, c, 0, \ldots, 0)$ then in the notation of [4], $E = \Phi(G'_\alpha, v, w)$. That is, E is formed from the shadows of G_α with the vector w. Note that the fourth coordinate is the coordinate that was deleted from $Hull_p(\Pi)$ to form G_α.

Example 2. To continue Example 1, let G_α be the code formed from $Hull_3(PG_2(F_3))$ with α any point in the plane. Then $W_{G_\alpha}(x, y, z) = x^{12} + 84x^6y^3z^3 + 72x^3y^6z^3 + 72x^3y^3z^6 + 4x^3z^9 + 4x^3y^9 + 6y^6z^6$, and the self-dual code G'_α has complete weight enumerator $W_{G'_\alpha}(x, y, z) = W_{G_\alpha}(x, y, z) + W_{G_\alpha}(z, x, y) + W_{G_\alpha}(y, z, x)$.

4. Weight Enumerators of Codes of Projective Planes

We shall examine further the weight enumerators of the projective planes considered previously. The following two results can be found in [1]. We denote both the line and its characteristic function by L depending on the context.

Theorem 4.1. *Let Π be a projective plane of order n and let p be a prime dividing n. If k is the dimension of $C_p(\Pi)$, then $Hull_p(\Pi)^\perp$ is an $[n^2+n+1, n^2+n+2-k, n+1]$ code. The minimum weight vectors of $Hull_p(\Pi)^\perp$ are precisely the vectors of the form aL, where a is a non-zero scalar and L is the characteristic function of a line L in Π. Moreover, $Hull_p(\Pi) = \langle L - M \mid L$ and M are lines of $\Pi\rangle$ and*

$$C_p(\Pi) = \langle Hull_p(\Pi), \mathbf{j}\rangle,$$

where $\mathbf{j}$ is the all one vector.

Corollary 4.2. *For a plane Π of order n with p a prime dividing n, the minimum weight of $Hull_p(\Pi)$ is at least $n+2$.*

In addition, we know that if p sharply divides n, then $\dim C_p(\Pi) = \frac{n^2+n+2}{2}$ and then, by the previous theorem, we have that $C_p(\Pi) = Hull_p(\Pi)^\perp$.

We shall give restrictions on the possible weight enumerators of the codes of projective planes of order n over the finite field F_p, with p a prime dividing n.

Lemma 4.3. *Let Π be a projective plane of order n, with p a prime dividing n, where the complete weight enumerator of $Hull_p(\Pi)$ is given as:*

$$W_{Hull_p(\Pi)}(x_0, x_1, \ldots, x_{p-1}) = \sum A_{(a_0,a_1,\ldots,a_{p-1})} x_0^{a_0} x_1^{a_1} \cdots x_{p-1}^{a_{p-1}},$$

then the following conditions hold for all nonzero coefficients $A_{(a_0,\ldots,a_{p-1})}$:

(1) $\sum a_i = n^2+n+1$,
(2) $\sum i a_i \equiv 0 \pmod p$,
(3) $\sum i^2 a_i \equiv 0 \pmod p$,
(4) *if* $\sum_{i\neq 0} a_i \neq 0$ *then* $\sum_{i\neq 0} a_i \geq n+2$ *and*
(5) $A_{(a_0,a_1,\ldots,a_{p-1})} = A_{(a_{\alpha 0},a_{\alpha 1},\ldots,a_{\alpha(p-1)})}$ *for* $\alpha \in F_p$.

Proof. The first assertion follows immediately from the fact that the ambient space is $F_p^{n^2+n+1}$. We know $\mathbf{j} \in C_p(\Pi) \subseteq Hull_p(\Pi)^\perp$, and hence if $v \in Hull_p(\Pi)$ then $[v, \mathbf{j}] = 0$, giving the second assertion. $Hull_p(\Pi)$ is self-orthogonal which gives the third assertion. The fourth follows from Corollary 4.2, which states that the minimum weight is at least $n+2$. The fifth assertion is a consequence of the linearity of the code. □

Theorem 4.4. *Let Π be a projective plane of order n with p a prime sharply dividing n, where W_C and W_H represent the complete weight enumerator of $C_p(\Pi)$ and $Hull_p(\Pi)$ respectively, then for ω a p-th root of unity, we have:*

$$\begin{aligned} &W_C(x_0, x_1, \ldots, x_{p-1}) \\ &\quad = W_H(x_0, \ldots, x_{p-1}) + W_H(x_{p-1}, x_0, x_1, \ldots, x_{p-2}) \\ &\qquad\qquad + \cdots + W_H(x_1, x_2, \ldots, x_0) \\ &\quad = \frac{1}{|Hull_p(\Pi)|} W_H(x_0 + x_1 + \cdots + x_{p-1}, \\ &\qquad x_0 + \omega x_1 + \cdots + \omega^{p-1} x_{p-1}, \ldots, x_0 + \omega^{p-1} x_1 + \cdots + \omega x_{p-1}), \end{aligned}$$

and

$$\begin{aligned} & W_C(x,y,y,\ldots,y) \\ &= W_H(x,y,y,\ldots,y) + W_H(y,x,y,\ldots,y) + \cdots + W_H(y,y,\ldots,x) \\ &= \frac{1}{|Hull_p(\Pi)|} W_H(x+(p-1)y, x-y, x-y, \ldots, x-y). \end{aligned}$$

Proof. In the first statement the complete weight enumerator is calculated first by using the fact that $C_p(\Pi) = \langle Hull_p(\Pi), \mathbf{j} \rangle$, and second by using the MacWilliams relations for complete weight enumerators and the fact that for p sharply dividing n, we have $Hull_p(\Pi)^{\perp} = C_p(\Pi)$. The second statement does the same as the first except that it uses the MacWilliams equations for the Hamming weight enumerator instead of the complete weight enumerator. □

The value of the second part of the previous theorem is that the computation involved is substantially smaller. Even though the second part used the MacWilliams relations for Hamming weight enumerators, it still incorporates the coefficients of the complete weight enumerator; so that it is possible to obtain the complete weight enumerator using only the relations for the Hamming weight enumerator.

Lemma 4.5. *Let Π be a projective plane of order n, with p a prime dividing n, where the complete weight enumerator of $Hull_p(\Pi)$ is given as:*

$$W_{Hull_p(\Pi)}(x_0, x_1, \ldots, x_{p-1}) = \sum A_{(a_0,a_1,\ldots,a_{p-1})} x_0^{a_0} x_1^{a_1} \cdots x_{p-1}^{a_{p-1}}.$$

Suppose $A_{(a_0,\ldots,a_{p-1})} \neq 0$. Then each $a_i \leq n^2$, and if some $a_i = n^2$, then necessarily $i \neq 0$, $a_0 = n+1$ and $A_{(a_0,a_1,\ldots,a_{p-1})} = n^2 + n + 1$.

Proof. With p a prime dividing n, $C_p(\Pi) \subseteq Hull_p(\Pi)^{\perp}$ and hence the minimum weight of this code is $n+1$ and all minimum weight vectors are scalar multiples of lines, as proven in Theorem 4.1. Any monomial with an a_i greater than n^2 represents vectors v such that $v + \beta\mathbf{j}$ will have weight less than $n+1$ for some $\beta \in F_p$. In the second case if i were 0 it would represent a weight $n+1$ vector which is impossible. For $i \neq 0$, since $C_p(\Pi) = \langle Hull_p(\Pi), \mathbf{j} \rangle$ given a vector with $a_i = n^2$ for some $\beta \in F_p$, $v + \beta\mathbf{j}$ will have weight $n+1$ and hence this corresponds to a constant weight $n+1$ vector in $C_p(\Pi)$, making some $a_s = n+1$. If some $a_s = n+1$ and all others are 0, we know that $in^2 + s(n+1) \equiv 0 \pmod{p}$. Therefore since p divides n, $s = 0$. The last assertion follows from the fact that there are $n^2 + n + 1$ lines in Π. □

A projective plane Π is said to be **tame** at p if $Hull_p(\Pi)$ has minimum weight $2n$ and the minimum weight vectors are precisely the scalar multiples of the vectors of the form $L - M$ where L and M are lines of Π.

For a full explanation of the importance of the preceding definition as well as proofs of the results mentioned here see [1]. All desarguesian planes

are tame but there are planes that are not tame, for example the non-desarguesian translation plane of order 9 is not tame at 3. It is also conceivable that a plane is tame at one prime and not at another. The importance of this definition is that tame planes might possible provide a class of planes, containing the desarguesian planes that can be dealt with more easily.

Lemma 4.6. *Let* Π *be a projective plane of order* n *and* p *a prime dividing* n*, where the complete weight enumerator of* $Hull_p(\Pi)$ *is*

$$W_{Hull_p(\Pi)}(x_0, x_1, \ldots, x_{p-1}) = \sum A_{(a_0,a_1,\ldots,a_{p-1})} x_0^{a_0} x_1^{a_1} \cdots x_{p-1}^{a_{p-1}}.$$

The projective plane Π *is tame at* p *if and only if the following conditions hold:*

(1) *If* $0 < \sum_{i\neq 0} a_i < 2n$ *then* $A_{(a_0,a_1,\ldots,a_{p-1})} = 0$,
(2) *If* $\sum_{i\neq 0} a_i = 2n$ *then there exists* j *such that* $a_j = n$ *and* $a_{n-j} = n$ *and* $A_{(a_0,a_1,\ldots,a_{p-1})} = (n^2+n+1)(n^2+n)$ *for* $p \neq 2$ *and* $(n^2+n+1)(n^2+n)/2$ *for* $p = 2$*, and* $n \neq 2$*. If* $n = p = 2$ *then* $A_{(3,4)} = 7$.

Proof. It follows from the definition, noting that there are $(n^2 + n + 1)(n^2 + n)$ ways of choosing two lines when $j \neq n - j$, namely when p is odd, and $(n^2 + n + 1)(n^2 + n)/2$ ways of choosing two lines when $j = -j$, that is when $p = 2$. The case $n = 2$ is an anomaly because different differences of parallel lines can produce the same vector. □

The following computational approach is then used. Take a linear combination of all possible monomials satisfying the appropriate lemmas of this section with variable coefficients. This represents all possible weight enumerators of $Hull_p(\Pi)$ for any plane Π of a given order n. Apply Theorem 4.4 to this polynomial, and set these two polynomials equal. This gives a system of linear equations in the number of unknowns involved in the possible weight enumerators of the Hull. If this has no solution or if any possible solution has at least one value which is not a non-negative integer then no plane of this order can exist.

At $n = p = 2$ there is a unique solution. At $n = p = 3$ using either form of Theorem 4.4 there is a unique solution. Note that the complete weight enumerator of $C_3(PG_2(F_3))$ is obtained using only the Hamming weight enumerator relations and the complete weight enumerator is given in Example 1.

For $n = 6$, $p = 2$ or $p = 3$ there is no solution to the system of equations. With $n = 10$, $p = 2$ there is a solution with three degrees of freedom, which is well know to be the case for possible weight enumerators of planes of order 10. If one assumes that the plane of order 10 is tame then the weight enumerator has both negative and non-integer coefficients and hence a plane of order 10 (known not to exist) could not be tame at 2. Note that no combinatorial information was needed to rule out a tame plane of order 10.

REFERENCES

[1] Assmus, Jr., E.F., Key, J.D., Designs and their codes. Cambridge: Cambridge University Press 1992.
[2] Assmus, Jr., E.F., Maher, D.P., Nonexistence proofs for projective designs. Amer. Math. Monthly **85**, 110–112 (1978).
[3] Bruck, R.H., Ryser H.J., The nonexistence of certain finite projective planes. Canadian J. Math. **1**, 88–93 (1949).
[4] Dougherty, S.T., Shadow codes and weight enumerators. IEEE Trans. Inform. Theory **41**, 762–768 (1995).
[5] Hall, Jr., M., Configurations in a plane of order 10. *Ann. Discrete Math.* **6**, 157–174 (1980).
[6] Hall, Jr., M., Combinatorial theory (2nd ed.). New York: Wiley 1986.
[7] Klemm, M., Über den p-Rang von Inzidenzmatrizen. J. Combin. Theory Ser. A **51**, 138–139 (1986).
[8] Lam, C.W.H., The search for a finite projective plane of order 10. Amer. Math. Monthly **98**, 305–318 (1991).
[9] MacWilliams, F.J., Sloane, N.J.A., The theory of error-correcting codes. Amsterdam: North-Holland 1983.
[10] Ott, U., An elementary introduction to algebraic methods for finite projective planes. *Seminario di Geometrie Combinatorie* **50** (1984).
[11] Pless, V., Symmetric designs and self-dual codes. Alg. Groups and Geom. **3**, 355–364 (1985).

STEVEN T. DOUGHERTY
DEPARTMENT OF MATHEMATICS
UNIVERSITY OF SCRANTON
SCRANTON, PA 18510
USA

(*Received February 2, 1999*)