The construction of self-dual binary codes from projective planes of odd order

DAVID G. GLYNN*

Department of Mathematics
University of Canterbury

Abstract. Every finite projective plane of odd order q has an associated self-dual binary code with parameters $(2(q^2+q+1), q^2+q+1, 2q)$. We also construct other related self-orthogonal and doubly-even codes, and classify the vectors of minimum weight. The weight enumerator polynomials for the planes of orders 3 and 5 are found. The boundary and coboundary maps are introduced.

1. Binary Codes from Projective Planes

The references [7] and [8] should be of help for non-experts in the field of error-correcting codes, while [5] and [6] contain much of the basic theory of finite projective planes. Let us denote a given projective plane of odd order q by π. A *binary code* $\mathcal{C}$ with parameters (n, m, d) is a subspace of dimension m of the vector space of dimension n over the finite field GF(2), such that the minimum weight of any non-zero vector of $\mathcal{C}$ is d, which is called the *distance* of the code. The *weight* of a vector (or *word*) of the code is the number of non-zero entries. We also denote the *orthogonal* (or *dual*) code of a binary code $\mathcal{C}$ by $\mathcal{C}^\perp$. A code $\mathcal{C}$ is said to be *self-orthogonal* if it is contained in $\mathcal{C}^\perp$, while it is called *self-dual* if $\mathcal{C} = \mathcal{C}^\perp$. In the latter case, such a code is of type $(n, n/2, d)$. There is a construction of such a code with parameters $(q^2+q+2, (q^2+q+2)/2, q+2)$ from any projective plane of order $q \equiv 2 \pmod 4$. However, it is not the same as the construction of the present paper, because here we deal only with planes of *odd* order. Let us agree to use the word *dual* to mean the point to line and line to point transformation of the plane taking the projective plane to its "geometrical" dual. Of course, *self-dual* can still take on its usual meaning for codes.

Before investigating the codes associated with π it is useful to define two mappings ∂ and δ, the *boundary* and *coboundary* mappings respectively. These mappings have been used by Glynn and Steinke [4] to define *generalised projectivities* of π.

DEFINITION. *If S is any subset of points of π, the coboundary of S, denoted by δS, is the set of lines that intersect S in an odd number of points, if $|S|$ is even, or an even number of points, if $|S|$ is odd. Similarly, if T is any subset of lines of π, the boundary of T, denoted by ∂T, is the set of points that are incident with an odd number of lines of $|T|$, if $|T|$ is even, or an even number of lines, if $|T|$ is odd.*

Let P and L denote the sets of points and lines respectively of π. Thus $|P| = |L| = q^2+q+1$, where q is the order of π. Associated with the boolean algebra of all

*This research was supported by a grant from the University of Canterbury.

subsets of $P \cup L$ is a vector space V of dimension $2(q^2+q+1)$ over $GF(2)$. We shall construct our codes in V. Addition in V is equivalent to the set-theoretic operation of symmetric difference Δ. Thus if E and F are subsets of $P \cup L$, E and F are also vectors in V, or words in the code which is V, and $E+F$ is the same as $E \Delta F$. The weight of a word of V is the same as its size as a subset of $P \cup L = P + L$. Finally, if x is a point or line of π let $\hat{x}$ denote the word of V that corresponds to the set of lines or points incident with x in π.

NOTE. *Here we leave some simple combinatorial exercises that are important for the following constructions.*

(1) $\partial = \delta^{-1}$;
(2) $\delta(R+S) = \delta R + \delta S, \forall R,\ S \subseteq P$;
(3) $\partial(U+V) = \partial U + \partial V, \forall U,\ V \subseteq L$;
(4) $|R| + |\delta R| \equiv 0 \pmod 2, \forall R \subseteq P$;
(5) $|U| + |\partial U| \equiv 0 \pmod 2, \forall U \subseteq L$;
(6) $\delta x = L + \hat{x},\ \partial \hat{x} = P + x,\ \forall x \in P$;
(7) $\partial y = P + \hat{y},\ \delta \hat{y} = L + y,\ \forall y \in L$;
(8) $\delta P = L,\ \partial L = P$.

Thus we see that δ and ∂ are non-singular, linear mappings from the code of all subsets of P to L and vice-versa. Also, the same holds for the restriction of δ and ∂ to the codes of all even subsets of P and L.

For example, in (1) above if we fix the natural bases of points and lines for the two subcodes of V corresponding to these sets, then δ corresponds to the linear mapping with matrix that is the complement $J - M$ of the incidence matrix M of π, and ∂ corresponds to the transpose M^t of M, where J is the matrix of all 1's. Thus (1) corresponds to the fact that $(J-M)(J-M)^t \equiv I \pmod 2$. Since $MM^t = J + qI \equiv J + I$, $MJ = JM = (q+1)I \equiv 0$, and $J^2 = (q^2+q+1)J \equiv J \pmod 2$, we see that $J - M$ is in fact an orthogonal matrix modulo 2.

Note also that the constructions of this paper can be generalised to certain symmetric (v, k, λ) designs that have an incidence matrix which is orthogonal modulo 2. This is the case when the parameter λ is even, and k is odd. The complementary design of the projective plane is a symmetric (q^2+q+1, q^2, q^2-q) design, and so it satisfies these conditions. The self-dual code (corresponding to $\mathcal{C}_B$ below) has a generating matrix that is made up of the identity matrix side-by-side with the incidence matrix of the design.

THEOREM 1.1. *Associated with π are three codes $\mathcal{C}_A \subset \mathcal{C}_B \subset \mathcal{C}_A^{\perp}$. $\mathcal{C}_A$ is self-orthogonal and $\mathcal{C}_B$ is self-dual.*

PROOF: First let $\mathcal{C}_A$ be the set of all even sets of points of P, together with the sets of lines that intersect those points in an odd number. Thus

$$\mathcal{C}_A := \{S + \delta S \mid S \subseteq P,\ |S| \equiv 0 \pmod 2\}.$$

Equivalently, one could define this code as the set of all even sets of lines of L, together with the sets of points on an odd number of those lines. Thus

$$\mathcal{C}_A := \{T + \partial T \mid T \subseteq L,\ |T| \equiv 0 \pmod 2\}.$$

$\mathcal{C}_A$ is a code because it is closed under addition. Thus

$$(S_1 + \delta S_1) + (S_2 + \delta S_2) = (S_1 + S_2) + \delta(S_1 + S_2), \ \forall S_1, \ S_2 \subseteq P.$$

It is easy to see that the dimension of $\mathcal{C}_A$ is $q^2 + q$, because this is the dimension of the code of sets of even size in P.

Next we form the orthogonal code $\mathcal{C}_A^\perp$ of all vectors in V orthogonal to those in $\mathcal{C}_A$. This gives a subcode of V of dimension $q^2 + q + 2$. One can easily see that it has a basis in V consisting of the $q^2 + q + 1$ words of weight $q + 2$ given by $m + \hat{m}$, where $m \in L$. In addition one can adjoin the word of all $q^2 + q + 1$ points P to get the basis. Now the words

$$m + n + \partial(m + n) = m + n + \hat{m} + \hat{n} = (m + \hat{m}) + (n + \hat{n})$$

generate $\mathcal{C}_A$ when we vary m and n in L. Thus $\mathcal{C}_A$ is contained in $\mathcal{C}_A^\perp$, and so is self-orthogonal. Since $\mathcal{C}_A$ is also a subgroup of index 4 in $\mathcal{C}_A^\perp$, when considered as an additive group, it has 4 cosets. These are: $\mathcal{C}_A$, $\mathcal{C}_A + P$, $\mathcal{C}_A + L$, $\mathcal{C}_A + P + L$. If we take the subgroups of dimension $q^2 + q + 1$ formed by unions of these cosets, we obtain three codes of which one is self-dual. It is the code $\mathcal{C}_B := \mathcal{C}_A \cup (\mathcal{C}_A + P + L)$, which is made up of all the words of $\mathcal{C}_A$, and their complements in $P + L$. These complements are all of the form $S + \delta S$, where $|S|$ is odd, $S \subseteq P$, because $|S + P|$ would then be even, and because $(S + P) + \delta(S + P) + P + L = S + \delta S$.

THEOREM 1.2.

(1) *Each word of $\mathcal{C}_A$ has weight divisible by 4. (Thus $\mathcal{C}_A$ is a doubly-even self-orthogonal code.)*
(2) *Each word of the coset $\mathcal{C}_B \setminus \mathcal{C}_A$ has weight $\equiv 2 \pmod 4$.*
(3) *Each word of the cosets $\mathcal{C}_A + P$ and $\mathcal{C}_A + L$ has weight $\equiv -q \pmod 4$.*

PROOF:

(1) Each word of $\mathcal{C}_A$ is of the form $S + \delta S$, where S is a subset of P and $n := |S|$ is even. Let there be λ_i lines of L intersecting S in i points. Then by counting flags and pairs of points of S on lines one has that $\sum_i i\lambda_i = (q + 1)n$, and that $\sum_i \binom{i}{2}\lambda_i = \binom{n}{2}$. Hence it follows that $\sum_i i^2\lambda_i = n(n + q)$ and so $n + \sum_{i \ odd} \lambda_i \equiv n(n + q + 1) \pmod 4$. Thus the weight of $S + \delta S$ is divisible by 4, since n is even and q is odd.
(2) The words of $\mathcal{C}_B \setminus \mathcal{C}_A$ are all complements of words of A. Since $|P + L| = 2(q^2 + q + 1) \equiv 2 \pmod 4$ the result follows from (1).
(3) Consider a word $S + P + \delta S$ of the coset $\mathcal{C}_A + P$, where $|S|$ is even. From part (1) $|S + \delta S| \equiv 0 \pmod 4$. But $q^2 + q + 1 \equiv -q \pmod 4$ and so

$$|S + P + \delta S| = |P| - |S| + |\delta S| \equiv |P| + |S| + |\delta S| \equiv -q \pmod 4,$$

since $S + P = P \setminus S$ and $|S|$ is even. The other coset is shown similarly.

N.B. These codes do not depend on whether the plane or its dual are taken, so that if a statement is made about points it can also be made about lines. For example, every word of $\mathcal{C}_A$ is given by an even set of lines and the lines intersecting it in an odd number of points. Dually, every word of $\mathcal{C}_A$ is also given by an even set of lines and the points which are on an odd number of those lines.

THEOREM 1.3. *The minimum distances of $\mathcal{C}_A$, $\mathcal{C}_B$ and $\mathcal{C}_A^{\perp}$ are at least $2q+2$, $2q$, and $q+2$ respectively.*

PROOF: If there was a non-zero word of $\mathcal{C}_A$ of weight less than $2q+2$ we would have that the number of points and/or lines would be less than $q+1$. Since everything we say about the code $\mathcal{C}_A$ also holds for the dual plane, let us assume that a minimal word of $\mathcal{C}_A$ is of type $S+\delta S$, where S is a set of n points,with n even and $2 \leq n < q+1$. Then at each point of S there are at least $q+2-n$ tangents, and so the number of lines belonging to δS is at least $n(q+2-n)$. Hence $|S+\delta S| \geq n(q+3-n)$. Since $2(q+1)-n(q+3-n) = (n-2)(n-(q+1)) \leq 0$, it follows that the minimum distance of $\mathcal{C}_A$ is least $2q+2$.

Now consider the code $\mathcal{C}_B = \mathcal{C}_A \cup (\mathcal{C}_A + P + L)$ and in particular the words of the coset $\mathcal{C}_A + P + L$. Such a word is given by $S+\delta S$, where $S \subseteq P$ and $n := |S|$ is odd. We can assume that $n \leq q$. There will be external lines to S, and each external line will be in δS. The main fact is that there will be at least $q.(q+1-|S|)$ external lines, the minimum occurring when the points of S are collinear. (We leave this as a simple exercise.) Thus $|S+\delta S| \geq n+q.(q+1-n)$. But $n+q(q+1-n)-2q = (q-1)(q+1-n) \geq 0$, and this proves that the minimum distance of $\mathcal{C}_B$ is least $2q$, since the minimum distance of $\mathcal{C}_A$ is greater than this.

Finally, consider the code $\mathcal{C}_A^{\perp}$ and in particular the coset $\mathcal{C}_A + L$. A word of this coset is given by $S+\delta S+L$, where $S \subseteq P$ and $n := |S|$ is even. Suppose that $n < q+1$. Then all external lines to S are in $\delta S + L$. But there are at least $q(q+1-n) \geq 2q$ of these, so we can exclude this case. Thus $n \geq q+1$. If $n \geq q+2$ then the weight of the word is at least $n \geq q+3$, since n is even. When $n = q+1$, the size of $\delta S + L$ is at least 1, and so the weight of the word is at least $q+2$. Our argument for the coset $\mathcal{C}_A + P$ is dual to this.

Now let us list the words of minimal weight in the three codes, so that the minimal distances of the codes are determined. The proofs are not hard and are very similar to the analysis of Theorem 1.3, so we omit them.

THEOREM 1.4. *The minimal words of $\mathcal{C}_A$ of weight $2q+2$ are of three types:*

(1) *$u+v+\hat{u}+\hat{v}$, where u and v are distinct points of P;*
(2) *$m+n+\hat{m}+\hat{n}$, where m and n are distinct lines of L;*
(3) *the union of an oval (or $(q+1)$-arc) and its set of tangent lines (a dual oval).*

N.B. The first two words above are dual to one another, while the last is "self-dual", in the geometrical sense. There are $\binom{q^2+q+1}{2}$ words of each type (1) and (2), while the number of ovals depends on the projective plane and is not given by any known function of q, except for $q^5 - q^2$ in the Desarguesian case where π is $PG(2,q)$.

THEOREM 1.5. *The minimal words of $\mathcal{C}_B$ of weight $2q$ are given by $u+v+\hat{u}+\hat{v}$, for flags (u,v) of π, where $u \in P$, $v \in L$, u is incident with v. Note that $u+\hat{v}$ is an odd set of q points, and that*

$$\delta(u+\hat{v}) = \delta u + \delta\hat{v} = (L+\delta u)+(L+\delta\hat{v}) = \hat{u}+v.$$

(See the previous Note, parts (6) and (7).) There are $(q^2+q+1)(q+1)$ such words.

THEOREM 1.6. *The minimal words of $\mathcal{C}_A^{\perp}$ of weight $q+2$ correspond to the words $u+\hat{u}$ where u is a point or line of π. There are $2(q^2+q+1)$ such words.*

EXAMPLE 1.1. *Any pair of ovals (i.e. $(q+1)$-arcs) of π intersect in an even total of points and tangents.*

PROOF: $\mathcal{C}_A$ is self-orthogonal, and so any pair of words of $\mathcal{C}_A$ intersect in an even number of elements. It is easy to check that an oval and its set of tangents is a word (of weight $2q+2$) of the code $\mathcal{C}_A$, because an oval has $q+1$ points, which is even, and the lines intersecting the oval in an odd number of points are just the tangents.

EXAMPLE 1.2. *Let q be a perfect odd square. Then a Baer subplane of π gives a word of $\mathcal{C}_B$ of weight $2(q+\sqrt{q}+1)$. A unital gives a word of $\mathcal{C}_A$ of weight $2(q\sqrt{q}+1)$. These words, together with the oval-words of Example 1.1, pairwise intersect in even numbers of elements.*

PROOF: For the definitions and basic properties of Baer subplanes and unitals see [5] or [6]. To construct the word from a Baer subplane first note that it has an odd number of points. Then the lines intersecting it in an even number are just the lines of the Baer subplane ... they intersect in $\sqrt{q}+1$ points. Thus we get a word of $\mathcal{C}_B$ of the given weight. To construct the word from a unital first note that it has an even number of points. Then the lines intersecting it in an odd number are just the tangents of the unital ... all other lines intersect in $\sqrt{q}+1$ points. Thus we get a word of $\mathcal{C}_A$ of the given weight. All these words from ovals, Baer subplanes and unitals belong to $\mathcal{C}_B$, which is self-dual, so that they pairwise intersect in an even number of elements.

Finally, let us summarize the results of this section with the *main theorem.*

THEOREM 1.7. *The code $\mathcal{C}_A$ of a projective plane π of odd order is a doubly-even self-orthogonal $(2(q^2+q+1), q^2+q, 2q+2)$ binary code. The code $\mathcal{C}_B$ is a self-dual $(2(q^2+q+1), q^2+q+1, 2q)$ binary code that contains $\mathcal{C}_A$ as a subcode. The code $\mathcal{C}_A^{\perp}$ is a $(2(q^2+q+1), q^2+q+2, q+2)$ binary code.*

2. Weight Enumerator Polynomials

The weight enumerator polynomial of a code in n-dimensional vector space is defined to be the homogeneous polynomial in x and y of degree n such that the coefficient of $x^{n-j}y^j$ is the number of code-words of weight j.

THEOREM 2.1. *The weight enumerator polynomial for the self-dual code $\mathcal{C}_B$ of the projective plane of order 3 is given by:*

$$x^{26}+52x^{20}y^6+390x^{18}y^8+1313x^{16}y^{10}+2340x^{14}y^{12}+2340x^{12}y^{14}$$
$$+1313x^{10}y^{16}+390x^8y^{18}+52x^6y^{20}+y^{26}$$

PROOF: By Gleason's theorem (see [8]), a self-dual code has a weight enumerator polynomial that is made up of the two polynomials $a(x,y) = x^2 + y^2$ and $b(x,y) = x^8 + 14x^4y^4 + y^8$. Hence the polynomial $W(x,y)$ for the $(26,13,6)$ code of the projective plane of order 3 is given by

$$W(x,y) = \alpha a^{13} + \beta a^9 b + \gamma a^5 b^2 + \delta a b^3,$$

for some rational numbers α, β, γ and δ. Let W_i be the coefficient of $x^{26-i}y^i$ in $W(x,y)$ ... it is the number of code-words of weight i in $\mathcal{C}_B$. Since we know the coefficients $W_0 = 1$, $W_2 = W_4 = 0$, $W_6 = 52$, we can solve the linear equations uniquely and obtain $\alpha = -23/16$, $\beta = 13/8$, $\gamma = 13/16$ and $\delta = 0$. Substituting these in the equation for $W(x,y)$ gives the code distribution above.

THEOREM 2.2. *The weight enumerator polynomial for the self-dual code $\mathcal{C}_B$ of the projective plane of order 5 is given by:*

$$\begin{aligned}
&x^{62} + 186y^{10}x^{52} + 4030y^{12}x^{50} + 16275y^{14}x^{48} + 259625y^{16}x^{46} \\
&+ 1775990y^{18}x^{44} + 8492450y^{20}x^{42} + 31874200y^{22}x^{40} + 90578280y^{24}x^{38} \\
&+ 195332612y^{26}x^{36} + 325217900y^{28}x^{34} + 420190275y^{30}x^{32} \\
&+ 420190275y^{32}x^{30} + 325217900y^{34}x^{28} + 195332612y^{36}x^{26} \\
&+ 90578280y^{38}x^{24} + 31874200y^{40}x^{22} + 8492450y^{42}x^{20} + 1775990y^{44}x^{18} \\
&+ 259625y^{46}x^{16} + 16275y^{48}x^{14} + 4030y^{50}x^{12} + 186y^{52}x^{10} + y^{62}
\end{aligned}$$

PROOF: The number of words in $\mathcal{C}_B$ of weights 0, 2, 4, 6, 8, 10, and 12 are 1, 0, 0, 0, 0, 186, and 4030 respectively. The number 186 comes from the classification of words of weight $2q$ coming from flags, since the number of flags is $(q^2+q+1)(q+1) = 31.6 = 186$. And the number 4030 comes from the knowledge that the number of ovals in the plane is $q^5 - q^2$ because the plane of order 5 is desarguesian. (See [9] for the classification of ovals.) To this one must add the number of pairs of points and the number of pairs of lines, which always sum in any projective plane of order q to $(q^2+q+1)(q^2+q)$. Thus the total number of words in $\mathcal{C}_B$ of weight $2q+2$ for a desarguesian projective plane of order q is $(q^2+q+1)(q^3+q)$, which is $31.130 = 4030$ in this case. The number of words of weight 14 (= 2q+4) is harder to calculate. However it can be found that there are two types of configuration of points corresponding to this weight, both with 7 points and 7 lines: each anti-flag (point not on a line), and also each 4-arc together with the set of 3 'diagonal points' on the intersections of 2 chords of the arc. (A word of weight $2q+4$ must be in the coset $\mathcal{C}_A + P + L$ and so consists of an odd set of points and the set of lines intersecting it evenly.) Counting the number of anti-flags (= 31.25) and adding the number of 4-arcs (= 31.30.25.16/4!) gives us 775 + 15500 = 16275. Table 4.8 of [3] was useful in finding and classifying these words of weight 14. Finally, we can find the polynomials of Gleason's theorem by solving a set of linear equations in 8 variables. In fact $256W(x,y)$

$= 101a^{31} - 155a^{27}b + 682a^{23}b^2 - 2666a^{19}b^3 + 2821a^{15}b^4 - 651a^{11}b^5 + 124a^7b^6 + 0a^3b^7.$

3. New Codes From Old

Every singly-even self-dual code can be extended to a doubly-even self-dual code by a method known as 'glueing', which is explained in the paper by Conway and Pless [2]. We now explain how this is done in the special case of the projective plane code $\mathcal{C}_B$.

THEOREM 3.1. *If $q \equiv 1 \pmod 4$ the self-dual code $\mathcal{C}_B$ can be extended to a unique doubly-even self-dual code $\mathcal{C}_D$ with parameters $(2(q^2+q+2), q^2+q+2, q+3)$.*

PROOF: Let us add two basis elements ∞ and ∞' to the set of basis elements $P \cup L$. Now extend the code $\mathcal{C}_A^{\perp}$, which is of the dimension needed. By

(1) setting words of $\mathcal{C}_A$ to be also zero on ∞ and ∞',
(2) setting words of $\mathcal{C}_A + P$ to be one on ∞ and zero on ∞',
(3) setting words of $\mathcal{C}_A + L$ to be zero on ∞ and one on ∞',
(4) setting words of $\mathcal{C}_A + P + L$ to be one on ∞ and one on ∞',

we obtain the code $\mathcal{C}_D$. From Theorem 1.2 every code-word has weight divisible by 4. Also, it is easy to check that every pair of code-words of $\mathcal{C}_D$ are orthogonal. The minimum weight of $\mathcal{C}_D$ is $q+3$ because the minimum weight of $\mathcal{C}_A + P$ and $\mathcal{C}_A + L$ is $q+2$, and the weight increases by 1 when we construct $\mathcal{C}_D$. The minimum weight of non-zero words in $\mathcal{C}_A$ is $2q+2$, and these stay the same in $\mathcal{C}_D$, while the minimum weight of words in $\mathcal{C}_A + P + L$ is $2q$, and these weights increase by 2 in $\mathcal{C}_D$.

THEOREM 3.2. *If $q \equiv 3 \pmod 4$ the self-dual code $\mathcal{C}_B$ can be extended to a doubly-even self-dual code $\mathcal{C}_E$ with parameters $(2(q^2+q+4), q^2+q+4, 4)$.*

PROOF: Let us add 6 basis elements to the set of basis elements $P \cup L$. Let D_6 be the (6,2,4) code on the new basis of size 6 generated by (110011) and (001111). From words w in the 4 different cosets of $\mathcal{C}_A$ in $\mathcal{C}_A^{\perp}$ we create new cosets of D_6.

(1) If $w \in \mathcal{C}_A$ we just add D_6;
(2) if $w \in \mathcal{C}_A + P$ we add $(010101) + D_6$;
(3) if $w \in \mathcal{C}_A + L$ we add $(010110) + D_6$;
(4) if $w \in \mathcal{C}_A + P + L$ we add $(000011) + D_6$.

In this case the code obtained has distance 4, because the zero code-word of $\mathcal{C}_A$ is added to D_6 to produce 4 words, three of which have weight 4.

NOTE. *The automorphism groups of the two extended codes $\mathcal{C}_D$ and $\mathcal{C}_E$ are the same as the codes $\mathcal{C}_A$, $\mathcal{C}_B$ and $\mathcal{C}_A^{\perp}$, which are isomorphic to the group of all collineations and correlations of the plane. One can see this from the classification of the minimal weight words of $\mathcal{C}_A$, $\mathcal{C}_B$ and $\mathcal{C}_A^{\perp}$ given in Theorems 1.4–6.*

EXAMPLES. *By Gleason's theorem every self-dual doubly-even binary code has a weight enumerator polynomial made up of the two polynomials*

$$b(x,y) = x^8 + 14x^4y^4 + y^8$$

and

$$c(x,y) = x^{24} + 759x^{16}y^8 + 2576x^{12}y^{12} + 759x^8y^{16} + y^{24}.$$

We can use this fact to calculate the polynomials for the codes C_D and C_E of small projective planes.

(1) The projective plane of order 3 gives a self-dual doubly-even code with parameters (32,16,4), which has 3 words of weight 4. In table III of [2], it is referred to by $d_6 + (2f_{13})$. Its weight enumerator polynomial is given in table IV of [2] by

$$x^{32} + 3x^{28}y^4 + 650x^{24}y^8 + 13741x^{20}y^{12} + 36746x^{16}y^{16} + 13741x^{12}y^{20} + 650x^8y^{24} + 3x^4y^{28} + y^{32}.$$

(2) The projective plane of order 5 gives a self-dual doubly-even code with parameters (64,32,8), which has 62 words of weight 8. The calculation of its weight enumerator polynomial can be left as an exercise.

4. Conclusions

The methods of coding theory are being applied with increasing frequency to finite geometry while the knowledge of geometry can lead to codes which have more of their properties specified than with purely algebraic constructions. Hopefully this paper will bring this class of projective geometry codes to the readers' attention, and that new results in both areas will arise.

References

1. P.J. Cameron and J.H. van Lint, "Graphs, Codes and Designs," London Math. Soc. Lecture Note Series Vol. **43**, Cambridge University Press, Cambridge, 1980.
2. J.H. Conway and Vera Pless, *On the enumeration of self-dual codes*, J. Combin. Th. Series A **28** (1980), 26–53.
3. D.G. Glynn, *Rings of geometries II*, J. Combin. Th., Series A **49** (1988), 26–66.
4. D.G. Glynn and G.F. Steinke, *Groups of generalised projectivities in projective planes of odd order*, preprint.
5. J.W.P. Hirschfeld, "Projective Geometries over Finite Fields," Oxford Uni. Press, Oxford, 1979.
6. D.R. Hughes and F.C. Piper, "Projective Planes," Springer, New York, Heidelberg, Berlin, 1973.
7. F.J. MacWilliams and N.J.A. Sloane, "The Theory of Error-Correcting Codes," North-Holland, Amsterdam, New York, Oxford, 1977.
8. V. Pless, "Introduction to the Theory of Error-Correcting Codes," Wiley, New York, 1982.
9. B. Segre, *Sulle ovali nei piani lineari finiti*, Atti Accad. Naz. Lincei Rend **17** (1954), 1–2.

1980 *Mathematics subject classifications*: 51E15, 51E20, 05B25, 94B05, 11T71