DUAL CODES OF TRANSLATION PLANES

K. L. Clark
Department of Mathematics
University of Virginia
Charlottesville VA 22904, U.S.A.

J. D. Key[1]
Department of Mathematical Sciences
Clemson University
Clemson SC 29634, U.S.A.

M. J. de Resmini
Dipartimento di Matematica
Universitá di Roma 'La Sapienza'
I-00185 Rome, Italy

October 25, 2002

[1]Support of NSF grant #9730992 and ONR grant #N00014-00-1-0565 acknowledged

Abstract

We improve on the known upper bound for the minimum weight of the dual codes of translation planes of certain orders by providing a general construction of words of small weight. We use this construction to suggest a possible formula for the minimum weight of the dual p-ary code of the desarguesian plane of order p^m for any prime p and any $m \geq 1$.

1 Introduction

Early in the study of codes associated with finite projective planes it was shown that the p-ary code of a projective plane of order n, where p is a prime dividing n, has minimum weight $n+1$ and the codewords of minimum weight are the scalar multiples of the incidence vectors of the lines (see [2, Chapter 6] for discussion of these results). For the dual code, neither the minimum weight nor the nature of the possible minimum words is known in the general case, even though these are the codes that are most useful in applications since they can be decoded using majority logic decoding (see [12]). Various bounds can be established, and for some particular classes precise results are known. In particular, for desarguesian planes of even order $q = 2^m$, where $p = 2$, the minimum weight is $q + 2$ and the minimum words are the incidence vectors of the hyperovals, which always exist in the desarguesian planes. See [9] for other results in the even case, and for instances when the plane has no hyperoval. In the latter case, again the minimum weight is not known except in some particular cases.

When p is an odd prime, even for the desarguesian planes the minimum weight of the dual code is not in general known, except for the case when the order is prime, in which case the minimum weight is $2p$. Some bounds have been found for p odd in Sachar [15] and in Clark and Key [6]: see the results quoted in Section 2. In this paper we obtain the following theorem, which implies some improved bounds for some translation planes of odd order:

Theorem 1 *Let Π be a projective translation plane of order q^m and kernel containing F_q, where $m = 2$ or 3, $q = p^t$, and p is a prime. Then the dual code of the p-ary code of Π has minimum weight at most $2q^m - (q^{m-1} + q^{m-2} + \cdots + q)$. If Π is desarguesian, this also holds for $m = 4$.*

We give the construction that leads to this result in Section 3. If this construction could be shown to be valid for translation planes of order q^m for any $m \geq 2$, then we would have a general upper bound for the minimum weight of $2q^m - (q^{m-1} + \cdots + q)$. In fact, for the desarguesian plane of order p^m, where p is a prime, in all cases where the minimum weight of the dual p-ary code is known, and in particular for $p = 2$, or for $m = 1$, the minimum weight is precisely as given in this formula, i.e. $2p^m - (p^{m-1} + p^{m-2} + \cdots + p)$. This suggests that this formula might hold for all p and m. We pose this as a question:

Question 1 *Is the minimum weight of the dual code of the p-ary code of the desarguesian plane of order p^m given by the formula*

$$2p^m - (p^{m-1} + p^{m-2} + \cdots + p) = 2p^m + 1 - \frac{p^m - 1}{p - 1}$$

for all primes p and all $m \geq 1$?

The other odd orders for which the minimum weight is known in the desarguesian case are $q = 9$ (see [10]) and $q = 25$ (see [5]). The discussion in the paragraph immediately following Result 3 has more details of these cases. See also Section 4 for further discussion on this issue. We note that there is some evidence to support this observation for translation planes in general, and not just for the desarguesian planes, but very little is known about the codes of these planes.

In Section 2 we give the background results, in Section 3 we prove the theorem, and in Section 4 we give some other possible constructions of codewords in the dual code.

2 Background and terminology

An incidence structure $\mathcal{D} = (\mathcal{P}, \mathcal{B}, \mathcal{I})$, with point set $\mathcal{P}$, block set $\mathcal{B}$ and incidence $\mathcal{I}$, is a t-(v, k, λ) design if $|\mathcal{P}| = v$, every block $B \in \mathcal{B}$ is incident with precisely k points, and every t distinct points are together incident with precisely λ blocks. A 2-$(n^2 + n + 1, n + 1, 1)$ design, for $n \geq 2$, is a finite projective plane of order n. We write $PG_{2,1}(F_q)$ for the desarguesian projective plane, i.e. the design of points and 1-dimensional subspaces of the projective space $PG_2(F_q)$. Further, $AG_{m,n}(F_q)$ will denote the 2-design of points and n-flats (cosets of dimension n) in the affine geometry $AG_m(F_q)$. If $\mathcal{S}$ is a set of points in a plane and if L is a line of the plane that meets $\mathcal{S}$ in m points, then L will be called an **m-secant** to $\mathcal{S}$. The set $\mathcal{S}$ is an $(n_1, \ldots, n_r)$-set if $\mathcal{S}$ has m-secants if and only if $m \in \{n_1, \ldots, n_r\}$.

A **linear code** of length n over a finite field F is any subspace of the vector space F^n. The **code** C_F, or $C_F(\mathcal{D})$, of the design $\mathcal{D}$ over the finite field F is the space spanned by the incidence vectors of the blocks over F. We take F to be a prime field F_p where the prime must divide the order of the design. If the point set of $\mathcal{D}$ is denoted by $\mathcal{P}$ and the block set by $\mathcal{B}$, and if $\mathcal{Q}$ is any subset of $\mathcal{P}$, then we will denote the incidence vector of $\mathcal{Q}$ by $v^{\mathcal{Q}}$. Thus $C_F(\mathcal{D}) = \langle v^B \mid B \in \mathcal{B} \rangle$, and is a subspace of $F^{\mathcal{P}}$, the full vector space of functions from $\mathcal{P}$ to F. For any code C, the **dual** or **orthogonal** code

$C^\perp$ is the orthogonal subspace with respect to the standard inner product. Thus $C^\perp = \{u \in F^{\mathcal{P}} | (u, c) = 0 \text{ for all } c \in C\}$. If c is a codeword then the **support** of c is the set of non-zero coordinate positions of c. The **weight** of c is the cardinality of the support. The **minimum weight** of a code C is the smallest non-zero weight of the words in C. If a linear code over a field of order q is of length n, dimension k, and minimum weight d, then we write $[n, k, d]_q$ to show this information. A **constant word** in the code is a codeword, all of whose coordinate entries are either 0 or 1.

The current state of knowledge of the minimum weight of the dual code of a projective plane in the odd-order case is summed up in the following results. The first is a special case for the desarguesian geometries and can be found discussed in [2, Theorem 5.7.9]:

Result 1 *Let C be the p-ary code of the desarguesian plane $PG_{2,1}(F_q)$ or $AG_{2,1}(F_q)$ where $q = p^t$ and p is prime. Then the minimum weight $d^\perp$ of $C^\perp$ satisfies*

$$(q + p) \leq d^\perp \leq 2q.$$

Note that a similar range holds for any projective plane: if Π is a plane of order n and $p|n$ is a prime, the minimum weight $d^\perp$ of $C_p(\Pi)^\perp$ satisfies

$$n + 2 \leq d^\perp \leq 2n.$$

The lower bound is obtained by simply noticing that every one of the $n + 1$ lines through a point in the support must meet the set again, and the upper bound follows since the vector $v^L - v^M$ is in $C_p(\Pi)^\perp$, where L and M are any two distinct lines of Π.

The next result can be found in [6, Corollary 4], but the first part of it was established earlier by Sachar [15]:

Result 2 *Let Π be a projective plane of odd order n, and let $p|n$. Then the minimum weight $d^\perp$ of $C_p(\Pi)^\perp$ satisfies $d^\perp \geq \frac{4}{3}n + 2$. Further, if $p \geq 5$ then $d^\perp \geq \frac{3}{2}n + 2$.*

In addition there is the following from [15, 6]:

Result 3 *A projective plane of order q^2 that contains a Baer subplane has words of weight $2q^2 - q$ in its p-ary dual code, where p is a prime dividing q.*

Looking at planes of various specific orders, in [10] the four projective planes of order 9 were examined: the desarguesian plane, Φ, the translation

(Hall) plane, Ω, the dual translation plane, Ω^D, and the Hughes plane, Ψ (see [14, 11]). It was shown that the minimum weight of the dual ternary code is 15 for Φ, Ω, and Ω^D, and is 14 for Ψ. In Clark [5] it is shown that for planes of order 25 the minimum weight of the dual 5-ary code is at least 42, and is exactly 45 in the desarguesian case.

A **translation plane** can be defined in many equivalent ways (see for example André [1], Bruck and Bose [4], or [2, Chapter 6.8] for more references). We use here the following construction (from [1]) for a **translation plane** of order q^m with **kernel** containing the finite field F_q of order q, where $q = p^t$, p is a prime, and $m \geq 2$. Let V denote the vector space $V_{2m}(q)$ of dimension $2m$ over $F = F_q$. A **spread** is a set $\mathcal{V}$ of $q^m + 1$ m-dimensional subspaces V_i of V, for $i \in I$, where $V_i \cap V_j = \{0\}$ for $i \neq j$, and where I is a set of cardinality $q^m + 1$. The points of the affine plane are the vectors of V, and the lines are all the cosets $u + V_i$ for $u \in V$, $i \in I$. The projective plane is obtained by adding a line at infinity consisting of points P_i corresponding to V_i, with P_i incident with $u + V_j$ if and only if $j = i$. Write $\mathcal{P}(\mathcal{V})$ and $\mathcal{A}(\mathcal{V})$ for the projective and affine planes defined by $\mathcal{V}$, respectively. The lines of $\mathcal{P}(\mathcal{V})$ (respectively $\mathcal{A}(\mathcal{V})$) will be denoted by $\mathcal{L}_{\mathcal{P}}$ (respectively $\mathcal{L}_{\mathcal{A}}$), with ℓ^∞ the line at infinity made up of the points P_i corresponding to the spread elements V_i. The desarguesian plane of order q^m is a translation plane where the m-dimensional subspaces over F_q are in fact 1-dimensional subspaces over F_{q^m}.

3 Construction

Given a vector space $V = V_{2m}(q)$ of dimension $2m$ over the finite field $F = F_q$ of order q, and a spread $\mathcal{V}$ of $q^m + 1$ m-dimensional subspaces V_i of V, and using the notation of Section 2, we can now describe a recursive construction leading to subsets S_n of points of $\mathcal{A}(\mathcal{V})$, where S_n will consist of q^n points, where $1 \leq n \leq m$, and have the property that projective (or affine) lines meet it in $0, 1$ or q points. The points of S_n and the lines meeting it in q points (the q-secants) will form a 2-$(q^n, q, 1)$ design, in fact the design $AG_{n,1}(F_q)$.

Take any non-zero vector of V, say $u_1 \in V_1$, and let $S_1 = \langle u_1 \rangle$, the 1-dimensional subspace spanned by u_1. Then $|S_1| = q$ and lines meet S_1 in $0, 1$ or q points. Pick any non-zero vector u_2 in a distinct spread element V_2, and let $S_2 = \langle u_1, u_2 \rangle$, a 2-dimensional subspace of V. Then $|S_2| = q^2$ and lines of the affine plane $\mathcal{A}(\mathcal{V})$ meet S_2 in 0, 1 or q points: for suppose

$M = u + W \in \mathcal{L}_{\mathcal{A}}$. If $a \in (u + W) \cap S_2$ then $u + W = a + W$ and $(a + W) \cap S_2 = a + (W \cap S_2)$ has the same size as $W \cap S_2$. Since u_1 and u_2 in S_2 were chosen from different spread elements, we have $W \cap S_2 \neq S_2$, so that $|W \cap S_2| = 1$ or q, as asserted. Let

$$\mathcal{V}_2 = \{W \in \mathcal{V} \mid |W \cap S_2| = q\}$$

and

$$\mathcal{L}_2 = \{u + W \mid W \in \mathcal{V}_2,\ u \in S_2\}.$$

Then for $M \in \mathcal{L}_2$, we have $|M \cap S_2| = q$. It is clear that the points and q-secants to S_2 (i.e. $\mathcal{L}_2$) form a 2-$(q^2, q, 1)$ design.

Lemma 1 *If $M, N \in \mathcal{L}_2$ are distinct lines, then $|(M \cap N) \cap S_2| = 0$ if and only if M and N are cosets of the same spread element.*

Proof: We show that if $M = u+W_1$ and $N = v+W_2$ are in $\mathcal{L}_2$ and $W_1 \neq W_2$, then M and N meet in S_2. Since $W_1, W_2 \in \mathcal{V}_2$ and are not equal, there exist $w_i \in W_i \cap S_2$, $i = 1, 2$, and $S_2 = \langle w_1, w_2 \rangle$. Thus $u = \alpha w_1 + \beta w_2$ and $v = \gamma w_1 + \delta w_2$ and $M = u + W_1 = \alpha w_1 + \beta w_2 + W_1 = \beta w_2 + W_1$ and $N = v + W_2 = \gamma w_1 + \delta w_2 + W_2 = \gamma w_1 + W_2$. It follows that $\gamma w_1 + \beta w_2 \in M \cap N$, and so the cosets meet in S_2 if the spread elements are distinct. Obviously, distinct cosets of the same spread element do not meet in the affine plane. Thus the elements of $\mathcal{V}_2$ form the line at infinity for the affine plane of order q made up of the points of S_2 and the lines $\mathcal{L}_2$. □

Now we form S_3 by adjoining, if such can be found, a vector u_3 that is not on any of the members of $\mathcal{L}_2$, and forming $S_3 = \langle S_2, u_3 \rangle = \langle u_1, u_2, u_3 \rangle$. Then S_3 is a $(0, 1, q)$-set and the points and q-secants form a 2-$(q^3, q, 1)$ design. Continue in this way, if possible, and suppose we have defined the n-dimensional subspace $S_n = \langle u_1, \ldots, u_n \rangle$ such that lines meet S_n in 0, 1 or q points, so that the points and q-secants of S_n form a 2-$(q^n, q, 1)$ design. We know this is possible for $n = 2$.

Lemma 2 *Suppose for some $n \geq 2$ the n-dimensional subspace $S_n = \langle u_1, \ldots, u_n \rangle$ of V is such that lines of $\mathcal{A}(\mathcal{V})$ meet S_n in 0, 1 or q points. Let $\mathcal{L}_n$ denote the set of (affine) q-secants to S_n, and let $\mathcal{V}_n$ denote the set of $\frac{q^n-1}{q-1}$ spread members corresponding to the lines in $\mathcal{L}_n$. If there exists $w \in V$ such that $w \notin U$ for any $U \in \mathcal{L}_n$ then $S_{n+1} = \langle S_n, w \rangle = \langle u_1, \ldots, u_n, w \rangle$ is a set of q^{n+1} points that is met by lines of the plane in 0, 1 or q points.*

Proof: Clearly the vectors in S_n and the q-secants form a 2-$(q^n, q, 1)$ design. As in the case when $n = 2$ it follows that each spread element in $\mathcal{V}_n$ will have q^{n-1} cosets that are q-secants to S_n. Write $S = S_{n+1} = \langle S_n, w\rangle$, where w satisfies the conditions of the lemma. Suppose for some $U \in \mathcal{L}_{\mathcal{A}}$, $|S \cap U| > q$. If $U = u + C$ where $C \in \mathcal{V}$, then $S \cap U = S \cap (u + C) = s + (S \cap C)$, for some $s \in S$, and thus without loss of generality we can assume that $|S \cap C| > q$ for some $C \in \mathcal{V}$. Thus $\dim(S \cap C) = k \geq 2$. Since

$$\dim(S_n) + \dim(S \cap C) = \dim(S_n + (S \cap C)) + \dim(S_n \cap (S \cap C)),$$

we have $n + k \leq n + 1 + d$, where $d = \dim(S_n \cap C)$. Thus $1 \leq k - 1 \leq d$, and since d is at most 1, we have $d = 1$ and $C \in \mathcal{V}_n$.

Thus $C = \langle v, x, S'\rangle$, where $v \in S_n$, $x \in (S \setminus S_n)$ and $S' \subset C$. So $S = \langle x, S_n\rangle$, and hence $w = \alpha x + u$ where $\alpha \in F_q$ and $u \in S_n$. It follows that $w \in u + C \in \mathcal{L}_n$, contrary to our construction. □

Thus provided we can find a vector w such that $w \notin U$ for any $U \in \mathcal{L}_n$, we can extend the subspace S_n to S_{n+1} of q^{n+1} points such that S_{n+1} is met by lines in 0, 1 or q points. If we can proceed as far as $n = m$ then the set will have size q^m and we get the following:

Proposition 1 *With the notation as above, if we can form a set S_m of size q^m from the construction, then if $X = S_m$ and $Y = \{P_i \mid i \in I\} \setminus \{P_i \mid V_i \in \mathcal{V}_m\}$, the vector $v^X - v^Y$ is in the dual code of the p-ary code of the plane $\mathcal{P}(\mathcal{V})$. Thus the minimum weight of the dual code is at most $2q^m + 1 - (q^m - 1)/(q - 1)$.*

Proof: Recall that v^Z denotes the characteristic vector of the set Z, a subset of the coordinate set of the code. We need to show that for every line ℓ of the projective plane, $(v^X - v^Y, v^\ell) = 0$. If ℓ meets X in q points then $\ell \cap Y = \emptyset$, and we are done. If ℓ is a tangent to X then $\ell \cap \ell^\infty \in Y$, and so $(v^X - v^Y, v^\ell) = 0$. Each point of Y is on q^m affine lines, and these lines must all be tangents to X, and thus satisfy our requirement. The line ℓ^∞ clearly satisfies the requirement, and any other line that does not meet X must have $\ell \cap Y = \emptyset$, so we are done.

The weight of the vector $v^X - v^Y$ is $|X| + |Y| = q^m + (q^m + 1 - \frac{q^m-1}{q-1}) = 2q^m + 1 - \frac{q^m-1}{q-1}$. □

Note: 1. The construction we obtain here has size quite close to the bound mentioned in Result 2, but will of course only hold for translation planes, and when we can find such sets.

2. If $q = p^t$ then a translation plane of order q^m can be viewed in a vector space of dimension $2mt$ over F_p. In this case the construction we have described would lead to a word of smaller weight, since clearly

$$2p^{mt} + 1 - \frac{p^{mt} - 1}{p - 1} < 2q^m + 1 - \frac{q^m - 1}{q - 1},$$

for $t > 1$.
3. If $q = 2$ the size of the word in the dual code is $q^m + 2$, and thus we have a hyperoval. If at any stage we cannot move from S_n up to S_{n+1}, then the set S_n is a complete arc in the affine plane. This will give a complete arc in the projective plane by adjoining any two points on ℓ^∞ that are not in the projective completion of S_n, i.e. not amongst the points corresponding to $\mathcal{V}_n$.

We can now start the proof of Theorem 1.

Proof of Theorem 1:
For $m = 2$ the existence is clear and the set is just the affine part of a Baer subplane, reaffirming the result, which, as far as the authors are aware, is well-known, that all translation planes of square order have Baer subplanes.

For $m = 3$ we can always produce such sets, by an easy counting argument. Clearly we can form the set S_2 of the construction. By Proposition 1, if we can form a set S_3 then we will have the required word in the dual code. By Lemma 2 we simply need to show that $w \in V$ not on any of the q-secants of S_2 can be found. Since S_2 is an affine plane of order q, all its lines either meet in the plane or on the line at infinity. The line at infinity for S_2 is made up of the elements of $\mathcal{V}_2$, as was shown in Lemma 1. Thus the number of points in V outside of S_2 that are on lines of the affine plane is $(q^2 + q)(q^3 - q)$. The number of points available for S_3 is thus

$$q^6 - ((q^2 + q)(q^3 - q) + q^2),$$

and this is easily seen to be greater than 0. This deals with the first part of the theorem. For the extension of this to $m = 4$ in the desarguesian case we need to give explicit constructions, for which we need another lemma.

Lemma 3 *Let $\Pi = PG_2(F_{q^m})$ where q is a power of a prime, and $m \geq 2$. Let $K = F_{q^m}$, $F = F_q$. Then using homogeneous coordinates for the points of Π,*

1. *the set*
$$S_2 = \{(1, a, b) \mid a, b \in F\}$$
has q^2 *points and is met by lines of* Π *in* 0, 1 *or* q *points;*

2. *the set*
$$S_3 = \{(1, a + b\omega, c + b\omega^2) \mid a, b, c \in F\},$$
where ω *is any primitive element of* K*, has* q^3 *points and is met by lines of* Π *in* 0, 1 *or* q *points, if* $m \geq 3$*;*

3. *if* q *is odd and* k *is a non-zero non-square in* F*, then the set*
$$S_4 = \{(1, a + b\omega + c\omega^2, d + b\omega^2 + ck\omega) \mid a, b, c, d \in F\},$$
where ω *is an element of* K *whose minimal polynomial* $m(x)$ *over* F *has degree* 4 *and has a non-zero cubic term, has* q^4 *points and is met by lines of* Π *in* 0, 1 *or* q *points, if* $m = 4$*.*

Proof: The proof is by a direct application of the construction, looking for a point of the plane that is not on any of the lines of the previous set.

The set S_2 clearly has the properties stated, since $m \geq 2$. To form S_3, with $m \geq 3$, notice that the lines of Π that meet S_2 in q points are the lines with homogeneous coordinates $(a, b, c)^T$ for $a, b, c \in F$, excluding the line at infinity $(1, 0, 0)^T$. If ω is any primitive element for K, the point $(1, \omega, \omega^2)$ will be on one of these lines if $a + b\omega + c\omega^2 = 0$, which will occur if ω is a root of the polynomial $p(x) = a + bx + cx^2 \in F[x]$. Since ω is a root of an irreducible polynomial of degree $m \geq 3$, it is not possible for it to satisfy a polynomial of smaller degree over F. Thus $P = (1, \omega, \omega^2)$ is a suitable point to use to get S_3, which is then just a simple span of all the points from S_2 and P, but not including the line at infinity, $(1, 0, 0)^T$. Clearly the set S_3 has the form stated, and the points and q-secants form a 2-$(q^3, q, 1)$ design.

For the next case, with $m = 4$, we need to find a point on none of the q-secants to S_3. We extend the field F to K using a root ω of an irreducible polynomial of degree 4 with a non-zero cubic term: such a primitive polynomial can always be found by Cohen [7, Theorem 1]. Consider the line through the two distinct points of S_3, $P = (1, a + b\omega, c + b\omega^2)$ and $Q = (1, a^* + b^*\omega, c^* + b^*\omega^2)$, where $a, a^*, b, b^*, c, c^* \in F$, and $P \neq Q$. If $a = a^*$ and $b = b^*$, the line will have coordinates $(a + b\omega, -1, 0)^T$ which will exclude from our choice all points of the form $(1, a + b\omega, \alpha)$ where $a, b \in F$ and $\alpha \in K$. If $b = b^*$ and $c = c^*$ then the line has coordinates $(c + b\omega^2, 0, -1)^T$

which also excludes points of the form $(1, \alpha, a + b\omega^2)$ where $a, b \in F$ and $\alpha \in K$.

In the general case a line through the two points P and Q has coordinates $(x_1, x_2, x_3)^T$ where

$$\begin{aligned} x_1 &= (ca^* - ac^*) + (cb^* - bc^*)\omega + (ba^* - ab^*)\omega^2 \\ x_2 &= (c^* - c) + (b^* - b)\omega^2 \\ x_3 &= (a - a^*) + (b - b^*)\omega. \end{aligned}$$

Now we can verify that with our choice of ω, the point $(1, \omega^2, k\omega)$, where k is a non-square in F, is not on any of these lines: it is clearly not on any of the lines $(a + b\omega, -1, 0)^T$ nor $(c + b\omega^2, 0, -1)^T$, since ω is not the root of a quadratic. Suppose it is on one of the lines in the general case. Then $x_1 + \omega^2 x_2 + k\omega x_3 = 0$, where x_1, x_2, x_3 are of the form given above. Thus $(ca^* - ac^*) + (cb^* - bc^*)\omega + (ba^* - ab^*)\omega^2 + (c^* - c)\omega^2 + (b^* - b)\omega^4 + (a - a^*)k\omega + (b - b^*)k\omega^2 = 0$. Since $\omega^4 = \sum_{i=0}^{3} a_i\omega^i$ and $a_3 \neq 0$, the term in ω^3 must be 0, so $b = b^*$. Equating coefficients of ω^i to 0 for $i = 0, 1, 2$ yields $k = b^2$, which contradicts our choice of k.

The point $(1, \omega^2, k\omega)$ can thus be taken as the next choice, allowing us to get S_4 in the same way. It clearly has the form stated in the lemma. □

We can now complete the proof of Theorem 1, using the notation of Lemma 3. First let $S = \{(0, 1, a) \mid a \in K\}$.

For $m = 2$ we let

$$S_2' = S \setminus \{(0, 1, a) \mid a \in F\}.$$

Then the word in the dual code is $v^{S_2} - v^{S_2'}$.

For $m = 3$ we let

$$S_3' = S \setminus \{(0, 1, \frac{a + b\omega^2}{c + b\omega}) \mid a, b, c \in F,\ c + b\omega \neq 0\}.$$

Then the word in the dual code is $v^{S_3} - v^{S_3'}$.

For $m = 4$ we let

$$S_4' = S \setminus \{(0, 1, \frac{a + b\omega^2 + ck\omega}{d + b\omega + c\omega^2}) \mid a, b, c, d \in F,\ d + b\omega + c\omega^2 \neq 0\}.$$

Then the word in the dual code is $v^{S_4} - v^{S_4'}$.

Notice that in each case we are simply omitting the points on the line at infinity where the q-secants meet it. The word is then easily seen to be in the dual code. □

Note: We first noticed sets of this nature in the case of $q = 3$ and $m = 3$ while using Magma [3] to construct the seven translation planes of order $n = 27$, as classified by Dempwolff [8], when words of weight 42 occurred in the echelonized basis for the dual code. Sets of this size were not found in the dual codes of any of the non-desarguesian dual translation planes of order 27, and we still have no better upper bound than $2n = 54$ for the minimum weight of the dual codes of these planes.

Clearly we would also like to be able to show the existence of these sets of size q^m for any $m > 3$ in any translation plane of order q^m. We have been unable to do this; simple counting is not good enough. We did make one step towards a set of q^5 points by constructing the set S_4 in the general case of a field of order q^m where $m \geq 5$ (notice that in Lemma 3, $m = 4$). We state this as a lemma:

Lemma 4 *Let $\Pi = PG_2(F_{q^m})$ where q is a power of an odd prime, and $m \geq 5$. Let $K = F_{q^m}$, $F = F_q$. Let the set S_3 be as in Lemma 3. Then if ω is a primitive element for K with minimal polynomial (over F) $m(x)$, then the point $(1, \omega^3, \omega)$ is not on any q-secant of S_3 if $m \geq 6$, or if $m = 5$ and ω is chosen such that $m(x)$ has a non-zero quartic term. The set S_4 is then given by*

$$S_4 = \{(1, a + b\omega + c\omega^3, d + c\omega + b\omega^2) \mid a, b, c, d \in F\},$$

has q^4 points and is met by lines of Π in 0, 1 or q points.

We have not been able to find a general form for an element not on a q-secant of S_4, but we have some computational results using Magma [3] for $q = 3$ and $m = 5$: if ω is a root of the primitive polynomial $x^5+x^4+x^3+x+1$ and S_4 is the $(0, 1, 3)$-set as described in Lemma 4, then there is no point of the projective plane $PG_2(3^5)$ not on the line at infinity that is not on any 3-secant of S_4. If, on the other hand, ω is a root of $x^5+2x^4+x^3+x^2+x+1$, then the point $(1, \omega^4, \omega^{13})$ is not on any 3-secant of S_4 and hence S_5 and an appropriate word in the dual ternary code of $PG_2(3^5)$ can be constructed. Thus the minimum weight of the dual ternary code of the desarguesian plane of order 3^5 is at most 366.

4 Possible words in the dual

In trying to establish bounds for the minimum weight of the dual code, we looked at some constructions that might give suitable words. We describe

here one such type of construction. Our results in this paper are of this type.

Let Π be a projective plane of order n, and let $p|n$, where p is a prime. Let $\mathcal{S}_i$ for $i \in \{1,2\}$ be a set of points of Π that is a $(0,1,h_i)$-set, where $h_i > 1$. Further, let $|\mathcal{S}_i| = s_i$. We will say that $\mathcal{S}_1$ and $\mathcal{S}_2$ are **absolutely disjoint** if they have no points in common, and if the h_i-secants to $\mathcal{S}_i$ are exterior to $\mathcal{S}_j$, and every 1-secant to $\mathcal{S}_i$ is a 1-secant to $\mathcal{S}_j$, for $\{i,j\} = \{1,2\}$.

For $i \in \{1,2\}$, the points of $\mathcal{S}_i$ and the h_i-secants form a 2-$(s_i, h_i, 1)$ design $\mathcal{D}_i$ (which might be a trivial design) by taking the blocks to be the intersections of the h_i-secants with $\mathcal{S}_i$.

Proposition 2 *Let Π be a projective plane of order n and p a prime dividing n. Suppose that $\mathcal{S}_i$ for $i = 1,2$ are a pair of absolutely disjoint $(0,1,h_i)$-sets of size $|\mathcal{S}_i| = s_i$, respectively, where $p|h_i$. Then $v^{\mathcal{S}_1} - v^{\mathcal{S}_2}$ is a word of weight $s_1 + s_2$ in $C_p(\Pi)^\perp$ and*

$$n + 1 = \frac{s_1 - 1}{h_1 - 1} + s_2 = \frac{s_2 - 1}{h_2 - 1} + s_1.$$

Further:

1. *If $s_1 = s_2 = s$ then $h_1 = h_2 = h$, and $s = n + 1 - \frac{n}{h}$. Conversely, if $h \neq 2$, then $h_1 = h_2 = h$ implies that $s_1 = s_2 = s$, $s = n + 1 - \frac{n}{h}$, and $s_1 + s_2 = 2n - 2\frac{n-h}{h}$.*

2. *If $s_2 = h_2$ (so $\mathcal{S}_2$ is part of a line of Π), then $s_1 = n$, $s_2 = n+1-\frac{n-1}{h_1-1}$, and $s_1 + s_2 = 2n - \frac{n-h_1}{h_1-1}$.*

Proof: The definition of $\mathcal{S}_i$, along with $p|h_i$ for $i = 1,2$, clearly gives $v^{\mathcal{S}_1} - v^{\mathcal{S}_2} \in C_p(\Pi)^\perp$. For any point $x \in \mathcal{S}_i$, counting the lines and blocks through x gives $n + 1 = \frac{s_i-1}{h_i-1} + s_j$ for $\{i,j\} = \{1,2\}$.

To prove (1), suppose first that $s_1 = s_2 = s$. Then $\frac{s-1}{h_1-1} + s = \frac{s-1}{h_2-1} + s$. Thus clearly $h_1 = h_2 = h$. From $n + 1 = \frac{s-1}{h-1} + s$ we can solve for s to get the stated equality.

Suppose now that $h_1 = h_2 = h$. Then $\frac{s_1-1}{h-1} + s_2 = \frac{s_2-1}{h-1} + s_1$ implies that $s_1(h-2) = s_2(h-2)$, so either $h = 2$ or $s_1 = s_2$.

To prove (2), suppose $s_2 = h_2$. Then $n + 1 = \frac{s_2-1}{h_2-1} + s_1$ implies that $s_1 = n$. From $n + 1 = \frac{s_1-1}{h_1-1} + s_2$ we get $n + 1 = \frac{n-1}{h_1-1} + s_2$ and hence $s_2 = n + 1 - \frac{n-1}{h_1-1}$, as required. □

Note: The support set $\mathcal{S}_1 \cup \mathcal{S}_2$ is a $(0, 2, h_1, h_2)$-set, where here we may have $h_1 = h_2$ and either or both may be 2. Also note that for $h = h_1 > 2$, the word in the dual code from the construction in (1) is smaller than the word from (2).

The following special cases are feasible:

1. $s_1 = s_2 = h_1 = h_2$: the configuration consists of two lines with the point of intersection omitted.
2. If $n = q^r = p^t$ and $s_2 = h_2$, then $p|h_1$ and $(h_1 - 1)|(q^r - 1)$ is possible if $h_1 = q$, which will give a word of weight $2q^r - (q^{r-1} + q^{r-2} + \ldots + q)$. This is the construction of our Theorem 1.
3. Other numerical possibilities:
   (a) $n = 9$, $s_1 = s_2 = 7$, $h_1 = h_2 = 3$: two absolutely disjoint Fano planes, weight 14 (see [10]).
   (b) $n = 25$, $s_1 = s_2 = 21$, $h_1 = h_2 = 5$: two absolutely disjoint planes of order 4, weight 42; in general it is unknown if a plane of order 25 can have an embedded plane of order 4 (see the note below).
   (c) $n = 27$, $s_1 = s_2 = 19$, $h_1 = h_2 = 3$: two absolutely disjoint Steiner triple systems, weight 38; it is not known if this is possible.
   (d) $n = 27$, $s_1 = 25$, $s_2 = 16$, $h_1 = 3$, $h_2 = 6$: 2-$(25, 3, 1)$ and 2-$(16, 6, 1)$ designs, weight 41; no design with the latter parameters can exist by Fisher's inequality.
   (e) $n = 49$, $s_1 = s_2 = 43$, $h_1 = h_2 = 7$: two absolutely disjoint 2-(43,7,1) designs, i.e. planes of order 6, weight 86; planes of order 6 do not exist, by the Bruck-Ryser theorem (see, for example, [2, Chapter 4]).
   (f) $n = 81$, $s_1 = 73$, $s_2 = 46$, $h_1 = 3$, $h_2 = 6$: 2-$(73, 3, 1)$ and 2-$(46, 6, 1)$ designs, weight 119; it is unknown if a design with the latter parameters exists.

Note: The desarguesian plane $PG_{2,1}(F_q)$ does not contain subplanes of orders other than those from subfields of F_q, so the configurations for $n = 9$ or 25 cannot exist for the desarguesian case. However, it is conjectured that any non-desarguesian plane contains a Fano plane (see Neumann [13]). Not all the known planes of order 25 have been checked for subplanes of order 4, but some are known not to have any; Clark [5] has a survey of the known results.

Acknowledgement

The second author thanks the Dipartimento di Matematica at the Universitá di Roma 'La Sapienza' for their hospitality, and the C.N.R. (Italy) for financial support, in June 1999. The authors thank the referee for careful reading and constructive comments.

References

[1] J. André. Über nicht-Desarguessche Ebenen mit transitiver Translationsgruppe. *Math. Z.*, 60:156–186, 1954.

[2] E. F. Assmus, Jr. and J. D. Key. *Designs and their Codes*. Cambridge: Cambridge University Press, 1992. Cambridge Tracts in Mathematics, Vol. 103 (Second printing with corrections, 1993).

[3] Wieb Bosma and John Cannon. *Handbook of Magma Functions*. Department of Mathematics, University of Sydney, November 1994.

[4] R. H. Bruck and R. C. Bose. The construction of translation planes from projective spaces. *J. Algebra*, 1:85–102, 1964.

[5] K. L. Clark. *Improved bounds for the minimum weight of the dual codes of some classes of designs*. PhD thesis, Clemson University, 2000.

[6] K. L. Clark and J. D. Key. Geometric codes over fields of odd prime power order. *Congr. Numer.*, 137:177–186, 1999.

[7] Stephen D. Cohen. Primitive elements and polynomials with arbitrary trace. *Discrete Math.*, 83:1–7, 1990.

[8] U. Dempwolff. Translation planes of order 27. *Des. Codes Cryptogr.*, 4:105–121, 1994. Correction in Vol. 5, 1995, page 81.

[9] J. D. Key and M. J. de Resmini. Small sets of even type and codewords. *J. Geom.*, 61:83–104, 1998.

[10] J. D. Key and M. J. de Resmini. Ternary dual codes of the planes of order nine. *J. Statist. Plann. Inference*, 95:229 – 236, 2001.

[11] C. W. H. Lam, G. Kolesova, and L. Thiel. A computer search for finite projective planes of order 9. *Discrete Math.*, 92:187–195, 1991.

[12] Shu Lin and Daniel J. Costello, Jr. *Error Control Coding: Fundamentals and Applications*. Prentice-Hall, 1983. Englewood Clifts, NJ.

[13] H. Neumann. On some finite non-desarguesian planes. *Arch. Math.*, VI:36–40, 1955.

[14] T. G. Room and P. B. Kirkpatrick. *Miniquaternion geometry: an introduction to the study of projective planes*. Cambridge University Press, 1971.

[15] H. Sachar. The F_p span of the incidence matrix of a finite projective plane. *Geom. Dedicata*, 8:407–415, 1979.