An upper bound for the minimum weight of the dual codes of desarguesian planes

J. D. Key
School of Mathematical Sciences
University of KwaZulu-Natal
Pietermaritzburg 3209
South Africa

T. P. McDonough and V. C. Mavron
Institute of Mathematics and Physics
Aberystwyth University, Aberystwyth
Ceredigion SY23 3BZ, U.K.

January 28, 2008

Running head:
Dual codes of desarguesian planes

Corresponding author:
Professor V. C. Mavron
Institute of Mathematics and Physics
Aberystwyth University, Aberystwyth
Ceredigion SY23 3BZ
U.K.

Abstract

We show that a construction described in Clark, Key and de Resmini [9] of small-weight words in the dual codes of finite translation planes can be extended so that it applies to projective and affine desarguesian planes of any order p^m where p is a prime, and $m \geq 1$. This gives words of weight $2p^m + 1 - \frac{p^m-1}{p-1}$ in the dual of the p-ary code of the desarguesian plane of order p^m, and provides an improved upper bound for the minimum weight of the dual code. The same will apply to a class of translation planes that this construction leads to; these belong to the class of André planes.

We also found by computer search a word of weight 36 in the dual binary code of the desarguesian plane of order 32, thus extending a result of Korchmáros and Mazzocca [19].

1 Introduction

The determination of the minimum weight and the nature of possible minimum words of the dual p-ary code of a projective plane, where p is a prime that divides the order n of the plane, is an open problem. This is in contrast to the question for the code itself where the minimum weight vectors have long been known to be the scalar multiples of the incidence vectors of the lines: see, for example, [2, Chapter 6]. Lower and upper bounds for the minimum weight of the dual code are known. Here we improve the general known upper bound of $2n$ (that holds for all planes) in the desarguesian case, and some classes of translation planes, with the following theorem:

Theorem 1 *Let Π be the desarguesian projective plane of order p^m where p is a prime and $m \geq 1$. Let C be the p-ary code of Π. Then the dual code $C^\perp$ contains words of weight $2p^m + 1 - \frac{p^m-1}{p-1}$ that can be constructed in the following way, using homogeneous coordinates: if ω is a primitive element of $\mathbb{F}_{p^m}$ and $S = \{(1, a, a^p) \mid a \in \mathbb{F}_{p^m}\}$, $Y = \{(0, 1, \omega^j) \mid 1 \leq j \leq \frac{p^m-1}{p-1}, (p-1) \text{ does not divide } j\} \cup \{(0, 1, 0), (0, 0, 1)\}$ then $v^S - v^Y$ is a word of weight $2p^m + 1 - \frac{p^m-1}{p-1}$ in $C^\perp$. The same is true for the dual code of the affine desarguesian plane.*

This upper bound applies also to some classes of André planes.

The theorem is proved by showing that a construction in [9] holds for desarguesian planes of all orders.[1] 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 $2p^m + 1 - \frac{p^m-1}{p-1}$, as given in this formula. The construction also holds for a class of André translation planes, giving the same upper bound for the minimum weight of the dual code for these planes. In fact this is the minimum weight in all known cases for translation planes. However, there is a non-translation plane of order 9 whose dual ternary code has a smaller minimum weight (see the discussion in Section 2).

[1] The authors thank one of the referees for pointing out that the bound for the desarguesian plane case follows from a result in [23] also.

In Section 2 we give the background results, definitions and constructions. In Section 3, in Proposition 1, we prove the main part of the theorem, as it applies to desarguesian planes. In Section 4, in Proposition 2, we show how the translation planes arise, and how the upper bound applies to this class as well. We show that these planes are André planes. Section 5 contains some counting arguments relevant to the construction, in particular with a view to constructions that could lead to words in the dual of the codes of other translation planes.

Finally, in Section 6 we show, in Proposition 4, how the word of weight 36 was obtained in the dual binary code of the desarguesian plane of order 32, and explain why this is an interesting discovery.

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. For $n \geq 2$, a finite projective plane of order n is a 2-$(n^2 + n + 1, n + 1, 1)$ design and a finite affine plane of order n is a 2-$(n^2, n, 1)$ design. We write $PG_{2,1}(\mathbb{F}_q)$ for the desarguesian projective plane of order q, i.e. the design of points and 1-dimensional subspaces of the projective space $PG_2(\mathbb{F}_q)$. Further, $AG_{m,n}(\mathbb{F}_q)$ will denote the 2-design of points and n-flats (cosets of dimension n) in the affine geometry $AG_m(\mathbb{F}_q)$. 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** $C_F(\mathcal{D})$, of the design $\mathcal{D}$ over the finite field F, is the space spanned by the incidence vectors of the blocks over F, where F is a prime field $\mathbb{F}_p$ and p divides the order of $\mathcal{D}$. If $\mathcal{D} = (\mathcal{P}, \mathcal{B}, \mathcal{I})$ and $\mathcal{Q} \subseteq \mathcal{P}$, then the incidence vector of $\mathcal{Q}$ is denoted 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** 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.

We use the terms **affine translation plane** and **projective translation plane** as defined in [2], omitting 'affine' or 'projective' if the context is clear. In order to apply results from [9], it will be more convenient to use the equivalent construction from [1] of a translation plane of order q^m with **kernel** containing the finite field $\mathbb{F}_q$ of order q, where $q = p^t$, p is a prime, and $m \geq 2$. Let V denote the vector space $V_{2m}(\mathbb{F}_q)$ of dimension $2m$ over 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 affine plane $\mathcal{A}(\mathcal{V})$ is the affine plane whose points are the the vectors of

V, and whose lines are all the cosets $u + V_i$ for $u \in V$, $i \in I$. The projective plane $\mathcal{P}(\mathcal{V})$ is the completion of $\mathcal{A}(\mathcal{V})$ in which the line at infinity ℓ^∞ consists of the points P_i, $i \in I$, where P_i incident with the line $u + V_j$ if and only if $j = i$. The lines of $\mathcal{P}(\mathcal{V})$ (respectively $\mathcal{A}(\mathcal{V})$) will be denoted by $\mathcal{L}_\mathcal{P}$ (respectively $\mathcal{L}_\mathcal{A}$). The desarguesian plane of order q^m is the translation plane obtained by identifying $V_{2m}(\mathbb{F}_q)$ with $V_2(\mathbb{F}_{q^m})$ and taking the spread subspaces to be the 1-dimensional subspaces over $\mathbb{F}_{q^m}$.

We now give a brief review of the main known results for the minimum weight of the dual codes of projective planes. For some classes there are precise results. 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 [15] for other results for non-desarguesian planes of even order, 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. For any prime p, the dual code of the desarguesian plane of order p has minimum weight $2p$. Other than this and some results for planes of small order, the main results for planes of odd order concern upper and lower bounds. An early result, quoted in [2, Theorem 5.7.9], is:

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

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

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

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

The lower bound is obtained by 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. A similar argument holds for affine planes.

For odd-order planes, from [8, Corollary 4] and Sachar [22]:

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 $\frac{4}{3}n + 2 \leq d^\perp$. Further, if $p \geq 5$ then $\frac{3}{2}n + 2 \leq d^\perp$.*

In addition there is the following from [8, 22]:

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.*

For planes of small non-prime odd order, the dual ternary codes of the four projective planes of order 9 were shown in [16] to all have $d^\perp = 15$ apart from the Hughes plane, for which $d^\perp = 14$. In [6, 7] the dual 5-ary code of any projective plane of order 25 was shown to have $d^\perp \geq 42$, with $d^\perp = 45$ in the desarguesian case. Planes of order

49 were studied in [18], giving the bounds $88 \leq d^{\perp} \leq 98$, with the upper bound 91 if the plane has a Baer subplane, which includes the desarguesian and all translation planes of order 49.

For translation planes, including desarguesian planes, the following was obtained in Clark, Key and de Resmini [9].

Result 4 *Let Π be a projective translation plane of order q^m 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 words of weight $2q^m + 1 - \frac{q^m-1}{q-1}$. If Π is desarguesian this also holds for $m = 4$.*

The construction of words of these weights is given; it is the Baer subplane construction when $m = 2$, and generalizes that construction.

A similar construction to that in Result 4 was applied to Figueroa planes [10] in Key and de Resmini [17]:

Result 5 *Let Φ be the Figueroa plane $\mathrm{Fig}(q^3)$ of order q^3 where $q = p^t$ and p is any prime. Let C denote the p-ary code of Φ. Then $C^{\perp}$ contains words of weight $2q^3-q^2-q$. Furthermore, if $d^{\perp}$ denotes the minimum weight of $C^{\perp}$ then*

1. *$d^{\perp} = q^3 + 2$ if $p = 2$;*
2. *$\frac{4}{3}q + 2 \leq d^{\perp} \leq 2q^3 - q^2 - q$ if $p = 3$;*
3. *$\frac{3}{2}q + 2 \leq d^{\perp} \leq 2q^3 - q^2 - q$ if $p > 3$.*

The binary case here follows from the fact that the even-order planes have hyperovals, from [21].

The relevant construction from [9] that we will use here can be summarized into the following, using notation as defined in this section:

Result 6 *Let $V = V_{2m}(\mathbb{F}_q)$ be a vector space of dimension $2m$ over the finite field $\mathbb{F}_q$, $\mathcal{V}$ a spread, and $\mathcal{A}(\mathcal{V})$ and $\mathcal{P}(\mathcal{V})$ the affine and projective planes, respectively, of order q^m, from $\mathcal{V}$. Suppose that S is an m-dimensional subspace of V such that lines of $\mathcal{A}(\mathcal{V})$ meet S in $0, 1$ or q points. Let $\mathcal{L}_m$ denote the set of affine q-secants to S and $\mathcal{V}_m$ the corresponding spread members. If $Y = \{P_i \mid i \in I\} \setminus \{P_i \mid V_i \in \mathcal{V}_m\}$, the vector $v^S - v^Y$ has weight $2q^m + 1 - \frac{q^m-1}{q-1}$ and is in the dual of the p-ary code of the plane $\mathcal{P}(\mathcal{V})$.*

Note: This word will be in the dual code of any affine plane from $\mathcal{P}(\mathcal{V})$ formed by taking as the line at infinity any line from the class V_i for $V_i \in \mathcal{V}$ that is not a q-secant to S.

3 Desarguesian planes

We will now consider the desarguesian plane of order q^m, where q is any prime-power, and we will show how to produce words of weight $2q^m + 1 - \frac{q^m-1}{q^h-1}$ in the dual p-ary

code of the plane (where q is a power of the prime p) for any $h|m$. The theorem will then follow.

We first set up some notation, following that given in Section 1. Let p be a prime, t and m positive integers, and $q = p^t$. Let $F = \mathbb{F}_q$, $K = \mathbb{F}_{q^m}$, and $V = V_{2m}(F)$. Let $\mathcal{V} = \{V_\infty\} \cup \{V_\gamma \mid \gamma \in K\}$ be a spread in V. Then V and $\mathcal{V}$ define an affine translation plane $\mathcal{A}(\mathcal{V})$ of order q^m whose points are the elements of V and whose lines are the point sets given by the elements of $\mathcal{V}$ and their translates by elements of V. If $\mathcal{A}(\mathcal{V})$ is the **desarguesian** plane, then $V = V_2(\mathbb{F}_{q^m}) = V_2(K) = K^2$, and we can write $V_\gamma = \{(\delta, \gamma\delta) \mid \delta \in K\}$, for all $\gamma \in K$, and $V_\infty = \{(0, \delta) \mid \delta \in K\}$, for a desarguesian spread for $\mathcal{A}(\mathcal{V})$.

Lemma 1 *Using the above notation, for any k such that $1 \leq k \leq m-1$, the set $S = \{(a, a^{q^k}) \mid a \in K\}$ is a $(0, 1, q^h)$-set for $\mathcal{A}(\mathcal{V})$ of size q^m, where $h = \gcd(k, m)$.*

Proof: Let ω be a primitive element of K. Clearly the mapping $\theta : x \mapsto x^{q^k}$ is an automorphism of K over F, and $S = \{(a, a\theta) \mid a \in K\}$ is an m-dimensional subspace of V.

We now see how S meets the spread members. It is immediate that $S \cap V_\infty = \{(a, a\theta) \mid a \in K, a = 0\} = \{0\}$ and $S \cap V_0 = \{(a, a\theta) \mid a \in K, a\theta = 0\} = \{0\}$. For $\gamma \in K^*$, $S \cap V_\gamma = \{(a, a\theta) \mid a \in K, a\theta = a\gamma\}$. Thus $S \cap V_\gamma \neq \emptyset$ if, and only if, $\gamma = a^{-1}(a\theta) = a^{q^k - 1}$ for some $a \in K^*$, that is $\gamma = \omega^{l(q^k-1)}$ for some $l \in \mathbb{Z}$. Since $q^h - 1$ is a factor of $q^k - 1$, $\gamma = \omega^{j(q^h-1)}$ for some $j \in \mathbb{Z}$. In this case, we compute the number of non-zero elements in $S \cap V_\gamma$. This is the number of elements $a \in K^*$ with $\gamma = a^{q^k-1}$. Consider the mapping $\psi : x \mapsto x^{q^k-1}$ from K^* into itself. This is a homomorphism of cyclic groups. The kernel is $\ker\psi = \{x \in K^* \mid x^{q^k-1} = 1\}$. Since $x^{q^m-1} = 1$ for all $x \in K^*$, we see that $x^c = 1$ for all $x \in \ker\psi$ where $c = \gcd(q^k - 1, q^m - 1)$. It is an elementary result that $c = q^h - 1$. Hence, $\ker\psi = \{x \in K^* \mid x^{q^h-1} = 1\}$, which is a cyclic subgroup of K^* of order $q^h - 1$. Since $(S \cap V_\gamma)\backslash\{0\}$ is a coset of $\ker\psi$ in K^*, $|S \cap V_\gamma| = q^h$. Thus S meets the spread members in $0, 1, q^h$ points, and hence also all the cosets of these, i.e. the lines of $\mathcal{A}(\mathcal{V})$. Thus S is a $(0, 1, q^h)$-set in $\mathcal{A}(\mathcal{V})$, as required. ■

Note: Since S is a subspace of V of the same size as the spread members, it follows that if $|S \cap V'| = 1$ for a spread member V', then $|S \cap (v + V')| = 1$ for every coset $v + V'$ of V' in V, and if $|S \cap V'| = q$ for a spread member V', then $|S \cap (v + V')| = q$ or 0 for every coset $v + V'$ of V' in V. Moreover, in the latter case, there is some coset $v + V'$ with $|S \cap (v + V')| = 0$.

Proposition 1 *The dual p-ary code of the desarguesian affine or projective plane of order q^m, where $q = p^t$, p is a prime, $m \geq 1$, contains words of weight $2q^m + 1 - \frac{q^m-1}{q^h-1}$ for any $h|m$.*

Proof: Taking $k = h = 1$ in Lemma 1, we see that $S = \{(a, a^q) \mid a \in K\}$ is a $(0, 1, q)$-set. ¿From Result 6, it follows that the dual p-ary code of the desarguesian projective plane of order q^m has words of weight $2q^m + 1 - \frac{q^m-1}{q-1}$. Now suppose $m = rh$ with $h > 1$. Then $q^m = (q')^r$ where $q' = q^h$, and the preceding argument shows that the desarguesian projective plane of order q^m has words of weight $2q^m + 1 - \frac{q^m-1}{q'-1}$, as asserted.

For the desarguesian affine plane, it is sufficient to observe that there is a line of the projective plane in Lemma 1 which avoids the set $S \cup Y$. ■

To establish the first part of Theorem 1, we need only take $q = p$ and $h = 1$ in Proposition 1 and note that the set S of Lemma 1 corresponds to the set S of Theorem 1 in the obvious way.

Note: 1. As mentioned in the footnote in Section 1, one of the referees has pointed out to us that the set $S \cup (\ell^\infty \backslash Y)$ is a Rédei-type blocking set and, using this fact together with arguments from [23], it will follow that we get a word in the dual code of the weight stated.
2. The word of weight $2q^m+1-\frac{q^m-1}{q^h-1}$, where $m = rh$, corresponds to the subfield of $\mathbb{F}_{q^m}$ of order q^h. The spread members are 1-dimensional over $\mathbb{F}_{q^m}$ and thus r-dimensional over $\mathbb{F}_{q^h}$. In the special case $h = m$, we get the earlier known upper bound of $2q^m$.

¿From the results quoted in Section 2 and Theorem 1 we get

Corollary 1 *Let $d^\perp$ be the minimum weight of the dual p-ary code of the desarguesian projective plane of order p^m, where p is a prime and $m \geq 1$. Then*

1. *if $p = 2$, $d^\perp = 2^m + 2$;*
2. *if $m = 1$, $d^\perp = 2p$;*
3. *if $p = 3$, then $3^m + 3^{m-1} + 2 \leq d^\perp \leq \frac{3}{2}(3^m + 1)$;*
4. *if $m \geq 2$, $p \geq 5$, then $\frac{3}{2}p^m + 2 \leq d^\perp \leq 2p^m + 1 - \frac{p^m-1}{p-1}$.*

Note: These bounds hold also for the desarguesian affine planes.

4 Derivation sets

The subspaces S produced in Proposition 1 give rise to derivation sets that yield a class of translation planes. The idea is related to the standard idea of derivation using Baer subplanes and is discussed in [2, Chapter 6].

Proposition 2 *Let p be a prime, t and m positive integers with $q = p^t$, $F = \mathbb{F}_q$ and $K = \mathbb{F}_{q^m}$. Let $\mathcal{V} = \{V_\gamma \mid \gamma \in K\} \cup \{V_\infty\}$ be the desarguesian spread, where $V_\infty = \{(0, \delta) \mid \delta \in K\}$ and $V_\gamma = \{(\delta, \gamma\delta) \mid \delta \in K\}$, for all $\gamma \in K$. Let $\theta : K \to K$ be the automorphism $\theta : a \mapsto a^{q^k}$ where k an integer such that $1 \leq k \leq m-1$, $h = \gcd(k, m)$,*

and $S = \{(a, a\theta) \mid a \in K\}$. *Let* $\mathcal{V}_S = \{V_\gamma \mid \gamma = \omega^{(q^h-1)j}, j = 0, \ldots, \frac{q^m-1}{q^h-1} - 1\}$. *Then if* $Sb = \{vb \mid v \in S\}$ *for* $b \in K^*$, *and* $Sb + u$ *is the translate of* Sb *by* $u \in V$, *the sets of points* $Sb + u$, *for* $b \in K^*$ *and* $u \in V$, *together with the original affine lines that are from the spread members not in* $\mathcal{V}_S$, *form an affine translation plane of order* q^m.

Proof: The set of points P_i for $V_i \in \mathcal{V}_S$ on the line at infinity form a derivation set, in the sense of [2, Definition 6.10.1], of size $\frac{q^m-1}{q^h-1}$. That the new set of lines form an affine plane follows from our construction. Thus note that the number of distinct Sb is $\frac{q^m-1}{q^h-1}$, and that these meet pairwise in $(0, 0)$. The next step gives the q^{m-1} distinct translates. ■

Note: 1. The constructed planes will also have words of weight $2q^m + 1 - \frac{q^m-1}{q^h-1}$ in their dual codes since any of the deleted lines, together with points at infinity, will provide such a word in the same way.
2. From [14, Chapter 16], it follows that these planes are André planes: in Definition 16.1 of that chapter, the André subnet $\mathcal{A}_1$, which is our set $\mathcal{L}_S$ with $k = h = 1$, is replaced by the set of subpaces $\mathcal{A}_1^\rho$, where ρ is any automorphism fixing F, and the latter sets are identical to our sets Sb by taking $k = 1$, $\rho = \theta$. This observation, together with the note above, completes the proof of the second part of Theorem 1.
3. We have not examined other classes of translation planes, or any non-translation planes, for words of this type. There may well be other classes for which the construction will apply.

5 Counting arguments

The construction used in Result 4 involved building up the subspace S of dimension m from a series of nested subspaces S_n of dimension n, for $1 \leq n \leq m$ that are all $(0, 1, q)$-sets. The result was obtained for all translation planes of order q^m where $m \leq 3$ since counting arguments could be used to show the existence of subspaces S_2 and S_3 that satisfy the requirements. An analogous counting argument for subspaces of size q^4 failed, and counter-examples have been found computationally: see below. However, for n small enough relative to m, the set can always be extended:

Proposition 3 *Let* $V = V_{2m}(\mathbb{F}_q)$ *be a vector space of dimension* $2m$ *over the finite field* $\mathbb{F}_q$, $\mathcal{V}$ *a spread, and* $\mathcal{A}(\mathcal{V})$ *and* $\mathcal{P}(\mathcal{V})$ *the affine and projective planes of order* q^m, *respectively, from* $\mathcal{V}$. *Suppose that for some* n *such that* $1 \leq n \leq m$, S_n *is an* n*-dimensional subspace of* V *that is a* $(0, 1, q)$*-set in* $\mathcal{A}(\mathcal{V})$. *If* $2n \leq m + 1$ *then* S_n *can be extended to an* S_{n+1}.

Proof: Let p be a prime, let t be a positive integer and let $q = p^t$. Let $F = \mathbb{F}_q$, $V = V_{2m}(q)$ and let $\mathcal{V} = \{V_1, V_2, \ldots, V_{q^m+1}\}$ be a spread of m-dimensional F-spaces in V.

Suppose that we have an n-dimensional F-space S_n meeting the spread spaces in subspaces of dimension at most 1. Since every non-zero point of S_n is in a unique V_i,

there are exactly $r_n = (q^n - 1)/(q - 1)$ of the V_i which meet S_n in q points. We may assume that these are the spaces V_i, $i = 1, \ldots, r_n$. For $i > r_n$, $V_i \cap S_n = 0$.

$$\dim_F(V_i + S_n) = \dim_F V_i + \dim_F S_n - \dim_F V_i \cap S_n = \begin{cases} m+n-1 & \text{if } i \leq r_n, \\ m+n & \text{if } i > r_n. \end{cases}$$

For $i \neq j$, $\dim_F(V_i + S_n) \cap (V_j + S_n) = \dim_F(V_i + S_n) + \dim_F(V_j + S_n) - \dim_F(V_i + V_j)$

$$= \begin{cases} 2n-2 & \text{if } i, j \leq r_n, \\ 2n & \text{if } i, j > r_n, \\ 2n-1 & \text{otherwise.} \end{cases}$$

In order to show that we can extend S_n to an S_{n+1}, we must show that there is an element in the set $V \setminus \bigcup_{i=1}^{r_n}(V_i + S_n)$. If $i, j \leq r_n$ and $i \neq j$, let $T_{i,j} = (V_i + S_n) \cap (V_j + S_n)$. Then $S_n \subseteq T_{i,j}$ and $\dim_F T_{i,j} = 2n - 2$.

A union of sets $A_1, \ldots, A_r$, all of the same size, and whose pairwise intersections have the same size, achieves a maximum size when there is a set B such that $A_i \cap A_j = B$ for all i, j with $i \neq j$. This maximum size is $|B| + r(|A_1| - |B|)$.

Applying this result to our situation, we find that

$$\begin{aligned} |V \setminus \bigcup_{i=1}^{r_n}(V_i + S_n)| &\geq q^{2m} - q^{2n-2} - r_n(q^{m+n-1} - q^{2n-2}) \\ &= q^{2n-1}(q^{m-n+1} - 1)(q^{m-n}(q-1) - (q^{n-1} - 1))/(q-1). \end{aligned}$$

This expression is clearly greater than zero if $m - n \geq n - 1$. Thus, if $2n \leq m + 1$, an S_n can be extended to an S_{n+1}. ■

Note: As was pointed out in [9], in the case of $q = 2$, if at any stage of the construction we find that an S_n cannot be extended to an S_{n+1}, then the set S_n and two points on the line at infinity not in the set $\mathcal{V}_n$ will form a complete arc in the projective plane.

A set of size 8 in a non-desarguesian plane of order 16 that could not be completed to one of size 16 with the required properties was found by computation using GAP [12] and Magma [4, 5]. Similarly, sets of size 16, 32 and 64 were found in desarguesian planes of order 32, 64, and 128, respectively. These, together with two points on the line at infinity, give complete arcs in the projective planes. There is a general construction, distinct from the sets we found by computation, due to Segre (see Hirschfeld [13, Theorem 9.12]), of complete arcs of size $2^{m-1} + 2$ in a desarguesian plane of order 2^m.

6 Small sets of even type

For projective planes of even order, n, the minimum weight for binary dual codes is at least the size of the hyperoval, i.e. $n+2$ and any vector that has this weight in $C^\perp$ must be the incidence vector of a hyperoval. For planes that do not have hyperovals, the next smallest weight would be $n + 4$, and the set of points would form a $(0, 2, 4)$-set. Sets of of this type in the desarguesian planes of even order were considered by Korchmáros and Mazzocca [19]. The 4-secants of such a set (in the desarguesian case) meet in a point called the nucleus of the set: see also Gács and Weiner [11]. A general canonical

form in the desarguesian case for such a set was deduced in [19], but examples only discovered for $q \leq 16$. The question of existence of such a set for $q \geq 16$ remains open. This type of set is also examined in [20, Chapter 6] and [3, 15].

In [15, Proposition 5] the following result was obtained:

Result 7 *Suppose the projective plane* Π *of even order* n *has two complete* $(\frac{1}{2}n+2)$*-arcs* $\mathcal{A}$ *and* $\mathcal{A}'$*, with the following properties:*

(i) $\mathcal{A}$ *and* $\mathcal{A}'$ *share exactly one interior point (i.e. a point on no tangent) and the* $\frac{1}{4}n+1$ *secants on it;*

(ii) the $\frac{1}{2}n(\frac{1}{2}n+2)$ *tangents to* $\mathcal{A}$ *are also tangents to* $\mathcal{A}'$*, and conversely;*

(iii) the $\binom{\frac{1}{2}n+2}{2} - (\frac{1}{4}n+1) = \frac{1}{8}n^2 + \frac{1}{2}n$ *secants to* $\mathcal{A}$ *other than the* $\frac{1}{4}n+1$ *secants on the common interior point are exterior to* $\mathcal{A}'$*, and similarly interchanging* $\mathcal{A}$ *and* $\mathcal{A}'$*.*

Then $\mathcal{A} \cup \mathcal{A}'$ *is a* $(0,2,4)$*-set of size* $n+4$*.*

We were able to use this idea to make a feasible computer search for such disjoint arcs in the desarguesian plane of order 32. We obtained the following:

Proposition 4 *If* Π *is the desarguesian plane of order* 32*, and* C *is its binary code, then if* u *is a primitive element for* $\mathbb{F}_{32}$ *with minimum polynomial* x^5+x^2+1*, the set of points*

$$\{(1, f(c), c) \mid c \in \mathbb{F}_{32}\} \cup \{(0,1,0), (0,1,u^3), (0,1,u^{24}), (0,1,u^{28})\}$$

where $f(x) = u^{29}x^{28} + u^5x^{26} + u^{18}x^{24} + u^2x^{22} + u^2x^{20} + x^{18} + u^{11}x^{16} + u^9x^{14} + u^{19}x^{12} + u^{26}x^{10} + u^{29}x^8 + u^{15}x^6 + u^{30}x^4 + u^{20}x^2 + u^6x$*, is a* $(0,2,4)$*-set for* Π*.*

Proof: The proof is by computation but we can describe the basic method of the search that led to this discovery. We used GAP and Magma for these computations. Firstly random arcs of size 18 were generated. The 16 tangents to each of the points on such an arc were collected, giving 288 lines. The points not on the arc that were each on exactly 16 of these lines were collected and if at least 18 such points were found, then 18-element subsets of this set were checked for being an arc. Two such arcs were found and indeed gave a word in the dual code, of weight 36. In order to express this set in the canonical form given in [19], the nucleus P was found, and then the coset $G_P g$ of the stabilizer, G_P, of P in the automorphism group G that mapped P onto the nucleus of the canonical form, i.e. $(0,0,1)$ in our notation, where we use $(1,0,0)'$ for the line at infinity (differing from [19] where $(0,0,1)'$ is used). With the added demand that the image of the arc should have $(1,0,0)'$ as a 4-secant, and contain the points $(1,0,0), (1,0,1), (0,1,0)$, a suitable element in $G_P g$ was found almost immediately. The interpolation function in Magma then found the polynomial f. ■

Acknowledgement

J. D. Key thanks the Institute of Mathematics and Physics at the Aberystwyth University for their hospitality. The authors thank the referees for their comments and constructive suggestions.

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] Aart Blokhuis, Tamás Szőnyi, and Zsuzsa Weiner. On sets without tangents in Galois planes of even order. *Des. Codes Cryptogr.*, 29:91–98, 2003.

[4] W. Bosma, J. Cannon, and C. Playoust. The Magma algebra system I: The user language. *J. Symb. Comp.*, 24, 3/4:235–265, 1997.

[5] J. Cannon, A. Steel, and G. White. Linear codes over finite fields. In J. Cannon and W. Bosma, editors, *Handbook of Magma Functions*, pages 3951–4023. Computational Algebra Group, Department of Mathematics, University of Sydney, 2006. V2.13, http://magma.maths.usyd.edu.au/magma.

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

[7] K. L. Clark, L.D. Hatfield, J. D. Key, and H. N. Ward. Dual codes of projective planes of order 25. *Adv. Geom.*, 3:140–152, 2003.

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

[9] K. L. Clark, J. D. Key, and M. J. de Resmini. Dual codes of translation planes. *European J. Combin.*, 23:529–538, 2002.

[10] R. Figueroa. A family of not (v, ℓ)-transitive projective planes of order q^3, $q \not\equiv 1 \pmod 3$ and $q > 2$. *Math. Z.*, 181:471–479, 1982.

[11] A. Gács and Zs. Weiner. On $(q + t, t)$-arcs of type $(0, 2, t)$. *Des. Codes Cryptogr.*, 29:131–139, 2003.

[12] GAP. Groups, Algorithms and Programming, Version 4. The GAP Group, Lehrstuhl D für Mathematik, RWTH Aachen, Germany and School of Mathematical and Computational Sciences, University of St. Andrews, Scotland. http://www-gap.dcs.st-and.ac.uk/ gap/.

[13] J. W. P. Hirschfeld. *Projective Geometries over Finite Fields*. Oxford: Clarendon Press, 1998. Oxford Mathematical Monographs.

[14] Norman L. Johnson, Vikram Jha, and Mauro Biliotti. *Handbook of Finite Translation Planes*. Chapman & Hall/CRC, Boca Raton, FL., 2007. Pure and Applied Mathematics, No. 289.

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

[16] 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.

[17] J. D. Key and M. J. de Resmini. An upper bound for the minimum weight of dual codes of Figueroa planes. *J. Geom.*, 77:102–107, 2003.

[18] J. D. Key and F. Ngwane. The minimum weight of the dual 7-ary code of a projective plane of order 49. *Des. Codes Cryptogr.*, 44:133–142, 2007.

[19] Gábor Korchmáros and Francesco Mazzocca. On $(q+t)$-arcs of type $(0, 2, t)$ in a desarguesian plane of order q. *Math. Proc. Cambridge Philos. Soc.*, 108:445–459, 1990.

[20] J. Limbupasiriporn. *Partial permutation decoding for codes from designs and finite geometries*. PhD thesis, Clemson University, 2005.

[21] Marialuisa J. de Resmini and Nicholas Hamilton. Hyperovals and unitals in Figueroa planes. *European J. Combin.*, 19:215–220, 1998.

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

[23] T. Szőnyi. Blocking sets in desarguesian affine and projective planes. *Finite Fields Appl.*, 3:187–202, 1997.