Ternary dual codes of the planes of order nine

J. D. Key
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

Abstract

We determine the minimum weight of the ternary dual codes of each of the four projective planes of order 9, and of the seven affine planes of order 9. The proof includes a construction of a word of small, sometimes minimal, weight in the dual code of any plane of square order containing a Baer subplane.

Dedicated to S. S. Shrikhande

Keywords: Designs, codes, finite geometries
AMS subject classification: 05

1 Introduction

The p-ary linear code obtained from a projective plane of order n divisible by p has long been known to have minimum weight $n+1$ and minimum weight vectors simply the scalar multiples of the incidence vectors of the lines. The dual code is not so well determined; bounds for the minimum weight are easy to establish, but the actual minimum weight in any case must be a function of the existence of a particular type of configuration in the plane. For example, in the case of the binary code of a projective plane of even order, the minimum possible weight is $n+2$ and the support of such a vector is a hyperoval in the plane. Up to fairly recently no planes without hyperovals were known, but we now know (see [16]) that there are planes of order 16 without hyperovals. In this case, the minimum weight turns out to be $n+4=20$: see [12].

The case of n odd is not as easy to describe, and in general the minimum weight is not known. In the case of $n=p$ a prime, the minimum weight is $2n$ in all known cases, all of which are desarguesian. Bounds are known from coding theory and geometry for the desarguesian case, since then the codes of the planes are generalized Reed-Muller, although the dual codes are not, unless n is a prime.

There are four projective planes of order 9: the desarguesian plane, Φ, the translation (Hall) plane, Ω, the dual translation plane, Ω^D, and the Hughes plane, Ψ: see [17, 13]. Here we prove the following:

Theorem 1 *Let Π be a projective plane of order 9. The minimum weight of the dual ternary code of Π is 15 if Π is Φ, Ω, or Ω^D, and 14 if Π is Ψ.*

Note that in fact the codes here are too large to be examined by current standard computational facilities, for example using Magma [5] on Sun stations. However, Magma was useful in searching for geometrical configurations of a particular type.

2 Notation and background

Notation will include $PG_{m,r}(F_q)$ to denote the design of points and r-dimensional subspaces of the projective space $PG_m(F_q)$, i.e. a 2-(v, k, λ) design with v points, k points per block, and any two points on exactly λ blocks, where

$$v = \frac{q^{m+1}-1}{q-1},\ k = \frac{q^{r+1}-1}{q-1},\ \lambda = \frac{(q^{m-1}-1)\dots(q^{m+1-r}-1)}{(q^{r-1}-1)\dots(q-1)}.$$

Similarly, $AG_{m,r}(F_q)$ will denote the 2-design of points and r-flats (cosets of dimension r) in the affine geometry $AG_m(F_q)$.

The code C_F 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; in the case of the designs from finite geometries, p will be the same as the characteristic of the field over which the geometry is defined. In the general case of a 2-design, the prime must divide the order of the design, i.e. $r - \lambda$, where r is the replication number for the design, that is, the number of blocks through a point. 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 $C_F = \left\langle v^B \mid B \in \mathcal{B} \right\rangle$, and is a subspace of $F^{\mathcal{P}}$. For any code C, the **dual** or **orthogonal** code $C^\perp$ is the orthogonal subspace under the standard inner product. 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.

For any design $\mathcal{D}$, a set of points is called an $(n_1, n_2, \dots, n_s)$-set if blocks of the design meet the set in n_i points for some i such that $1 \le i \le s$, and if for each i there exists at least one block meeting the set in n_i points. The n_i's are the **intersection numbers** for the set, and an n_i**-secant** is a block meeting the set in n_i points.

The following construction is used in [6] and we mention it here as it can be modified to help in the non-binary case for projective geometry designs of larger dimension: see Section 4.

Result 1 *Let $\mathcal{D} = PG_{m,1}(F_q)$ where $q = 2^t$ for $t \geq 1$, i.e. $\mathcal{D}$ is the 2-$(\frac{q^{m+1}-1}{q-1}, q+1, 1)$ design of points and lines in $\mathcal{P} = PG_m(F_q)$. Let $\mathcal{H}$ be a hyperplane in $\mathcal{P}$, and let $\mathcal{S}$ be a set of even type in $\mathcal{H}$, i.e. $\mathcal{S}$ is a set of points such that every line of $\mathcal{H}$ meets $\mathcal{S}$ evenly. Let V be a point of $\mathcal{P}$ that is not in $\mathcal{H}$. Then the set of points*

$$\mathcal{S}^* = \{X | X \text{ on a line } VY \text{ for } Y \text{ on } \mathcal{S}\} - \{V\}$$

is a set of even type for $\mathcal{D}$, of size $q|\mathcal{S}|$.

The known bounds in the general case are summed up in [1, Theorem 5.7.9] and are given as follows:

Result 2 *Let C be the p-ary code of the design $PG_{m,r}(F_q)$ or $AG_{m,r}(F_q)$ where $q = p^t$, $0 < r < m$ and p is prime. Then the minimum weight $d^\perp$ of $C^\perp$ satisfies*

$$(q+p)q^{m-r-1} \leq d^\perp \leq 2q^{m-r}.$$

See also Blake and Mullin [4, Section 2.2], Delsarte, Goethals and MacWilliams [9] or Delsarte [10, 8]. The lower bounds for the affine case are deduced in [8] from the BCH bound using the fact that the projective codes are cyclic and the affine codes are extended cyclic; the bound for the projective case follows by an induction argument given in [6]. The precise value for the binary case is determined in [6]; here we improve on the values for some cases when q is odd.

3 Odd order planes

Suppose Π is a projective plane of order $q = p^t$, where p is odd. Let $\mathcal{S}$ be a set of size s that is the support of a word in $C_p(\Pi)^\perp$. For $i = 0, \ldots, q+1$, let x_i denote the number of i-secants to $\mathcal{S}$; for a fixed point $y \notin \mathcal{S}$, let y_i denote the number of i-secants that pass through y; for a fixed point $z \in \mathcal{S}$, let z_i be the number of i-secants passing through z. Standard counting gives the following sets of equations, noting first that $x_1 = y_1 = z_1 = 0$ since $\mathcal{S}$ is the support of a codeword in the dual:

$$\sum_{i=0}^{q+1} x_i = q^2 + q + 1; \quad \sum_{i=2}^{q+1} i x_i = s(q+1); \quad \sum_{i=2}^{q+1} i(i-1)x_i = s(s-1), \tag{1}$$

and hence

$$\sum_{i=3}^{q+1} i(i-2)x_i = s(s-2-q), \tag{2}$$

(where the last equation is obtained from the previous two);

$$\sum_{i=0}^{q+1} y_i = q+1; \quad \sum_{i=1}^{q+1} i y_i = s, \tag{3}$$

and

$$\sum_{i=2}^{q+1} z_i = q+1; \quad \sum_{i=2}^{q+1} (i-1)z_i = s-1, \tag{4}$$

and hence

$$\sum_{i=3}^{q+1} (i-2)z_i = s-2-q, \tag{5}$$

(where the last equation is obtained from the previous two).

In all that follows let $C = C_p(\Pi)$ where p is an odd prime. Further, let w be a codeword in $C^\perp$ with support $\mathcal{S}$. The coordinate of w at the point x will be written $w(x)$. If $q = p$, then the only planes known are desarguesian and in this case the general theory of generalized Reed-Muller codes tells us that the minimum weight of $C^\perp$ is $2p$. Thus we exclude these cases from our arguments where necessary.

Lemma 2 *For any $q = p^t$ where $t > 1$, we have $s \geq q + 4$.*

Proof: Clearly $s \geq q + 2$; if $s = q + 2$ then every point is on $q + 1$ 2-secants. Thus if $w(x) = a$ at a point $x \in \mathcal{S}$, then w must take the value $-a$ on all the other $q+1$ points. Since the same must be true of any point, we have a contradiction.

Suppose $s = q + 3$. Then, from Equation (5), we have $z_3 + 2z_4 + \cdots = 1$, so that $z_i = 0$ for $i \geq 4$, and $z_3 = 1$, for any point of $\mathcal{S}$. Thus each point of $\mathcal{S}$ is on a unique 3-secant, and the entries in w at the points on this 3-secant must be the same, a say, and we can only possibly have $p = 3$. The entries at any other point must be $-a$, but since $q > 3$, there are more than six points, so we have a contradiction. □

Lemma 3 *For $q = 3^t$ where $t > 1$, we have $s \geq q + 5$.*

Proof: Suppose $s = q + 4$. Then, from Equation (5), we have $z_3 + 2z_4 + \cdots = 2$, so that $z_4 \leq 1$ for any point of $\mathcal{S}$. If $z_4 = 1$ for some point x, then if $w(x) = a$, we must have $w(y) = -a$ for every point off the 4-secant through x. Thus all the points on the 4-secant must take the same value a, which means that $4a = 0$ and thus $a = 0$, which is a contradiction. Thus $z_4 = 0$ for all the points, and thus $x_4 = 0$. From Equation (2) then $3x_3 = 2(q + 4)$, so that $3|(q + 1)$, which is impossible since $q = 3^t$. □

Lemma 4 *If $q = 9$ and $s = 14$, then $\mathcal{S}$ is the union of two disjoint Fano subplanes, neither of whose lines contains points of the other Fano subplane. Further, $\mathcal{S}$ is a $(0, 2, 3)$-set.*

Proof: Suppose $s = q+5$, so that, from Equation (5), we have $z_3+2z_4+3z_5+\cdots = 3$, which implies $z_5 \leq 1$ and $z_i = 0$ for $i \geq 6$. If $z_5 = 1$ for some point, then $z_3 = z_4 = 0$, and the entries in w at the points on the 5-secant must all be the same, which is

impossible. So $z_5 = 0$ for all the points, and hence $x_5 = 0$. Suppose that $z_4 = 1$ and $z_3 = 1$ for some point x. If $w(x) = a$, then all the points on the 3-secant have entry a, and the remaining points on the 4-secant must have entries a and $-a$. Every point not on these two lines must have entry $-a$, since the line joining it with x must be a 2-secant. Let z be a point on the 4-secant with $w(z) = a$ and let $y \neq x$ be a point on the 3-secant through x. Then the line yz must be a 3-secant and thus the third point on it must have coordinate a, contradicting what we have just said. Thus $z_4 = 1$ is impossible, and hence we must have $z_4 = 0$ and $z_3 = 3$ for all points of $\mathcal{S}$. The configuration described is thus all we can have, with $w(x) = a$ on the one Fano subplane, and $w(x) = -a$ on the other Fano subplane. □

Note: We will call a pair of Fano subplanes that satisfy the conditions of Lemma 4, **absolutely disjoint** complements of one another.

Proposition 5 *A projective plane of square order q^2 that contains a Baer subplane has words of weight $2q^2 - q$ in its p-ary dual code, where $p|q$.*

Proof: Suppose Π is the projective plane containing a Baer subplane, π. If $\mathcal{Q}$ is the set of points of π, and L is a line of Π that is a line of π, i.e. meets $\mathcal{Q}$ in $q + 1$ points, then, writing v^X for the incidence vector of a set X of points, we find that the vector $v^{\mathcal{Q}} - v^L$ is in the dual code of the design, and is of weight $2q^2 - q$. The intersection numbers for the set $\mathcal{S}$ which is the symmetric difference of $\mathcal{Q}$ and L are $(0, 2, q, q^2 - q)$. This set can clearly be found in an affine plane as well by taking for the line at infinity a tangent to the Baer subplane that meets L in π. □

Recall that the four projective planes of order 9 are: the desarguesian plane, Φ, the translation (Hall) plane, Ω, the dual translation plane, Ω^D, and the Hughes plane, Ψ. We now complete the proof of Theorem 1.

Proof of Theorem 1
It is well known that all the planes have Baer subplanes (see, for example, [15]), so all have words of weight 15 in the dual ternary code. Further, Φ has no Fano subplanes at all, so 15 must be the minimum weight, by Lemma 4. The Hall plane and its dual do have Fano subplanes, but no pairs of absolutely disjoint complements, so the minimum weight is 15 here too.

In the case of the Hughes plane Ψ, the Fano subplanes fall into three orbits under the collineation group of the plane, which, in the notation of Denniston [11], are α of length 5616, β of length 16,848, and γ of length 11,232. Using Magma [5] we tested all the Fano subplanes planes for a suitable absolutely disjoint complement, and found that the only such pairs that occur are both in the γ orbit. Using the Denniston notation

for points and lines, a suitable pair is the following:

$a3:$	$P3$	$S3$	$T3$	$a4:$	$P4$	$S4$	$V7$
$b3:$	$T3$	$V6$	$X6$	$b5:$	$T5$	$V7$	$Z8$
$d3:$	$S3$	$X6$	$Z6$	$d4:$	$S4$	$X8$	$Z8$
$g6:$	$V6$	$Z6$	$P3$	$g8:$	$Z8$	$P4$	$R5$
$i6:$	$P3$	$R3$	$X3$	$i8:$	$X8$	$P4$	$T5$
$k6:$	$Z6$	$R3$	$T3$	$k7:$	$R5$	$T5$	$S4$
$m3:$	$R3$	$S3$	$V6$	$m5:$	$R5$	$V7$	$X8$

Thus the code $C^{\perp}$ for the Hughes plane has minimum weight 14. □

Since the 3-ranks of the planes are well known, we now have completed the information on the parameters for the ternary codes of the four projective planes:

plane	code	dual
Φ	$[91, 37, 10]_3$	$[91, 54, 15]_3$
Ω	$[91, 41, 10]_3$	$[91, 50, 15]_3$
Ω^D	$[91, 41, 10]_3$	$[91, 50, 15]_3$
Ψ	$[91, 41, 10]_3$	$[91, 50, 14]_3$

The seven affine planes that can be obtained from the projective planes, i.e. one from Φ, and two each from the others, have the parameters:

plane	code	dual
Φ	$[81, 36, 9]_3$	$[81, 44, 15]_3$
Ω	$[81, 40, 9]_3$	$[81, 41, 15]_3$
Ω^D	$[81, 40, 9]_3$	$[81, 41, 15]_3$
Ψ	$[81, 40, 9]_3$	$[81, 41, 14]_3$

This was justified in the case of minimum weight 15 in the proof of Proposition 5, and for the affine planes from the Hughes plane, absolutely disjoint Fano planes can be found with the line at infinity exterior in each case.

Note: 1. By considering cases, it is not hard to show that the words of weight 15 described in Proposition 5 in the dual code of the ternary code of a projective plane of order 9, are the only words of this weight in the dual.
2. If the smallest weight for an incidence vector (i.e. a vector all of whose entries are 0 or 1) in the dual code is sought, we must look for an $(n_1, n_2, \ldots, n_s)$-set where all the n_i are divisible by 3. Clearly such a set must have at least 21 points, and if such a set existed it would be a $(0, 3)$-set, which does not exist, by Cossu [7] for the desarguesian plane, and according to [15, Section 5] for the other planes of order 9. (See also [3, 2] for desarguesian planes of other odd orders.) The next possibility is 24 (since the size of the set must be divisible by 3), and this does exist for each of the planes, simply

by taking the set of 24 points on four lines of a Baer subplane, through a point of the Baer subplane, that are not in the subplane. This gives a $(0, 3, 6)$-set. Thus 24 is the minimum size for a constant (i.e. $(0, 1)$) vector in each case. This construction works for any plane of square order q^2 with a Baer subplane, yielding a set of size $q(q^2 - 1)$ with intersection numbers $(0, q, q^2 - q)$.
3. Sachar [18] deduces the lower bound $\frac{4}{3}q + 2$ for any projective plane of odd order q, which agrees with our value of 14 for $q = 9$; he also mentions the Baer subplane construction for planes of square order. Further, he obtains some bounds for the minimum weight of the hull of a projective plane, i.e. $C \cap C^{\perp}$, which is just 18, in the case of order 9.
4. Magliveras and Tam [14] have some estimation of the weight enumerator of the ternary code of the desarguesian plane of order 9.

4 The general case

Values for the minimum weight of the dual codes of the p-ary codes of the geometry for $p > 2$ are known, in general, only for $q = p$. In this case the minimum weight for the designs of points and r-dimensional subspaces or flats in an m-dimensional projective or affine geometry is $2p^{m-r}$, since the codes here are generalized Reed-Muller codes and the lower and upper bounds in the affine case of Result 2 actually coincide. The minimum vectors are not constant in this case, and unlikely to be in the general case. Words of weight $2q^{m-r}$ are easily constructed, and this does provide an upper bound for the minimum weight: see [1, Chapter 5].

In some cases, however, we can construct words of smaller weight in the dual code: In fact, a construction as in Result 1, but placing signs on added points, will yield a word in the dual code for $PG_{m,1}(F_q)$ from a word in the dual code for $PG_{m-1,1}(F_q)$: we use the sign + for points on lines through V that meet the set for the hyperplane in a point with a positive sign, and $-$ for points on lines through V that meet in points with a negative sign. This will provide a vector in the dual code for $PG_{m,1}(F_q)$ of weight qs, where s is the weight of the word in the dual code for the hyperplane. For example, using the construction of Proposition 5 with a Baer subplane, we get a word of weight $(2q^2 - q)(q^2)^{m-2}$ in the dual code of the p-ary code for $PG_{m,1}(F_{q^2})$. This does work in the even case as well, but is not particularly useful, since the word will be larger than the minimum, except in the case $q^2 = 4$, where the construction gives a hyperoval.

Using this, we get an improvement on the upper bound in Result 2 in the case where q is a square:

Proposition 6 *Suppose $q = p^t$, where t is even and p is prime. Let C be the p-ary code of the design $PG_{m,r}(F_q)$ or $AG_{m,r}(F_q)$, where $0 < r < m$. Then the minimum*

weight $d^\perp$ of $C^\perp$ satisfies

$$(q+p)q^{m-r-1} \leq d^\perp \leq (2q-\sqrt{q})q^{m-r-1}.$$

Note: In the case where $q = p$, the upper bound of Result 2 is attained, so we cannot hope to do better in every case.

References

[1] 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).

[2] Simeon Ball and Aart Blokhuis. An easier proof of the maximal arcs conjecture. Preprint.

[3] Simeon Ball, Aart Blokhuis, and Francesco Mazzocca. Maximal arcs in Desarguesian planes of odd order do not exist. *Combinatorica*, 17:31–41, 1997.

[4] Ian F. Blake and Ronald C. Mullin. *The Mathematical Theory of Coding*. New York: Academic Press, 1975.

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

[6] Neil J. Calkin, Jennifer D. Key, and Marialuisa J. de Resmini. Minimum weight and dimension formulas for some geometric codes. *Des. Codes Cryptogr.*, 17:105–120, 1999.

[7] A. Cossu. Su alcune proprietá dei $\{k, n\}$-archi di un piano proiettivo sopra un corpo finito. *Rend. Mat. Appl.*, 20:271–277, 1961.

[8] P. Delsarte. *BCH* bounds for a class of cyclic codes. *SIAM J. Appl. Math.*, 19:420–429, 1970.

[9] P. Delsarte, J. M. Goethals, and F. J. MacWilliams. On generalized Reed-Muller codes and their relatives. *Inform. and Control*, 16:403–442, 1970.

[10] Philippe Delsarte. A geometric approach to a class of cyclic codes. *J. Combin. Theory*, 6:340–358, 1969.

[11] R. H. F. Denniston. Subplanes of the Hughes plane of order 9. *Proc. Cambridge Philos. Soc.*, 64:589–598, 1968.

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

[13] 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.

[14] Spyros S. Magliveras and Kok-Cheung Tam. On the ternary codes of the desarguesian plane of order 9. Technical report, University of Nebraska-Lincoln, 1986. Department of Computer Science, Report Series # 28.

[15] Tim Penttila and Gordon F. Royle. Sets of type (m, n) in the affine and projective planes of order nine. *Des. Codes Cryptogr.*, 6:229–245, 1995.

[16] Tim Penttila, Gordon F. Royle, and M. K. Simpson. Hyperovals in the known projective planes of order 16. *J. Combin. Des.*, 4:59–65, 1996.

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

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