Geometric Codes over Fields of Odd Prime Power Order

K. L. Clark and J. D. Key
Department of Mathematical Sciences
Clemson University
Clemson SC 29634, U.S.A.

Abstract

We obtain improved bounds for the minimum weight of the dual codes associated with the codes from finite geometries in the case of odd order, and some results that apply also to the dual codes of non-desarguesian planes of odd order.

1 Introduction

The duals of the codes associated with the designs from finite geometries over fields of prime power order q are the so-called "geometric codes" ([2, Chapter 2]) and are of importance in applications because they are cyclic and because the structure of the geometry allows these codes to be decoded using majority logic decoding: see, for example, [9]. The actual minimum weight of these codes is not known in general, apart from the case where the characteristic of the underlying geometry is even, or a prime, and other sporadic small cases. In [4] we obtained the value of the minimum weight when $q = 2^m$ for any m. Here we improve on the known bounds for the odd case, and prove

Proposition 1 *For any $m > n \geq 1$ let $\mathcal{D}$ be the design $PG_{m,n}(F_q)$ of points and n-dimensional subspaces of the projective geometry of dimension m over the field of order q, where $q = p^t$, with $t > 1$ and p odd. Let $d^\perp$ be the minimum weight of the dual code $C_p^\perp$ of the design. Then*

$$\frac{4(q^m-1)}{3(q^n-1)} + \frac{2}{3} \leq d^\perp \leq 2q^{m-n}.$$

If $p \neq 3$ then

$$\frac{3(q^m-1)}{2(q^n-1)} + \frac{1}{2} \leq d^\perp \leq 2q^{m-n}.$$

We exclude the case where $q = p$ since in this case the value for $d^{\perp}$ is known and is precisely $2q^{m-n}$. Further, the result implies the same bounds for the affine geometry designs, $AG_{m,n}(F_q)$, of points and n-flats.

Note that in fact the codes here are too large to be examined by current standard computational facilities, for example using Magma [3]. However, Magma was useful in searching for geometrical configurations of a particular type.

2 Notation and background

We write $PG_{m,n}(F_q)$ for the design of points and n-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

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

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

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 which case we write also C_p for C_F; 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 $F^{\mathcal{P}}$, 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 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. If c is a codeword then the **support** of c is the set of non-zero coordinate positions of c.

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 $1 \leq i \leq s$, 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 [4] and we mention it here as it can be modified to help in the non-binary case for projective geometry designs of larger dimension.

Result 1 *Let $\mathcal{D} = PG_{m,1}(F_q)$ where $q = 2^t$ for $t \geq 1$, and $m \geq 2$. Let $\mathcal{H}$ be a hyperplane in $\mathcal{P}$, and let $\mathcal{S}$ be 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*

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

has size $q|\mathcal{S}|$, and is met evenly by every line of $\mathcal{D}$.

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 $PG_{m,n}(F_q)$ or of $AG_{m,n}(F_q)$ where $q = p^t$, $t \geq 1$, $m > n \geq 1$ and p is prime. Then the minimum weight $d^\perp$ of $C^\perp$ satisfies*

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

See also Blake and Mullin [2, Section 2.2], Delsarte, Goethals and MacWilliams [6] or Delsarte [7, 5]. The lower bounds for the affine case are deduced in [5] 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 [4]. The precise value for the binary case is determined in [4]; here we improve on the values for some cases when q is odd.

3 New bounds

Suppose $\mathcal{D}$ is a 2-(v, k, λ) design with b blocks and with replication number r, the number of blocks through a point. Let $n = r - \lambda$ be the order of $\mathcal{D}$, and let p be a prime dividing n. Let $\mathcal{S}$ be any set of points of $\mathcal{D}$ that is the support of a word in $C_p(\mathcal{D})^\perp$. Let $|\mathcal{S}| = s$. For $i = 0, \ldots, k$, let x_i denote the number of i-secants to $\mathcal{S}$; for a fixed point $y \notin \mathcal{S}$, let y_i (or $y_i(y)$) denote the number of i-secants that pass through y; for a fixed point $z \in \mathcal{S}$, let z_i (or $z_i(z)$) 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:

$$\sum_{i=0}^{k} x_i = b; \quad \sum_{i=2}^{k} i x_i = sr; \quad \sum_{i=2}^{k} i(i-1)x_i = s(s-1)\lambda, \tag{1}$$

and hence

$$\sum_{i=3}^{k} i(i-2)x_i = s((s-1)\lambda - r), \tag{2}$$

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

$$\sum_{i=0}^{k} y_i = r; \quad \sum_{i=1}^{k} i y_i = s\lambda, \tag{3}$$

and

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

and hence

$$\sum_{i=3}^{k} (i-2) z_i = (s-1)\lambda - r, \tag{5}$$

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

Using this notation,

Definition 1 *A non-empty set of points $\mathcal{S}$ in a design $\mathcal{D}$ will be called a* j**-secant set** *if there exists an integer $j \geq 3$ such that $x_i = 0$ for $2 < i < j$, but $x_j \neq 0$.*

Thus any non-empty set of points that is not an arc will be a j-secant set for some $j \geq 3$.

In the following lemmas let $C = C_p(\mathcal{D})$ where p is an odd prime and where $\mathcal{D}$ is a 2-(v, k, λ) design. Further, let w be a non-zero codeword in $C^\perp$ with support $\mathcal{S}$. The coordinate of w at the point x will be written $w(x)$. If $\mathcal{S}$ is not a j-secant set for any $j \geq 3$, then $s = \frac{r}{\lambda} + 1$, from Equation (2), which is not possible.

Lemma 2 *For any $x \in \mathcal{S}$, $z_2(x) \geq 2r - (s-1)\lambda$.*

Proof: Write $z_i = z_i(x)$. Then $\sum_{i=2} z_i = r$, so that

$$z_2 = r - \sum_{i=3} z_i \geq r - \sum_{i=3} (i-2) z_i = r - \{(s-1)\lambda - r\} = 2r - (s-1)\lambda$$

by Equation (5). □

Note that since every block through $x \in \mathcal{S}$ must meet $\mathcal{S}$ again, $s \geq \frac{r}{\lambda} + 1$.

In our applications the design $\mathcal{D}$ will be either (i) a desarguesian projective geometry design, $PG_{m,n}(F_q)$, where $q = p^t$ is odd, or (ii) an odd-order projective plane. In the first case, we are looking for minimal words, so we can assume that $s \leq 2q^{m-n}$, since words of that weight are known to exist: see [1, Chapter 5]. Also we can assume the BCH bound that gives $s \geq (q+p)q^{m-n-1}$. Here, $\frac{r}{\lambda} = \frac{q^m - 1}{q^n - 1}$, and thus $s \leq 2q^{m-n} < 2\frac{r}{\lambda} + 1$. Thus from Lemma 2, we must have 2-secants. Further, if $q = p$ then we know that the minimum weight is $2q^{m-n}$, so we will omit this case.

In (ii), $r = q+1$ and $\lambda = 1$, and $\mathcal{D}$ need not be desarguesian. Although no non-desarguesian planes of prime order are known, they have not been proved not to exist, and thus in the plane case we will allow q to be a prime.

Lemma 3 *If $\mathcal{S}$ is a j-secant set of size s, then*

1. *for any $x \in \mathcal{S}$,*
$$z_2(x) \geq r\frac{j-1}{j-2} - \lambda\frac{s-1}{j-2};$$

2. $$s \geq \frac{2}{j}\left[\frac{r(j-1)}{\lambda} + 1\right].$$

Proof: For (1), note that for every $x \in \mathcal{S}$, $z_i = 0$ for $2 < i < j$ and $z_j(x) \neq 0$ for some x. Thus, for any point in $\mathcal{S}$, $z_2 = r - \sum_{i=j} z_i$, and

$$\sum_{i=j}(i-2)z_i = \lambda(s-1) - r \geq (j-2)\sum_{i=j} z_i = (j-2)(r-z_2),$$

which simplifies to the stated result.

For (2), by (1), every $x \in \mathcal{S}$ has $z_2 \geq \frac{1}{j-2}[r(j-1) - \lambda(s-1)]$. For some $x \in \mathcal{S}$, let $\mathcal{S}'(x) = \{y \in \mathcal{S} \mid xy \text{ is a 2-secant}\}$. Then with $s' = |\mathcal{S}'(x)|$, we have $\lambda s' \geq z_2$, so that $s' \geq \frac{1}{\lambda(j-2)}[r(j-1) - \lambda(s-1)]$. Recalling that w is a word with support $\mathcal{S}$, if $w(x) = a$ then $w(y) = -a$ for all $y \in \mathcal{S}'(x)$. Any such y is also on $z_2(y)$ 2-secants, and this number is also bounded below by (1). Clearly $\mathcal{S}'(x) \cap \mathcal{S}'(y) = \emptyset$, so $s \geq |\mathcal{S}'(x)| + |\mathcal{S}'(y)| \geq \frac{2}{\lambda(j-2)}[r(j-1) - \lambda(s-1)]$, which simplifies to give the stated result. □

Corollary 4 1. *If $\mathcal{D} = PG_{m,n}(F_q)$ where $q = p^t$ is odd, $t \geq 1$, $m > n \geq 1$, then the minimum weight $d^\perp$ of the dual code of the p-ary code of $\mathcal{D}$ satisfies*
$$d^\perp \geq \frac{4}{3}\frac{(q^m-1)}{(q^n-1)} + \frac{2}{3}.$$
If $p \geq 5$ then
$$d^\perp \geq \frac{3}{2}\frac{(q^m-1)}{(q^n-1)} + \frac{1}{2}.$$

2. *If $\mathcal{D}$ is a projective plane of odd order $q = p^t$, then $d^\perp \geq \frac{4}{3}q + 2$. If $p \geq 5$ then $d^\perp \geq \frac{3}{2}q + 2$.*

Proof: The first parts in each case follow from Lemma 3 (2), by taking $j \geq 3$ and recalling that $\frac{r}{\lambda} = \frac{q^m-1}{q^n-1}$.

Now take $p \geq 5$. If $x_3 \neq 0$ then there exists a 3-secant. The values of $w(x)$ for these three points must be distinct, since $p \geq 5$. Thus arguing as in the proof of Lemma 3 (2), we see that

$$s \geq \frac{4}{\lambda}(2r - \lambda(s-1)) = 8\frac{r}{\lambda} - 4(s-1),$$

which simplifies to

$$s \geq \frac{8}{5}\frac{(q^m-1)}{(q^n-1)} + \frac{4}{5}.$$

If $x_3 = 0$ then $\mathcal{S}$ is a j-secant set where $j \geq 4$, so Lemma 3 (2) with $j = 4$, gives immediately

$$s \geq \frac{3}{2}\frac{(q^m-1)}{(q^n-1)} + \frac{1}{2}.$$

Since

$$\frac{8}{5}\frac{(q^m-1)}{(q^n-1)} + \frac{4}{5} \geq \frac{3}{2}\frac{(q^m-1)}{(q^n-1)} + \frac{1}{2},$$

we have the result. □

Note:
1. The bound $\frac{4}{3}q + 2$ for odd-order planes was also found by Sachar [10].
2. The bounds given in Corollary 4 are better than

(i) the BCH bound $(q+p)q^{m-n-1}$ if $q = p^t$ where p is odd and $t \geq 2$, when $\mathcal{D} = PG_{m,n}(F_q)$;

(ii) $q + p$ for planes of order $q = p^t$ where p is odd and $t \geq 2$.

3. The bounds will hold for the dual codes of the affine designs $AG_{m,n}(F_q)$ as well.

4 Words of small weight

When the order of the plane is a square, we have the following small words (also noted in Sachar [10]):

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. □

Actual 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 n-dimensional subspaces or flats in an m-dimensional projective or affine geometry is $2p^{m-n}$, 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 are unlikely to be in the general case. Words of weight $2q^{m-n}$ are easily constructed, and this does provide an upper bound for the minimum weight: see [1, Chapter 5].

Recall that we have the following inclusions:

$$C_p(PG_{m,1}(F_q)) \geq C_p(PG_{m,2}(F_q)) \geq \ldots \geq C_p(PG_{m,m-1}(F_q)),$$

so that

$$C_p^{\perp}(PG_{m,1}(F_q)) \leq C_p^{\perp}(PG_{m,2}(F_q)) \leq \ldots \leq C_p^{\perp}(PG_{m,m-1}(F_q)).$$

Thus we see that if $\mathcal{D} = PG_{m,n}(F_q)$ and if $c \in C_p^{\perp}(\mathcal{D})$, then $c' \in C_p^{\perp}(PG_{m+1,n+1}(F_q))$ for any larger space, where c' has the same support as c, and zeros in the new positions. This gives

Proposition 6 *For any $q = p^t$ and $m > n \geq 1$, if $C_p^{\perp}(PG_{2,1}(F_q))$ contains a word of weight a, then $C_p^{\perp}(PG_{m,n}(F_q))$ contains a word of weight aq^{m-n-1}.*

Proof: Notice that the vertex-cone construction allows us to construct a word of weight aq in the dual code of $C_p(PG_{m,1}(F_q))$ from a word of weight a in the dual code of $C_p(PG_{m-1,1}(F_q))$. This is achieved by placing the entry α in a coordinate position of the side of the cone if the side meets the hyperplane at a point with entry α. Now use the facts discussed above. □

Using the Baer subplane construction in the plane of square order we thus obtain:

Corollary 7 *For any $q = p^{2t}$, where $t \geq 1$, if C is the p-ary code of $PG_{m,n}(F_q)$ where $m > n \geq 1$, and $d^{\perp}$ is the minimum weight of $C^{\perp}$, then*

$$\frac{4(q^m - 1)}{3(q^n - 1)} + \frac{2}{3} \leq d^{\perp} \leq (2q - \sqrt{q})q^{m-n-1}.$$

We note also that the vertex-cone construction will also give a word of weight qs in the dual of the p-ary code of the design $PG_{m+1,r}(F_q)$ from a word of weight s in the dual code of the design $PG_{m,r}(F_q)$, as a simple argument will show.

5 Special cases

It is not easy to be more precise about the bounds in the general case. We can say the following for the design $PG_{m,m-1}(F_9)$:

Proposition 8 *Let $\mathcal{D}$ be the design $PG_{m,m-1}(F_9)$, $m \geq 2$, and let C be the ternary code of $\mathcal{D}$. If $d^\perp$ denotes the minimum weight of $C^\perp$, then $d^\perp \in \{14, 15\}$.*

Proof: By Corollary 4,

$$d^\perp \geq \frac{4}{3}\frac{(q^m-1)}{(q^{m-1}-1)} + \frac{2}{3},$$

so that with $q = 9$ this gives $d^\perp \geq 13$. (We know that for $m = 2$, $d^\perp = 15$ by [8].) We prove that 13 is impossible by induction, knowing this to be true for $m = 2$.

Let $\mathcal{S}$ be the support of a word $c \in C^\perp$ where C is the ternary code of the design $\mathcal{D} = PG_{m,m-1}(F_9)$. Then $|S| = s \geq 13$. If $\mathcal{S}$ is a j-secant set in $\mathcal{D}$ for some $j \geq 4$ then, by Lemma 3 (2), we have

$$s \geq \frac{1}{2}\left[3\frac{(q^m-1)}{(q^{m-1}-1)} + 1\right],$$

which with $q = 9$ yields that $s \geq 15$, as required. Thus we can assume that $\mathcal{S}$ is not a j-secant set for $j \geq 4$. This implies that $x_3 \neq 0$, using the notation of Equation (1), since if not we would have, by Equation (2), $s = \frac{r}{\lambda} + 1$, which is impossible.

If $\mathcal{S}$ is inside some hyperplane of $\mathcal{D}$, then we have the result by the induction hypothesis that $s \neq 13$, since $\mathcal{S}$ would give the support of a codeword in the dual of the ternary code of the hyperplane's design. So suppose that $x_n \neq 0$ where $n < s$, i.e. $\mathcal{S}$ meets a hyperplane $\mathcal{H}$ in $n < s$ points. Let $\mathcal{T} = \mathcal{H} \cap \mathcal{S}$ and look at the codeword c restricted to $\mathcal{H}$; call it c^*. If c^* is in the dual of the code of the ternary code of the design of points and hyperplanes of $\mathcal{H}$, then we contradict the induction hypothesis. Thus the incidence vector of some hyperplane $\mathcal{H}_1$ of $\mathcal{H}$ does not have inner product 0 with c^*, and so every hyperplane of $\mathcal{D}$ that contains $\mathcal{H}_1$ must meet $\mathcal{S}$ again. There are 9 more hyperplanes, so we obtain $s \geq 9 + n$, i.e. $n \leq 4$ if $s = 13$, and $n \leq 5$ if $s = 14$. Either way, $x_n = 0$ for $n \geq 6$.

Denote by X_n the number of lines of $PG_m(F_9)$ meeting $\mathcal{S}$ in n points, and suppose that $s = 13$. Then $x_n = 0$ for $n \geq 5$ and hence also $X_t = 0$ for $t \geq 4$. We also have that $x_3 \neq 0$; if $X_3 = 0$ then $\mathcal{S}$ is an arc and this is not possible for $s = 13$ (since then $s - 1 = r$, which is too large for $m \geq 3$). Thus $X_3 \neq 0$, and there is a line ℓ meeting $\mathcal{S}$ in three points, a, b and c say. Denote the remaining points of $\mathcal{S}$ by p_i for $i \in \{1..10\}$; each must be on a distinct hyperplane with ℓ. Since $\mathcal{S}$ is the support of a word in the dual code, the only possible arrangement of the field elements at the coordinate positions corresponding to $\mathcal{S}$ is effectively $+1$ at a and b and -1 at all the other positions. We show that this cannot happen. Consider a hyperplane containing $\{a, p_1, p_2\}$. It must contain another point, and the only possibility is b, and hence c also, which is a contradiction, since $x_i = 0$ for $i \geq 5$. Thus we have shown that we cannot have $s = 13$. $\square$

An apparently non-contradictory possibility for a word of weight 14 is one inside 3-space with the following properties, using the same notation as in the last proposition, and taking $m = 3$: $x_i = 0$ except for $i = 0, 2, 3, 5$ and $x_3 = 72$, $x_5 = 22$ and $X_i = 0$ except for $i = 0, 1, 2, 4$ and $X_4 = 1$. We have not been able to determine if such a set can be constructed. If it can, then the minimum weight will be 14 for all $m \geq 3$.

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

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

[4] 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.

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

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

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

[8] J. D. Key and M. J. de Resmini. Ternary dual codes of the planes of order nine. J. Statist. Plann. Inference, To appear.

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

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