

AFFINE BLOCKING SETS, THREE-DIMENSIONAL CODES AND THE GRIESMER BOUND

SIMEON BALL AND ELISA MONTANUCCI

ABSTRACT. We construct families of three-dimensional linear codes that attain the Griesmer bound and give a probabilistic construction of linear codes that are close to the Griesmer bound. All these codes contain the all-1 codeword and are constructed from small multiple blocking sets in $AG(2, q)$.

1. INTRODUCTION

A linear $[n, k, d]$ -code over \mathbb{F}_q is a subspace C of rank k of the vector space \mathbb{F}_q^n in which every non-zero vector in C has at least d non-zero co-ordinates and some vector in C has exactly d non-zero co-ordinates. The Griesmer bound [14, Theorem 5.2.6], states that

$$(1.1) \quad n \geq \sum_{i=0}^{k-1} \left\lceil \frac{d}{q^i} \right\rceil.$$

Our aim in this note is to construct three dimensional linear codes ($k = 3$) which meet the Griesmer bound.

Let G be a $k \times n$ matrix whose rows form a basis of C , i.e. G is a generator matrix for C , and let $x \in \mathbb{F}_q^k$ be the j -th column of G . The codeword that is the linear combination of the rows of G given by the vector $a \in \mathbb{F}_q^k$ has a zero in the j -th coordinate if and only if

$$(1.2) \quad \sum_{i=1}^k a_i x_i = 0.$$

Since each codeword has at least d non-zero coordinates there are at most $n - d$ columns of G incident with the hyperplane defined by the equation (1.2). Note that this property holds for any non-zero scalar multiple of the columns. If we view the columns of G as points of $PG(k - 1, q)$ we have that a linear $[n, k, d]$ -code C over \mathbb{F}_q is equivalent to a set K of n points in $PG(k - 1, q)$ with the property that some hyperplane is incident with r points of K and no hyperplane is incident with more, where $r = n - d$. Such a set of points K is called an (n, r) -arc.

Putting $d = n - r$ in (1.1) it follows that an (n, r) -arc in $PG(k - 1, q)$ is equivalent to a code meeting the Griesmer bound if

$$r = \sum_{i=1}^{k-1} \left\lceil \frac{n - r}{q^i} \right\rceil.$$

Date: 21 June 2005.

The first author acknowledges the support of the Ministerio de Ciencia y Tecnologia, España.

Now if $n - r \leq q^2$ the last $k - 2$ terms in the sum all contribute exactly one. So if $d \leq q^2$ we have equality if and only if

$$(1.3) \quad (r - k + 1)q + r + 1 \leq n \leq (r - k + 2)q + r.$$

If $k = 2$ then finding such codes is trivial. Indeed it suffices to take any (multi-)set of n points of $PG(1, q)$ where no point is chosen with multiplicity more than r .

If $k = 3$ then the only values of r for which it is known that there is a code of length n within these bounds are, for $q = p^h$ odd,

$$r \in \{2, 3, (q + 1)/2, (q + 3)/2, q - p^e, q - 2, q \mid e = 0, 1, \dots, h - 1\},$$

for q even

$$r \in \{2^e, 3, q - 2^e, q \mid e = 0, 1, \dots, h - 1\},$$

with the addition of

$$r \in \{\sqrt{q} + 1, q - \sqrt{q} + 2, q - \sqrt{q} + 3, \dots, q - 3\}$$

when q is square, see [3].

We shall construct explicit codes meeting the Griesmer bound when $r = q - 3$ and $q - 4$.

Apart from trivial bounds nothing is known in general for a given r and q about how close a code can be to the Griesmer bound. If $d \leq q^2$ an (n, r) -arc is equivalent to a code that is ϵ away from the Griesmer bound if and only if

$$(1.4) \quad (r - k + 1 - \epsilon)q + r + 1 \leq n \leq (r - k + 2 - \epsilon)q + r.$$

We shall also show, by means of an algorithmic construction, that there are codes one away from the Griesmer bound for all $q - (8q)^{1/5} \leq r < q$.

To conclude the introduction we note that a three dimensional code ($k = 3$) with $d > q^2$ has multiple columns in its generator matrices and hence the minimum distance of the dual code is 2. These codes are of less interest and we do not consider them here.

2. CODES CONTAINING THE ALL-1 CODEWORD AND AFFINE BLOCKING SETS

If a code C contains the all-1 codeword then we can assume that the first row in the generator matrix of the code is the all-1 vector and every point of the (n, r) -arc K constructed from C as in the previous section will have a 1 in its first coordinate. Hence K is a subset of the points of $AG(k - 1, q)$. The same argument in reverse implies that if an (n, r) -arc is contained in $AG(k - 1, q)$ then the corresponding linear $[n, k, d]$ -code will contain the all-1 codeword.

A t -fold blocking set B of $AG(k - 1, q)$ is a set of points with the property that every hyperplane of $AG(k - 1, q)$ is incident with at least t points of B and some hyperplane is incident with exactly t points of B . The complement of an (n, r) -arc in $AG(k - 1, q)$ is a $(q^{k-2} - r)$ -fold blocking set of size $q^{k-1} - n$.

In [7], Bruen proves the lower bound

$$|B| \geq (k + t - 2)q - k - t + 1.$$

This bound, translated to codes containing the all-1 codeword by substituting $t = q^{k-2} - r$ and $|B| = q^{k-1} - n$, implies

$$n \leq (r - k + 2)q + q^{k-2} - r - 1 + k.$$

Compare this to (1.3).

Some improvements are made to Bruen's bound in [2], including the following in the case $k = 3$,

$$(2.1) \quad |B| \geq (t + 1)q - (t, q).$$

This bound first appeared in [1]; the case $(t, q) = 1$ having previously been obtained by Blokhuis in [4]. This bound in terms of codes containing the all-1 codeword, substituting $t = q - r$ and $|B| = q^2 - n$, gives

$$n \leq rq - q + (r, q).$$

3. THE GENERAL CONSTRUCTION

Let S be a set of t points in $PG(2, q)$ with the property that no three of its points are collinear. A line is a *bisecant* to S if it is incident with exactly two points of S and an *external line* if it is incident with no points of S . Let $L(S)$ be a subset of the external lines to S with the property that a point not in S incident with m bisecants of S is incident with $m - 1$ lines of $L(S)$.

Hill points out at the end of his article [9] that the set B , that consists of points dual to lines of $L(S)$ together with the points lying on a line dual to a point of S , forms a $(t - 1)$ -fold blocking set of $PG(2, q)$ of size

$$t(q + 1) - \binom{t}{2} + |L(S)|.$$

This is easily seen for if a line is incident with m of the points that lie on two lines dual to the points of S then it is incident $m - 1$ points of the dual of $L(S)$ and hence

$$t - 2m + m + m - 1 = t - 1$$

points of B .

By removing a line, dual to a point of S , one can make a $(t - 2)$ -fold blocking set of $AG(2, q)$ of size

$$(t - 1)(q + 1) - \binom{t}{2} + |L(S)|.$$

The bound (2.1) gives the lower bound

$$(3.1) \quad |L(S)| \geq \binom{t - 1}{2} - (t - 2, q).$$

The corresponding code has length $q^2 + q + 1 - |B|$ and minimum distance $n - q - 2 + t$ and will meet the Griesmer bound, according to (1.3) if

$$|L(S)| \leq \binom{t}{2} - 2.$$

In the next section we give a probabilistic construction of such a set S and $L(S)$ which gives codes that are one away from the Griesmer bound. In Section 5 we give explicit constructions of sets S and their corresponding sets of lines $L(S)$ which produce codes meeting the Griesmer bound and which are good in the sense that $L(S)$ is small. In some cases $|L(S)|$ attains the bound (3.1).

4. A NON-EXPLICIT CONSTRUCTION

Let S_t be a set of t points in $PG(2, q)$ with the property that no three of its points are collinear and that no three of its bisecants are concurrent. In the terminology of [11], S_t is a t -arc with $c_m = 0$ for $m \geq 3$.

Suppose that $t \geq 4$ and that S_t is contained in the set of points of a large arc of size about q , a conic for example. There are $\binom{t}{2}$ bisecants and there are $3\binom{t}{4}$ points incident with exactly two bisecants, every four points of S_t determines three pairs of bisecants. At worst there are

$$3(t-4)\binom{t}{4}$$

points of the large arc that we cannot add to S_t without destroying the property that no point is incident with three bisecants. Hence if $3(t-4)\binom{t}{4} < q-t$ we can extend S_t to set S_{t+1} .

Now fix $t < (8q)^{1/5}$ and put $S = S_t$. Let $L(S)$ be a set of external lines that cover every point on two bisecants constructed by simply choosing any external line through such a point in order until all such points are covered. Then

$$|L(S)| \leq 3\binom{t}{4}$$

and we have a $(t-1)$ -fold blocking set of size at most

$$t(q+1) - \binom{t}{2} + 3\binom{t}{4}$$

and an (n, r) -arc in $PG(2, q)$ where $r = q + 2 - t$ and

$$n \geq (r-1)q + 1 - t + \binom{t}{2} - 3\binom{t}{4}$$

which is one away from the Griesmer bound according to (1.4) since $t < (8q)^{1/5}$.

5. EXPLICIT EXAMPLES

In all but the first example, the set of t points S was found by choosing a subgroup G of $GL(3, q)$ and looking for orbits of length t whose points lying on at least two bisecants can be covered (with multiplicity) by relatively few lines. i.e. $|L(S)|$ is small. In some cases this set of lines $L(S)$ is the union of the G -orbits and so G is a subgroup of the group of the corresponding code, and in other cases not. The idea of prescribing a stabiliser group to construct linear codes and (n, r) -arcs was first used, and with considerable success for small q , in [5] and [6].

If $t = 4$ then there is but one choice for S , and $L(S)$ can be chosen such that $|L(S)| = 1$ if q is even and $|L(S)| = 2$ if q is odd, see [10].

We use the notation (x, y, z) to be the projective point $\langle(x, y, z)\rangle$ and $[a, b, c]$ to be the projective line which is incident with (x, y, z) if and only if $ax + by + cz = 0$.

5.1. $t = 5$. A 4-fold blocking set in $PG(2, q)$ of size $5q + 1$, $\text{char} > 3$, where char is the characteristic of q .

Let S be the set of points

$$\{(1, 0, 0), (1, 1, 1), (1, 2, 4), (1, 3, 9), (1, 3/2, 9/4)\}$$

contained in the conic $X_0X_2 = X_1^2$. Put $y_i = (1, i, i^2)$.

The three points incident with two bisecants to S that lie on the bisecant $\langle y_0, y_1 \rangle$ are $\{(2, 3, 3), (5, 6, 6), (7, 9, 9)\}$.

The three points incident with two bisecants to S that lie on the bisecant $\langle y_0, y_2 \rangle$ are $\{(2, 3, 6), (1, 3, 6), (5, 9, 18)\}$.

The three points incident with two bisecants to S that lie on the bisecant $\langle y_0, y_3 \rangle$ are $\{(0, 1, 3), (1, -3, -9), (1, 6, 18)\}$.

The three points incident with two bisecants to S that lie on the bisecant $\langle y_0, y_{\frac{3}{2}} \rangle$ are $\{(3, 4, 6), (5, 6, 9), (7, 12, 18)\}$.

The three points that are incident with two of the six bisecants spanned by y_1, y_2, y_3 and $y_{\frac{3}{2}}$ are $\{(3, 5, 9), (1, 0, -3), (5, 9, 15)\}$.

If the $\text{char} > 3$ then these points are all distinct and are the 15 points that are incident with exactly two bisecants of S . It is a laborious task to verify that the lines

$$\{[-3, 3, -1], [18, -24, 7], [9, -18, 7], [3, 0, -1], [18, -21, 7], [6, -5, 0]\}$$

are external lines to S and cover these 15 points. To be precise and labelling the points in the order they appear from 1 to 15, $[-3, 3, 1]$ is incident with 1, 5, 7 and 14. The line $[18, -24, 7]$ is incident with 6, 9 and 10. The line $[9, -18, 7]$ is incident with 8 and 11. The line $[3, 0, -1]$ is incident with 4, 13 and 15. The line $[18, -21, 7]$ is incident with 3 and 12. The line $[6, -5, 0]$ is incident with 2.

Therefore if we let $L(S)$ be this set of six lines then we satisfy the required property for the construction in section 3. The lower bound (3.1) gives $|L(S)| \geq 5$ so we do not quite manage to attain the bound in this case. However we do get a code meeting the Griesmer bound since we satisfy the bound (1.3) $|L(S)| \leq 8$.

In 1984, Mason [13] constructed 4-fold blocking sets of $PG(2, q)$ of size $5q - 2$ when $\text{char} = 3$. These examples contain exactly 3 lines as opposed to 5.

5.2. $t = 5$. A 4-fold blocking set in $PG(2, q)$ of size $5q + 1$, $q = 1 \pmod{5}$.

Let $q = 1 \pmod{5}$, $e^5 = 1$, $e \neq 1$. Let G be the group generated by $\sigma : (x, y, z) \mapsto (x, ye, ze^2)$ and $\tau : (x, y, z) \mapsto (z, y, x)$. Since G has a transitive action of degree 5 on the orbit of $(1, 1, 1)$ and has order 10 it follows that $G \cong ASL(1, 5)$, [8, Table 2.1, pp.60]. Now let S

be the G -orbit of $x = (1, 1, 1)$, i.e.

$$S = Gx = \{(1, 1, 1), (1, e, e^2), (1, e^2, e^4), (1, e^3, e), (1, e^4, e^3)\}.$$

Let $y_0 = (1, 0, -1)$, $y_1 = (e + e^2, e^3 + 1, e + e^2)$ and $y_2 = (e + e^3, e^4 + 1, e + e^3)$ and $z_i = (1, e^i, e^{2i})$. The lines $\langle z_1, z_4 \rangle$ and $\langle z_2, z_3 \rangle$ meet in y_0 , since

$$\begin{vmatrix} 1 & e & e^2 \\ 1 & e^4 & e^3 \\ 1 & 0 & -1 \end{vmatrix} = \begin{vmatrix} 1 & e^2 & e^4 \\ 1 & e^3 & e \\ 1 & 0 & -1 \end{vmatrix} = 0.$$

The lines $\langle z_1, z_2 \rangle$ and $\langle z_3, z_4 \rangle$ meet in y_1 , since

$$\begin{vmatrix} 1 & e & e^2 \\ 1 & e^2 & e^4 \\ e + e^2 & e^3 + 1 & e + e^2 \end{vmatrix} = \begin{vmatrix} 1 & e^3 & e \\ 1 & e^4 & e^3 \\ e + e^2 & e^3 + 1 & e + e^2 \end{vmatrix} = 0.$$

The lines $\langle z_1, z_3 \rangle$ and $\langle z_2, z_4 \rangle$ meet in y_2 , since

$$\begin{vmatrix} 1 & e & e^2 \\ 1 & e^3 & e \\ e + e^3 & e^4 + 1 & e + e^3 \end{vmatrix} = \begin{vmatrix} 1 & e^2 & e^4 \\ 1 & e^4 & e^3 \\ e + e^3 & e^4 + 1 & e + e^3 \end{vmatrix} = 0.$$

Now y_0, y_1 and y_2 lie in different G -orbits, so the 15 points that lie on exactly 2 bisecants of S are $Gy_0 \cup Gy_1 \cup Gy_2$. The line $[0, 1, 0]$ is incident with all the points in the G -orbit of $y_0 = (1, 0, -1)$ and is external to S . The line $[e^2 - e - 1, e^2 + e, -e(e^2 + e - 1)]$ is incident with both y_1 and $\sigma(y_2) = (e + e^3, e + 1, e^3 + 1)$ and is external to S . So if we let $L(S)$ be the union of the orbit of this line under $\langle \sigma \rangle$ together with $[0, 1, 0]$ then S and $L(S)$ satisfy the required property for the construction in section 3 and $|L(S)| = 6$. The lower bound (3.1) in this case is $|L(S)| \geq 5$.

5.3. $t = 6$. A 5-fold blocking set in $PG(2, q)$ of size $6q$, $q = 1 \pmod{4}$.

Let G be the group generated by $\sigma : (x, y, z) \mapsto (z, x, y)$ and $\tau : (x, y, z) \mapsto (x, y, -z)$. Since $q = 1 \pmod{4}$ there exists an element a satisfying $a^2 = -1$. Let S be the G -orbit of the point $(1, a, 0)$ i.e.

$$S = \{(1, a, 0), (0, 1, a), (1, 0, -a), (0, 1, -a), (1, 0, a), (1, -a, 0)\}.$$

The lines $\langle (1, a, 0), (0, 1, a) \rangle$, $\langle (1, -a, 0), (0, 1, -a) \rangle$ and $\langle (1, 0, a), (1, 0, -a) \rangle$ are all incident with the point $(1, 0, 1)$. Thus the set of points in the G -orbit of this point

$$D = \{(1, 0, 1), (1, 0, -1), (1, -1, 0), (0, 1, 1), (0, 1, -1), (1, 1, 0)\},$$

is a set of 6 points all incident with exactly 3 bisecants of S .

The lines $\langle (1, a, 0), (0, 1, a) \rangle$ and $\langle (1, -a, 0), (1, 0, a) \rangle$ are incident with the point $y_1 = (1, 1, a + 1)$ since

$$\begin{vmatrix} 1 & a & 0 \\ 0 & 1 & a \\ 1 & 1 & a + 1 \end{vmatrix} = \begin{vmatrix} 1 & -a & 0 \\ 1 & 0 & a \\ 1 & 1 & a + 1 \end{vmatrix} = 0,$$

and so the 12 points in the G -orbit of this point $C_1 = Gy_1$ are all points incident with exactly 2 bisecants of S .

The lines $\langle(1, -a, 0), (0, 1, a)\rangle$ and $\langle(1, a, 0), (1, 0, a)\rangle$ are incident with the point $y_2 = (1, 1, a - 1)$ since

$$\begin{vmatrix} 1 & -a & 0 \\ 0 & 1 & a \\ 1 & 1 & a-1 \end{vmatrix} = \begin{vmatrix} 1 & a & 0 \\ 1 & 0 & a \\ 1 & 1 & a-1 \end{vmatrix} = 0,$$

and so the 12 points in the G -orbit of this point $C_2 = Gy_2$ are all points incident with exactly 2 bisecants of S . Clearly the points of $C_3 = \{(0, 0, 1), (1, 0, 0), (0, 1, 0)\}$ are also points incident with exactly 2 bisecants of S . Since there are at least six points incident with 3 bisecants of S , a simple counting argument shows there are at most 27 points incident with exactly two bisecants. Thus $C_1 \cup C_2 \cup C_3$ is the set of all points incident with exactly two bisecants of S and D is the set of all points incident with exactly three bisecants of S .

The lines

$$\{[1, 0, 1], [1, 0, -1], [1, -1, 0], [0, 1, 1], [0, 1, -1], [1, 1, 0]\}$$

are incident with 2 points of C_1 , 2 points of C_2 , a point of C_3 and a point of D and it's a simple matter to check they cover the points of $C_1 \cup C_2 \cup C_3 \cup D$. Since $a \neq +1, -1$ they are external lines to S . The lines

$$\{[1, 1, -1], [1, -1, 1], [1, -1, -1]\}$$

cover the points of D and are also external to S . Let $L(S)$ be the union of these six and three lines. Thus $L(S)$ has the required property from section 3. Moreover it attains the lower bound (3.1) since $|L(S)| = \binom{t-1}{2} - (t-2, q) = 9$.

5.4. $t = 6$. A 5-fold blocking set in $PG(2, q)$ of size $6q$, some restrictions.

Let G be the symmetric group on 3 elements consisting of the permutations of the coordinates of the points of $PG(2, q)$. Let $a \neq 0, \pm 1$ and S be the G -orbit of the point $x = (1, a, 0)$, i.e.

$$S = Gx = \{(0, a, 1), (1, a, 0), (1, 0, a), (0, 1, a), (a, 0, 1), (a, 1, 0)\}.$$

The lines $\langle(0, a, 1), (0, 1, a)\rangle$, $\langle(1, a, 0), (1, 0, a)\rangle$ and $\langle(a, 0, 1), (a, 1, 0)\rangle$ are all incident with the point $(0, 1, -1)$. Hence the three points in the G -orbit of $(0, 1, -1)$

$$D = \{(0, 1, -1), (1, 0, -1), (1, -1, 0)\}$$

are incident with exactly 3 bisecants of S .

The point $y_1 = (1, 0, -a^2)$ is incident with the lines $\langle(1, a, 0), (0, 1, a)\rangle$ and $\langle(a, 0, 1), (1, 0, a)\rangle$ and $|Gy_1| = 6$ if we choose $a^4 \neq 1$.

The point $y_2 = (0, 0, 1)$ is incident with the lines $\langle(0, a, 1), (0, 1, a)\rangle$ and $\langle(a, 0, 1), (1, 0, a)\rangle$ and $|Gy_2| = 3$.

The point $y_3 = (1, 1, a-1)$ is incident with the lines $\langle(1, a, 0), (1, 0, a)\rangle$ and $\langle(a, 1, 0), (0, 1, a)\rangle$ and $|Gy_3| = 3$ if we choose $a \neq 2$.

The point $y_4 = (1, 1, (a-1)/a^2)$ is incident with the lines $\langle(1, a, 0), (a, 0, 1)\rangle$ and $\langle(a, 1, 0), (0, a, 1)\rangle$ and $|Gy_4| = 3$ if we choose $a^2 - a + 1 \neq 0$.

The point $y_5 = (1, 1, a-a^2)$ is incident with the lines $\langle(1, a, 0), (0, 1, a)\rangle$ and $\langle(a, 1, 0), (1, 0, a)\rangle$ and $|Gy_5| = 3$ if we choose $a^2 - a + 1 \neq 0$.

The point $y_6 = (1, 1, (1-a)/a)$ is incident with the lines $\langle(1, a, 0), (0, a, 1)\rangle$ and $\langle(a, 1, 0), (a, 0, 1)\rangle$ and $|Gy_6| = 3$ if we choose $2a \neq 1$.

The point $y_7 = (1, 1, (a^2+1)/a)$ is incident with the lines $\langle(1, 0, a), (0, a, 1)\rangle$ and $\langle(0, 1, a), (a, 0, 1)\rangle$ and $|Gy_7| = 3$ if we choose $a^2 - a + 1 \neq 0$.

The point $y_8 = (a^2 - a + 1, a - a^2, a)$ is incident with the lines $\langle(1, 0, a), (0, 1, a)\rangle$ and $\langle(a, 0, 1), (1, a, 0)\rangle$ and $|Gy_8| = 6$ if we choose $2a^2 - 2a + 1 \neq 0$ and $a^2 - a + 1 \neq 0$. This is non-trivial and involves some checking. Under G the orbit of $(1, b, c)$ is of size 6 unless $(b, c) = (0, -1)$ or $(-1, 0)$, $b = 1$ or $c = 1$, $b = c$ or $b = c^2$ where $b^3 = 1$. One has to check that in this case the only conditions we need to avoid are the aforementioned.

The point $y_9 = (a, a^2 - a + 1, a - 1)$ is incident with the lines $\langle(1, 0, a), (1, a, 0)\rangle$ and $\langle(0, a, 1), (a, 1, 0)\rangle$ and $|Gy_9| = 6$ if we choose $a^2 - 2a + 2 \neq 0$ and $a^2 - a + 1 \neq 0$.

Let a be such that $a^4 \neq 1$, $a \neq 2$, $a^2 - a + 1 \neq 0$, $2a \neq 1$, $2a^2 - 2a + 1 \neq 0$ and $a^2 - 2a + 2 \neq 0$. The set $\{(1-a)/a, (a^2+1)/a, a - a^2, (a-1)/a^2, a - 1\}$ contains five distinct elements if in addition we choose $a^3 \neq -1$.

Then the set of 36 points incident with exactly 2 bisecants of S is $C = \bigcup_{i=1}^9 Gy_i$.

We have now to choose some lines to cover the points in C and to cover twice the points in D .

The 3 external lines in the G -orbit of the line $[1, -1, 0]$ are incident with all the points of $\bigcup_{i=2}^7 Gy_i$.

If we can find an a such that $a^3 - 3a^2 + 2a - 1 = 0$ then the points $y_8, (-a^2, 0, 1)$ and $(0, 1, -1)$ are all incident with the external line $[a^{-2}, 1, 1]$ and so the three lines in the G -orbit of this line cover the points in $D \cup Gy_1 \cup Gy_8$. The points $(a, a^2 - a + 1, a - 1)$ and $(a^2 - a + 1, a, a - 1)$ are incident with the line $[1, 1, -(a^2 + 1)/(a - 1)]$ and hence the points in Gy_9 and D are covered by the three lines in the G -orbit of $[1, 1, -(a^2 + 1)/(a - 1)]$. Thus we have a set $L(S)$ with the required property consisting of 9 lines.

If we can find an a such that $a^3 - a^2 + 2a - 1 = 0$ then the points $y_9, (1, 0, -a^2)$ and $(1, -1, 0)$ are all incident with the external line $[1, 1, a^{-2}]$ and so the three lines in the G -orbit of this line cover the points in $D \cup Gy_1 \cup Gy_9$. The points $(a^2 - a + 1, a - a^2, a)$ and $(a - a^2, a^2 - a + 1, a)$ are incident with the line $[1, 1, -a^{-1}]$ and hence the points in Gy_8 and D are covered by the three lines in the G -orbit of $[1, 1, -a^{-1}]$. Thus we have a set $L(S)$ with the required property consisting of 9 lines.

If the field \mathbb{F}_q contains no such element a then we can always take $L(S)$ to be the union of all 12 lines, that is the union the orbits of the lines $[1, -1, 0]$, $[1, 1, a^{-2}]$, $[1, 1, -a^{-1}]$ and $[1, 1, -(a^2 + 1)/(a - 1)]$. This will give a 5-fold blocking set of size $6q + 3$.

To give a rough idea of when \mathbb{F}_q contains an element such that $a^3 - 3a^2 + 2a - 1 = 0$ or $a^3 - a^2 + 2a - 1 = 0$, the prime fields of order 11, 17, 19, 23, 37, 43, 53, 59, 61, 67, 79, 83, 89, 97, 101, 103, 107, 113 all contain such an element. Note that $a^3 - 3a^2 + 2a - 1 = 0$ implies all the other restrictions on a are satisfied with the exception when $\text{char} = 5$ and $a = 2$ and that $a^3 - a^2 + 2a - 1 = 0$ implies all the other restrictions on a are satisfied with the exceptions $\text{char} = 5$ and $a = 4$ and $\text{char} = 7$ and $a = 2$. So the lower bound (3.1) $|L(S)| \geq \binom{t-1}{2} - (t-2, q) = 9$ is attained in many more cases than just $q = 1 \pmod{4}$ implied by the previous example.

The upper bound (1.3) implies $|L(S)| \leq 13$ is satisfied for all q and so there is always a code meeting the Griesmer bound for $r = q - 4$.

5.5. $t = 7$. A 6-fold blocking set in $PG(2, q)$ of size $7q + 7$, where $q = 1 \pmod 7$.

Let e be primitive 7-th root of unity. Let G be the group generated by $\sigma : (x, y, z) \mapsto (x, ey, e^2z)$, $G \cong C_t$. Let S be the G -orbit of the point $u = (1, 1, 1)$, i.e.

$$S = \{(1, e^i, e^{2i}), i = 0, \dots, t - 1\}.$$

Note that S is a subset of the conic defined by $X_0X_2 = X_1^2$.

Let $p_{\{i,j\}\{k,l\}}$ be the point where $\langle (1, e^i, e^{2i}), (1, e^j, e^{2j}) \rangle$ meets $\langle (1, e^k, e^{2k}), (1, e^l, e^{2l}) \rangle$. By calculation $p_{\{i,j\}\{k,l\}} = (e^k + e^l - e^i - e^j, e^{k+l} - e^{i+j}, e^{k+l}(e^i + e^j) - e^{i+j}(e^k + e^l))$. If $k+l = i+j \pmod 7$, then $p_{\{i,j\}\{k,l\}} = (1, 0, -e^{i+j})$ and this point is incident with 3 bisecants of S , since $i + j = m \pmod 7$, $i < j$ has 3 solutions. Let

$$C = \{p_{\{i,j\}\{k,l\}} \mid i + j \neq k + l\}.$$

Note that there may be points incident with three bisecants of S in C . However we shall construct a set of lines $L(S)$ that covers every point of C twice.

Now consider the line $[1, \theta, 1]$. The line is incident with $p_{\{i,j\}\{k,l\}}$ if and only if

$$(e^{k+l} - e^{i+j})\theta = -e^k - e^l + e^i + e^j - e^{k+l+i} - e^{k+l+j} + e^{i+j+k} + e^{i+j+l}.$$

Dividing by e^{i+k} we get

$$(e^{j-k} - e^{l-i})\theta = -e^{-k} - e^j + e^{-i} + e^l - e^{-i-k+j} - e^{l-k+j} + e^{-i+l-k} + e^{-i+l+j}.$$

Hence the line contains also the point $p_{\{-i,l\}\{-k,j\}}$. Similarly the line also contains the points $p_{\{i,-k\}\{l,-j\}}, p_{\{-i,-j\}\{-k,-l\}}, p_{\{i,-l\}\{-j,k\}}$ and $p_{\{-i,k\}\{-l,j\}}$.

Thus when $|\{\pm i, \pm j, \pm k, \pm l\}| = 7$ or 8, the line $[1, \theta, 1]$ is a 6-secant to C . All numbers are taken modulo 7.

Let $L(S)$ be the union of the G -orbits of all the lines $[1, \theta, 1]$ where θ is a solution of

$$(e^{k+l} - e^j)\theta = -e^k - e^l + 1 + e^j - e^{k+l} - e^{k+l+j} + e^{j+k} + e^{j+l}.$$

for some j, k and l where $j \neq k + l \pmod t$ and $|\{0, \pm j, \pm k, \pm l\}| = 7$.

We claim that there are two lines in $L(S)$ incident with the point $p_{\{a,b\}\{c,d\}}$, where $a + b \neq c + d$. The G -orbit of this point is

$$\{p_{\{a+n,b+n\}\{c+n,d+n\}} \mid n = 0, \dots, 6\}.$$

So we have to show that two of the sets $\{\pm 0, \pm(b-a), \pm(c-a), \pm(d-a)\}$, $\{\pm(a-b), 0, \pm(c-b), \pm(d-b)\}$, $\{\pm(a-c), \pm(b-c), 0, \pm(d-c)\}$ or $\{\pm(a-d), \pm(b-d), \pm(c-d), 0\}$ have size 7.

Assume that this is not the case and, without loss of generality, that the first three sets do not have size 7. Since the first set has size less than 7 and a, b, c and d are all distinct we can assume that $b - a = -(c - a)$. So the sets $\{\pm(c - a), \pm 2(c - a), \pm(d - 2a + c)\}$ and $\{\pm(a - c), \pm 2(a - c), \pm(d - c)\}$ have size less than 6. If $d - c = -(a - c)$ then the first set is $\{\pm(c - a), \pm 2(c - a), \pm 3(c - a)\}$ and has size 6. If $d - c = 2(a - c)$ then $b = d$. If $d - c = -2(a - c)$ then the first set is $\{\pm(c - a), \pm 2(c - a), \pm 4(c - a)\}$ and has size 6. Hence the second set has size 6 and we have a contradiction.

To calculate the size of the set $L(S)$ we count the number of $(0, j), (k, l)$, with $j \neq k + l$, j, k, l all different and such that $|\{0, \pm j, \pm k, \pm l\}| = 7$. There are 6 choices for j and then we have to distinguish the cases $k = 2j$ and $k = j/2$, because in both cases two of the three conditions $l \neq -j$, $l \neq j - k$ and $l \neq k$, coincide. Hence there is 1 way to choose $k \neq \{\pm j, 2j, j/2\}$ and then 2 choices for l . And if $k = 2j$ or $k = j/2$ there are 2 choices for l . Since there are 6 points on each line of $L(S)$ and we have counted (k, l) unordered there are $42(4 + 2)/12 = 21$ lines in $L(S)$.

Every point in C is incident with at least two lines of $L(S)$ and the points

$$\{(1, 0, e^m) \mid m = 0, \dots, t - 1\}$$

are incident with $|L(S)|/7 = 3$ lines. Thus $L(S)$ has the required property from section 3. The bound (3.1) in this case is $|L(S)| \geq 15 - (5, q)$, so there is room for improvement. We just fail to get a code meeting the Griesmer bound since the bound (1.3) is $|L(S)| \leq 19$. However we have covered all the points in C one more time than is necessary unless a point occurs in C with multiplicity. So it is likely that the 6-fold blocking set is not minimal and some of the lines in $|L(S)|$ are not required.

REFERENCES

- [1] S. Ball, On nuclei and blocking sets in Desarguesian spaces, *J. Combin. Theory Ser. A*, **85** (1999) 232–236.
- [2] S. Ball, On intersection sets in Desarguesian affine spaces, *European J. Combin.*, **21** (2000) 441–446.
- [3] S. Ball and J. W. P. Hirschfeld, Bounds on (n, r) -arcs and their application to linear codes, *Finite Fields Appl.*, to appear.
- [4] A. Blokhuis, On multiple nuclei and a conjecture of Lunelli and Sce, *Bull. Belg. Math. Soc.*, **3** (1994) 349–353.
- [5] M. Braun, A. Kohnert and A. Wassermann, Optimal Linear Codes From Matrix Groups, preprint.
- [6] M. Braun, A. Kohnert and A. Wassermann, Construction of (n, r) -arcs in $PG(2, q)$, *Innovations in Incidence Geometry*, **1** (2005) 133–141.
- [7] A. A. Bruen, Polynomial multiplicities over finite fields and intersection sets, *J. Combin. Theory Ser. A*, **60** (1992) 19–33.
- [8] J. D. Dixon and B. Mortimer, *Permutation Groups*, Springer-Verlag New York, 1996.
- [9] R. Hill, Some problems concerning (k, n) arcs in finite projective planes, *Rend Sem. Mat. Brescia*, **7** (1984) 367–383.
- [10] R. Hill and J.R.M. Mason, On (k, n) -arcs and the falsity of the Lunelli–Sce conjecture, *Finite Geometries and Designs*, London Math. Soc. Lecture Note Series **49**, Cambridge University Press, Cambridge, 1981, 153–168.
- [11] J.W.P. Hirschfeld, *Projective Geometries over Finite Fields*, Second edition, Oxford University Press, Oxford, 1998.
- [12] F.J. MacWilliams and N.J.A. Sloane, *The Theory of Error-Correcting Codes*, North-Holland, 1977.
- [13] J.R.M. Mason, A class of $((p^n - p^m)(p^n - 1), p^n - p^m)$ -arcs in $PG(2, p^n)$, *Geom. Dedicata*, **15** (1984) 355–361.
- [14] J.H. van Lint, *An Introduction to Coding Theory*, Third edition, Springer-Verlag, 1998.

S. Ball

Departament de Matemàtica Aplicada IV

Universitat Politècnica de Catalunya

Jordi Girona 1-3

Mòdul C3, Campus Nord

08034 Barcelona

Spain

simeon@mat.upc.es

<http://www-ma4.upc.es/~simeon/>

E. Montanucci

Dipartimento di Matematica

Università degli Studi di Perugia

Via Vanvitelli 1

06123 Perugia

Italy