ON LINEAR CODES WHOSE WEIGHTS AND LENGTH HAVE A COMMON DIVISOR

SIMEON BALL, AART BLOKHUIS, ANDRÁS GÁCS, PETER SZIKLAI, AND ZSUZSA WEINER

1. Introduction

Let $GF(q)$ denote the unique finite field with q elements. An $[n,k,d]$-*linear code over* $GF(q)$ is a k-dimensional subspace C of the n-dimensional vector space over $GF(q)$, in which all non-zero vectors have weight at least d. The *weight* of a vector is the number of non-zero coordinates it has with respect to the canonical basis. The $(k-1)$-dimensional projective space $PG(k-1,q)$ is the incidence system (geometry) whose points, lines, planes, ..., hyperplanes are the 1-dimensional, 2-dimensional, 3-dimensional,...,$(k-1)$-dimensional subspaces of the k-dimensional vector space over $GF(q)$. The k-dimensional affine space $AG(k,q)$ is the incidence system (geometry) whose points, lines, planes, ..., hyperplanes are the cosets of the 0-dimensional, 1-dimensional, 2-dimensional,...,$(k-1)$-dimensional subspaces of the k-dimensional vector space over $GF(q)$.

Let C be a $[n,k,d]$-linear code over $GF(q)$ and suppose there is an r such that r divides n and the weights of the codewords. Our aim in this note is to prove, when the dual minimum distance is at least three, the lower bound

$$n \geq (r-1)q + (p-1)r.$$

Note that if we allow the dual minimum distance to be 2 then we could take the repetition code of length r. In contrast to the Griesmer bound and the Singleton bound (see [8], [10]), this bound does not directly involve the minimum distance. If $k=3$ it is possible to prove the bound $n \geq (r-1)q + r$ rather trivially, as we shall see. The fact that this trivial bound was not attainable for $p > 2$ was already known [2], however this only leads to the bound $n \geq (r-1)q + 2r$. It was also known that this bound is attainable for $p = 2$ and we shall show that it is also attainable when $q = p^2$ for some prime p, see section 4.

A *generator matrix* of a linear code is a matrix whose rows form a basis for the code. The columns of the generator matrix of C are vectors of the k-dimensional vector space over $GF(q)$. Let x be the j-th column of C. For each $a \in GF(q)^k$ there is a codeword w in C whose j-th coordinate is

$$\sum_{i=1}^{k} a_i x_i.$$

Date: 10 November 2005.

This work was carried out in part under the "Hungarian-Spanish Intergovernmental S and T cooperation programme". The first author also acknowledges the support of the Ministerio de Ciencia y Tecnologia, España. The second author was supported by the "Finite Structures" project carried out by the Alfréd Rényi Institute of Mathematics - Hungarian Academy of Sciences, in the framework of the European Community's "Structuring the European Research Area" programme. The last three authors were partially supported by OTKA F-043772, T-043758, T-049662 and Magyary grants.

The weight $wt(w)$ of the codeword w is the number of columns in C for which this value is non-zero and so the number of columns x for which

$$\sum_{i=1}^{k} a_i x_i = 0$$

is $n - wt(w)$. Thus the columns of the generator matrix form a set S of distinct points in $PG(k-1,q)$ with the property that every hyperplane is incident with a multiple of r points of S.

Note that if we can find a $(k-2)$-dimensional subspace U containing a single point of S (which we obviously can if $k = 3$), then we can count points of S on hyperplanes containing U and deduce the lower bound $n \geq (r-1)(q+1)+1 = (r-1)q + r$. This is the trivial bound referred to previously.

One of the motivations for this work comes from the "strong cylinder conjecture" which states that a set of p^2 points in $AG(3,p)$ which intersects every plane in 0 mod p points is the union of p parallel lines, i.e. a cylinder, see [5] and [3]. By embedding the space in $AG(4,p)$, and using the set of p^2 points as a base of a cylinder of size p^3 points, we can construct a set of p^3 points S in the plane $AG(2,p^2)$ with the property that every line is incident with 0 mod p points of S. For more details on how this is done see [9, Section 2]. This led to the question whether a set with such a property could have size less than p^3. As we shall see, example 4.4, the answer is affirmative, there are examples of size $p^3 - p$ and, moreover, Theorem 2.1 implies this is best possible.

2. A lower bound for three dimensional codes

We first consider the three dimensional case and then the more general k-dimensional case. The proofs in both cases are similar and are streamlined and then generalised versions of the proof in [1].

If we view $GF(q^2)$ as the two dimensional vector space over $GF(q)$ then the points of $AG(2,q)$ can be viewed as $(1,y)$ where $y \in GF(q^2)$. In the quotient space of y the points $(0, y-b)$ and $(0, y-c)$ are the same point in $PG(1,q)$ if and only if there is a non-zero $\gamma \in GF(q)$ such that $y - b = \gamma(y-c)$ which is if and only if $(y-b)^{q-1} = (y-c)^{q-1}$. Hence $(1,y)$, $(1,b)$ and $(1,c)$ are collinear in $AG(2,q)$ if and only if $(y-b)^{q-1} = (y-c)^{q-1}$. Normally we just say that a subset of the points of $AG(2,q)$ can be viewed as a subset of $GF(q^2)$.

Theorem 2.1. *A set of points S in $PG(2,q)$ which is incident with 0 mod r points of every line has at least $(r-1)q + (p-1)r$ points, where $1 < r < q = p^h$.*

Proof. Let us first see that r divides q. By counting the points of S on lines through a point not in S we have that $|S| = 0 \bmod r$. By counting points of S on lines through a point in S we have $|S| = 1 + (-1)(q+1) \bmod r$ and combining these two equalities we see that $q = 0 \bmod r$.

Assuming $|S| < r(q+1)$ (for if not the theorem is proved) there is an external line to S, so we can view S as a subset of $GF(q^2) \simeq AG(2,q)$ and consider the polynomial

$$R(X,Y) = \prod_{b \in S}(X + (Y-b)^{q-1}) = \sum_{j=0}^{|S|} \sigma_j(Y) X^{|S|-j}.$$

For all y, b and $c \in GF(q^2)$ the corresponding points of $AG(2,q)$ are collinear if and only if $(y-b)^{q-1} = (y-c)^{q-1}$ and each factor $X + (y-b)^{q-1}$ of $R(X,y)$ divides $X^{q+1}-1$ whenever $y \neq b$.

For $y \in S$ we have

$$R(X,y) = X(X^{q+1}-1)^{r-1} g_1(X)^r,$$

and for $y \notin S$

$$R(X,y) = g_2(X)^r.$$

In both cases $\sigma_j(y) = 0$ for $0 < j < q$ and r does not divide j. The degree of σ_j is at most $j(q-1)$ and there are q^2 elements in $GF(q^2)$, hence $\sigma_j \equiv 0$ when $0 < j < q$ and r does not divide j. So

$$R(X,Y) = X^{|S|} + \sigma_r X^{|S|-r} + \sigma_{2r} X^{|S|-2r} + ... + \sigma_q X^{|S|-q} + \sigma_{q+1} X^{|S|-q-1} + ... + \sigma_{|S|}.$$

For all $y \in GF(q^2)$ we have

$$\frac{\partial R}{\partial Y}(X,y) = \left(\sum_{b \in S} \frac{-(y-b)^{q-2}}{X + (y-b)^{q-1}} \right) R(X,y).$$

In all terms the denominator is a divisor of $X^{q+1}-1$ so multiplying this equality by $X^{q+1}-1$ we get an equality of polynomials and we see that

$$R(X,y) \mid (X^{q+1}-1)\frac{\partial R}{\partial Y}(X,y),$$

or even better

$$R(X,y)G_y(X) = (X^{q+1}-1)\frac{\partial R}{\partial Y}(X,y) =$$

$$(X^{q+1}-1)(\sigma'_r X^{|S|-r} + \sigma'_{2r} X^{|S|-2r} + ... + \sigma'_q X^{|S|-q} + \sigma'_{q+1} X^{|S|-q-1} + ...). \qquad (*)$$

Here $G = G_y$ is a polynomial in X of degree at most $q+1-r$. The term of highest degree on the right-hand side of $(*)$ that has degree not 1 mod r is of degree $|S|$ and has coefficient σ'_{q+1}, where $'$ is differentiation with respect to Y.

Consider first the case $y \notin S$. As $R(X,y)$ is an r-th power, any non-constant term in G, with degree not 1 mod r would give a term on the right-hand side of degree $> |S|$ and not 1 mod r, but such a term does not exist. Hence every term in G has degree 1 mod r except for the constant term which has coefficient σ'_{q+1}.

For any natural number κ and $i = 1, \ldots, r-2$ the coefficient of the term of degree $|S| - i(q+1) - \kappa r$ (which is not 0 or 1 mod r) on the right-hand side of $(*)$ is

$$-\sigma'_{i(q+1)+\kappa r} + \sigma'_{(i+1)(q+1)+\kappa r}$$

and must be zero. However if $(r-1)(q+1)+\kappa r > |S|$ then $\sigma_{(r-1)(q+1)+\kappa r} \equiv 0$ and we have $\sigma'_{i(q+1)+\kappa r} = 0$ for all $i = 1, \ldots, r-2$. Now consider the coefficient of the term of degree $|S| - \kappa r$. On the right hand side of $(*)$ this has coefficient $-\sigma'_{\kappa r}$ (since $\sigma'_{q+1+\kappa r} = 0$). The

only term of degree zero mod r in G is the constant term which is σ'_{q+1}. The coefficient of the term of degree $|S| - \kappa r$ in $R(X, y)$ is $\sigma_{\kappa r}$. Hence

$$\sigma_{\kappa r}\sigma'_{q+1} = -\sigma'_{\kappa r} \quad \text{for all } y \notin S. \tag{$**$}$$

If $y \in S$ then $\sigma_{q+1}(y) = 1$ and if $y \notin S$ then $\sigma_{q+1}(y) = 0$. Let

$$f(Y) = \prod_{y \in S}(Y - y).$$

Then $f\sigma_{q+1} = (Y^{q^2} - Y)g(Y)$ for some $g \in GF(q^2)[Y]$ of degree at most $|S| - 1$ (the degree of σ_{q+1} is at most $q^2 - 1$). Differentiate and substitute for a $y \in S$ and we have $f'(y) = -g(y)$. Since the degree of f' and g are less than $|S|$ we have $g \equiv -f'$. Now differentiate and substitute for a $y \notin S$ and we get $\sigma'_{q+1}f = f'$.

Thus for $y \notin S$ we have $\sigma_{\kappa r}f'/f = -\sigma'_{\kappa r}$ and so $(f\sigma_{\kappa r})'(y) = 0$. The polynomial $(f\sigma_{\kappa r})'$ has degree at most $\kappa r(q-1) + |S| - 2$, which is less than $q^2 - |S|$ if $\kappa r \leq q - 2r$.

So from now on let $|S| = (r-1)q + \kappa r$. The polynomial $(f\sigma_{\kappa r})' \equiv 0$ and so $f\sigma_{\kappa r}$ is a p-th power. Hence f^{p-1} divides $\sigma_{\kappa r}$.

If $\kappa \leq p - 2$ then $(p-1)(r-1)q + \kappa r(p-1) > \kappa r(q-1)$ and so $\sigma_{\kappa r} \equiv 0$. However the polynomial whose terms are the terms of highest degree in $R(X, Y)$ is $(X + Y^{q-1})^{|S|}$ which has a term $X^{(r-1)q}Y^{\kappa r(q-1)}$ since $\binom{|S|}{\kappa r} = 1$.

Thus $\sigma_{\kappa r}$ has a term $Y^{\kappa r(q-1)}$ which is a contradiction. Therefore $\kappa \geq p - 1$. □

Corollary 2.2. *A code of dimension* 3 *whose weights and length have a common divisor* $r < q$ *and whose dual minimum distance is at least* 3 *has length at least* $(r-1)q + (p-1)r$.

A *maximal arc* in a projective plane is a set of points S with the property that every line is incident with 0 or r points of S. Apart from the trivial examples of a point, an affine plane and the whole plane, that is where $r = 1$, q or $q+1$ respectively, there are examples known for every r dividing q for q even, see [6].

Corollary 2.3. *There are no non-trivial maximal arcs in* $PG(2, q)$ *when* q *is odd.*

Proof. A maximal arc has $(r-1)q + r$ points. □

This was first proven in [2].

3. A lower bound for higher dimensional codes

In this section we prove the same upper bound for 0 modulo r sets (with respect to hyperplanes) in higher dimensions. The main difference is that now it is more difficult to prove that we are allowed to do everything in the affine space (that is we have a hyperplane disjoint from the set) and that $r|q$. In fact we will only be able to prove this for a possible counter-example (that is, for a set of size less than $(r-1)q + (p-1)r$.) We will do this in a separate lemma. After this lemma we give a representation of $AG(k-1, q)$ that generalizes the one used in the previous section for the affine plane. Finally, before stating and proving the result we will also need a statement which allows us to repeat the step of replacing σ_{q+1} with f in the proof of Theorem 2.1. Let $k \geq 4$.

LEMMA 3.1. *Let S be a set of points of $PG(k-1,q)$ with the property that every hyperplane is incident with $0 \bmod r$ points of S. If $r < q$ and $|S| < (r-1)q + (p-1)r$ then r divides q and there is a hyperplane incident with 0 points of S.*

Proof. Throughout the proof, by dimension we mean projective dimension. From the conditions it is easy to deduce that $|S| < 2q^2 - 2q$, we will use this fact several times. Let T be a subspace of maximal dimension t with the property $|T \cap S| = 1$. Counting points of S on $(t+1)$-dimensional subspaces through T we see at least $1 + \frac{q^{k-1-t}-1}{q-1}$ points. Since this has to be less than $2q^2 - 2q$, we have $t \geq k-4$. Let T_1 be a $(k-4)$-dimensional subspace in T with $|T_1 \cap S| = 1$. One of the q^2+q+1 $(k-3)$-dimensional subspaces containing T_1 contains at most 2 points of S (otherwise $|S| > 1 + 2(q^2+q+1)$). Hence we have a $(k-3)$-dimensional subspace meeting S in 1 or 2 points. From now on we distinguish two cases according as S blocks every $(k-3)$-dimensional (that is, co-dimension 2) subspace or not.

Case 1. There exists a co-dimension 2-space N skew to S.

Counting the points of S on the hyperplanes through N, we have that $|S| \equiv 0 \mod r$. If there is a co-dimension 2-space M, such that $|M \cap S| = 1$, then again counting the points of S on the hyperplanes through M, we get that $-1(q+1) + 1 \equiv |S| \mod r$ and hence r divides q. If not, there is a co-dimension 2-space intersecting S in exactly 2 points (by the first paragraph of the proof). Counting as before we have that $-2(q+1) + 2 \equiv |S| \mod r$ and hence r divides $2q$. If all the co-dimension 2-spaces intersect S in even number of points, then by induction on the dimension k we have that q is even and so r divides q. If there is a co-dimension 2-space M^*, such that $|M^* \cap S| = 2n+1$, then as before we get that $-(2n+1)(q+1) + (2n+1) \equiv |S| \mod r$, hence r divides $(2n+1)q$. Combining this divisibility with the divisibility r divides $2q$ yields r divides q. Now we have that r divides q and $r < q$, hence we know that $r \leq q/p$ and so $|S| < rq$. Counting the points of S on the hyperplanes containing N we see that there is a hyperplane containing no points of S.

Case 2. S blocks every co-dimension 2 subspace.

By [7], S contains a plane π. Let W be a subspace of maximal dimension w with the property $W \cap S = \pi$. Counting points on $(w+1)$-dimensional subspaces through W, we see at least $q^2+q+1+\frac{q^{k-1-w}-1}{q-1}$ points of S. Since this has to be less than $2q^2$, we have $w \geq k-3$. Let W_1 be a $(k-3)$-dimensional subspace of W containing π. Counting the number of points through W_1 we have $|S| \equiv q^2+q+1+(q+1)(-q^2-q-1) = -q(q^2+q+1) \mod r$.

Next take a line l in π and a subspace U of maximal dimension u such that $U \cap S = l$. Counting points on $(u+1)$-dimensional subspaces through U, we see at least $q^2+q+1+\frac{q^{k-1-u}-1}{q-1} - 1$ points of S (note that $\pi \setminus l$ is contained in exactly one such subspace). Since this has to be less than $2q^2$, we have $u \geq k-3$. Let U_1 be a $(k-3)$-dimensional subspace of U containing l. Counting the number of points through U_1 we have $|S| \equiv q+1+(q+1)(-q-1) = -q(q+1) \mod r$. Combining this with $|S| \equiv -q(q^2+q+1) \mod r$ (and using $r < q$), we have $r|q$.

Now we have that r divides q and $r < q$, hence $r \leq q/p$ and so $|S| < rq$. But then S cannot contain a plane and we have a contradiction. □

If we view $GF(q)^{k-3} \times GF(q^2)$ as the $(k-1)$-dimensional vector space over $GF(q)$ then the points of $AG(k-1,q)$ can be viewed as $a = (1, a_1, a_2, \ldots, a_{k-2})$ where $a_{k-2} \in GF(q^2)$ and the other a_i are elements of $GF(q)$. In the quotient space of the span of

$$w_0 = (1, 0, \ldots, 0, y_0),\ w_1 = (0, 1, 0, \ldots, 0, y_1), \ldots, w_{k-3} = (0, \ldots, 0, 1, y_{k-3})$$

the point a is given by $(0, \ldots, 0, y_0 - a_{k-2} + \sum_{i=1}^{k-3} a_i y_i)$. As in the previous section the points a and b are quotient to the the same point in $PG(1,q)$ if and only if $(y_0 - a_{k-2} + \sum_{i=1}^{k-3} a_i y_i)^{q-1} = (y_0 - b_{k-2} + \sum_{i=1}^{k-3} b_i y_i)^{q-1}$ if and only if $\langle w_0, w_1, \ldots, w_{k-3}, a\rangle = \langle w_0, w_1, \ldots, w_{k-3}, b\rangle$. Note that $y_0 - a_{k-2} + \sum_{i=1}^{k-3} a_i y_i = 0$ if and only if $a \in \langle w_0, w_1, \ldots, w_{k-3}\rangle$.

LEMMA 3.2. *Let q be an arbitrary prime power, $S \subseteq GF(q)^n$ and define the following two polynomials in n variables:*

$$f(X_0, \ldots, X_{n-1}) = \prod_{a \in S} (a_0 X_0 + \cdots + a_{n-1} X_{n-1}),$$
$$g(X_0, \ldots, X_{n-1}) = \sum_{a \in S} (a_0 X_0 + \cdots + a_{n-1} X_{n-1})^{q-1}.$$

Then we have the following identity between polynomials:

$$f(X)(g(X) - |S|) = \sum_{i=0}^{n-1} (X_i^q - X_i) \frac{\partial f}{\partial X_i}.$$

Proof. We use induction on $|S|$. For $|S| = 1$, we have

$$(a_0 X_0 + \cdots + a_{n-1} X_{n-1})((a_0 X_0 + \cdots + a_{n-1} X_{n-1})^{q-1} - 1)) = \sum_i a_i (X_i^q - X_i),$$

and the partial derivative of $a_0 X_0 + \cdots + a_{n-1} X_{n-1}$ with respect to X_i is a_i.

For the general step let $S_1 = S \cup \{(b_0, ..., b_{n-1})\}$ and denote by f_1 and g_1 the corresponding functions for S_1, that is

$$f_1 = (b_0 X_0 + \cdots + b_{n-1} X_{n-1}) f,$$
$$g_1 = (b_0 X_0 + \cdots + b_{n-1} X_{n-1})^{q-1} + g.$$

We have

$$f_1(g_1 - |S| - 1) = (b_0 X_0 + \cdots + b_{n-1} X_{n-1}) f (g - |S| + (b_0 X_0 + \cdots + b_{n-1} X_{n-1})^{q-1} - 1) =$$

$$((b_0 X_0 + \cdots + b_{n-1} X_{n-1})^q - (b_0 X_0 + \cdots + b_{n-1} X_{n-1})) f + (b_0 X_0 + \cdots + b_{n-1} X_{n-1})(\sum_{i=0}^{n-1} (X_i^q - X_i) \frac{\partial f}{\partial X_i}) =$$

$$= \sum_{i=0}^{n-1} (X_i^q - X_i)(b_i f + (b_0 X_0 + \cdots + b_{n-1} X_{n-1}) \frac{\partial f}{\partial X_i}) =$$

$$= \sum_{i=0}^{n-1} (X_i^q - X_i) \frac{\partial f_1}{\partial X_i}.$$

□

THEOREM 3.3. *A set of points S in $PG(k-1,q)$ which is incident with $0 \bmod r$ points of every hyperplane has at least $(r-1)q+(p-1)r$ points, where $1<r<q=p^h$ and $k \geq 4$.*

Proof. Assume that $|S| < (r-1)q+(p-1)r$. By Lemma 3.1, we have that r divides q and that we can view S as a subset of $GF(q)^{k-3} \times GF(q^2) \simeq AG(k-1,q)$. Consider the polynomial in $k-1$ variables

$$R(X,Y) = \prod_{a \in S}(X + (Y_0 - a_{k-2} + \sum_{i=1}^{k-3} a_i Y_i)^{q-1}) = \sum_{j=0}^{|S|} \sigma_j(Y) X^{|S|-j}.$$

For all $y = (y_0, y_1, \ldots, y_{k-3}) \in GF(q^2)^{k-2}$ the points a, b and

$$w_0 = (1,0,\ldots,0,y_0), w_1 = (0,1,0,\ldots,0,y_1), \ldots, w_{k-3} = (0,\ldots,0,1,y_{k-3}),$$

span the same hyperplane if and only if

$$(y_0 - a_{k-2} + \sum_{i=1}^{k-3} a_i y_i)^{q-1} = (y_0 - b_{k-2} + \sum_{i=1}^{k-3} b_i y_i)^{q-1} \neq 0.$$

Suppose that $W = \langle w_0, w_1, \ldots, w_{k-3} \rangle$ is a $(k-3)$-dimensional subspace incident with t points of S. By hypothesis every $(k-2)$-dimensional subspace contains a multiple of r points of S and so

$$R(X,y) = X^t (X^{q+1}-1)^{r-t_0} g(X)^r,$$

where $t_0 = t \bmod r$.

For all $y \in GF(q^2)^{k-2}$ the polynomial $\sigma_j(y) = 0$ whenever $0 < j < q$ and r does not divide j. However σ_j has degree at most $j(q-1)$ and so, for $0 < j < q$ and r does not divide j, the polynomial $\sigma_j \equiv 0$.

For future reference note that $\sigma_{q+1}(y) = -(r-t_0) = t \bmod p$, hence

$$\sigma_{q+1}(Y) = -\sum_{a \in S}(Y_0 - a_{k-2} + \sum_{i=1}^{k-3} a_i Y_i)^{q^2-1}.$$

(To see this identity, note that both sides are polynomials of degree at most q^2-1 and are equal as functions.)
Let $|S| = (r-1)q + \kappa r$.
If $t = 1$ then $\sigma_{\kappa r}(y) = 0$ since the degree of g in this case is $\kappa - 1$.
Fix any i and let $'$ be differentiation with respect to the variable Y_i.
As in the proof of the planar case, Theorem 2.1, we have

$$R(X,y) \mid (X^{q+1}-1)\frac{\partial R}{\partial Y_i}(X,y).$$

If $|W \cap S| = 0$ then $R(X,y)$ is an r-th power and in exactly the same way as in the proof of Theorem 2.1 we have

$$\sigma_{\kappa r}\sigma'_{q+1} = -\sigma'_{\kappa r}.$$

Let

$$f(Y) = \prod_{a \in S}(Y_0 - a_{k-2} + \sum_{i=1}^{k-3} a_i Y_i).$$

We apply Lemma 3.2 to f and σ_{q+1} (the field is $GF(q^2)$, the variables are $Y_0, \ldots, Y_{k-2}$ and we put $Y_{k-2} = -1$) to find

$$f\sigma_{q+1} = -\sum_{i=0}^{k-3}(Y_i^{q^2} - Y_i)\frac{\partial f}{\partial Y_i}.$$

Differentiating (with respect to the previously selected variable Y_i) and evaluating for any $y \in GF(q^2)^{k-2}$ we have

$$\sigma'_{q+1} f + \sigma_{q+1} f' = f'.$$

The equation $\sigma_{\kappa r}\sigma'_{q+1} = -\sigma'_{\kappa r}$ is only valid for $|W \cap S| = 0$, but if we multiply it with f (which is zero whenever $|W \cap S| > 0$), we have an equation valid for any y. Combining this with $\sigma'_{q+1} f = f' - \sigma_{q+1} f'$ we have that $(f\sigma_{\kappa r})' = f'\sigma_{q+1}\sigma_{\kappa r}$. But the right hand side is 0 for any choice of y: if $|W \cap S| = 0$ then $\sigma_{q+1} = 0$, if $|W \cap S| = 1$ then $\sigma_{\kappa r} = 0$, while for $|W \cap S| > 1$ $f' = 0$ (since in this case y is a root of multiplicity at least 2).

We deduce that the polynomial $(f\sigma_{\kappa r})'$ is zero for all $y \in GF(q^2)^{k-2}$, but it is a polynomial of degree at most $|S| + \kappa r(q-1) < q^2$. Thus $(f\sigma_{\kappa r})' \equiv 0$. This holds for which ever indeterminate Y_i we choose to differentiate with respect to and so we conclude that

$$f\sigma_{\kappa r} \in GF(q^2)[Y_0^p, \ldots, Y_{k-3}^p].$$

Hence f^{p-1} divides $\sigma_{\kappa r}$.

If $\kappa \leq p-2$ then $(p-1)(r-1)q + \kappa r(p-1) > \kappa r(q-1)$ and so $\sigma_{\kappa r} \equiv 0$. However the polynomial whose terms are the terms of highest degree in $R(X, Y_0, 0, \ldots, 0)$ is $(X + Y_0^{q-1})^{|S|}$ which has a term $X^{(r-1)q} Y_0^{\kappa r(q-1)}$ since $\binom{|S|}{\kappa r} = 1$.

Thus $\sigma_{\kappa r}$ has a term $Y^{\kappa r(q-1)}$ which is a contradiction. Therefore $\kappa \geq p-1$. □

Corollary 3.4. *A linear code whose weights and length have a common divisor $r < q$ and whose dual minimum distance is at least 3 has length at least $(r-1)q + (p-1)r$.*

4. Constructions

Firstly note that any planar examples can be embedded in higher dimensions. When q is even the maximal arcs in a plane attain the bound and they exist for all possible r, see [6]. Also note that an affine plane is always an example (in any dimension) with $r = q$ showing that the condition $r < q$ is necessary in the theorems.

Here we give an outline of a general construction of such codes which will give us examples of size less than rq in the case where $GF(r)$ is a subfield of $GF(q)$.

If $GF(r)$ is a subfield of $GF(q)$ then $q = r^t$. The points of $PG(k-1, r^t)$ are the subspaces of rank 1 of $V = V(k, r^t)$, the vector space of rank (vector space dimension) k over $GF(q)$. These subspaces form a spread of rank t subspaces when we consider V as a vector space of rank kt over $GF(r)$. Let U be a subspace of V and let $B(U)$ be the set of points of $PG(k-1, q)$ whose spread elements have a non-trivial intersection with U.

LEMMA 4.1. *Let U be a subspace of V of rank at least $t+1$. For any hyperplane H of $PG(k-1,q)$ the number $|B(H) \cap B(U)| = 1 \bmod r$.*

Proof. A hyperplane of $PG(k-1,q)$ is a subspace of rank $(k-1)t$ and so the rank d of $U \cap H$ is at least 1. The number of linearly independent vectors (mutually independent over $GF(r)$) in this intersection is $(r^d-1)/(r-1)$. Let a_j be the number of spread elements contained in H that have an intersection of rank j with U. Then

$$\sum_{j=1}^{t} a_j(r^j-1)/(r-1) = (r^d-1)/(r-1)$$

and thus $\sum_{j=1}^{t} a_j = 1 \bmod r$. □

THEOREM 4.2. *Let W be a subspace of V of rank $t+1$ and let U be a subspace of rank $t+2$ containing W. The set of points $S = B(U) \setminus B(W)$ of $PG(k-1,q)$ has the property that every hyperplane is incident with 0 modulo r points of S.*

Proof. Apply Lemma 4.1 and $1-1=0$. □

We will only investigate one example in the planar case, that is, when points and lines of $PG(2,r^t)$ are represented by some t-dimensional and $(2t)$-dimensional subspaces of $V(3t,r)$, respectively. In general it is difficult to calculate the size of an example, but for a particular case it is easy.

LEMMA 4.3. *If a subspace U of dimension k meets a line L in $k-1$ dimensions, then the number of points of $B(U)$ outside L is $\frac{q^k-q^{k-1}}{q-1}$. If $k \geq t+2$, then $B(U)$ contains the whole line.*

Proof. For the first statement what we need is that any t-space corresponding to a point out of the line meets U in at most one dimension. This has to be true, since otherwise the t-space would have a non-trivial intersection with $U \cap L$, contradicting the fact that any point is contained in a line or has a trivial intersection with the line.

For the second statement note that if the intersection has dimension at least $t+1$, then it has a non-trivial intersection with any t-dimensional subspace of L. □

EXAMPLE 4.4. *An example in $PG(2,r^t)$ of size $r^{t+1} - r^{t-1} - r^{t-2} - \cdots - r$.*

Proof. Choose a $(2t)$-dimensional subspace L corresponding to a line of $PG(2,r^t)$. Due to a result of Blokhuis and Lavrauw ([4] Lemma 4.1) we can choose a t-space $W_1 \subset L$ so that it meets every t-space corresponding to points of $PG(2,r^t)$ in at most one dimension. Let W be a $(t+1)$-dimensional subspace meeting L in W_1. By the previous lemma (and the choice of W_1), the size of $B(W)$ is $\frac{r^t-1}{r-1} + \frac{r^{t+1}-r^t}{r-1}$.

Choosing U to be a $(t+2)$-dimensional subspace containing W and meeting L in t dimensions, by the previous lemma, $|B(U)| = r^t + 1 + \frac{r^{t+2}-r^{t+1}}{r-1}$, so we have the desired size. □

The particular case $t=2$ gives a set of size $r^3 - r$ showing that the bound in Theorem 2.1 (and hence Theorem 3.3) is sharp in the case $q = p^2$.

References

[1] S. Ball and A. Blokhuis, An easier proof of the maximal arcs conjecture, *Proc. Amer. Math. Soc.*, **126** (1998) 3377–3380.
[2] S. Ball, A. Blokhuis and F. Mazzocca, Maximal arcs in Desarguesian planes of odd order do not exist, *Combinatorica*, **17** (1997) 31–41.
[3] S. Ball and M. Lavrauw, On the graph of a function in two variables over a finite field, *J. Algebraic Combin.*, to appear.
[4] A. Blokhuis, M. Lavrauw, Scattered spaces with respect to a spread in $PG(n, q)$, *Geom. Dedicata*, **81** (2000) 231–243.
[5] P. J. Cameron, Problems from the twentieth British Combinatorial Conference, preprint.
[6] R. H. F. Denniston, Some maximal arcs in finite projective planes, *J. Combin. Theory*, **6** (1969) 317–319.
[7] U. Heim, Blockierende Mengen in endlichen projektiven Räumen, *Mitt. Math. Semin. Giessen* , **226** (1996) 4–82.
[8] F.J. MacWilliams and N.J.A. Sloane, *The Theory of Error-Correcting Codes*, North-Holland, 1977.
[9] T. Szőnyi and Zs. Weiner, Small blocking sets in higher dimensions, *J. Combin. Theory Ser. A*, **95** (2001) 88–101.
[10] J.H. van Lint, *An Introduction to Coding Theory*, Third edition, Springer-Verlag, 1998.