Multiple blocking sets in finite projective spaces and improvements to the Griesmer bound for linear codes

Simeon Ball*, Szabolcs L. Fancsali†

27 February 2009

Abstract

In this article we shall prove that, for $q = p$ prime and roughly $\frac{3}{8}$-th's of the values of $d < q^{k-1}$, there is no linear code meeting the Griesmer bound. This result uses Blokhuis' theorem on the size of a t-fold blocking set in $\mathrm{PG}(2, p)$, p prime, which we generalise to higher dimensions. We also give more general lower bounds on the size of a t-fold blocking set in $PG(\delta, q)$, for arbitrary q and $\delta \geq 3$.

It is known that from a linear code of dimension k with minimum distance $d < q^{k-1}$ that meets the Griesmer bound one can construct a t-fold blocking set of $PG(k-1, q)$. Here, we calculate explicit formulas relating t and d.

Finally we show, using the generalised version of Blokhuis' theorem, that nearly all linear codes over $\mathbb{F}_p$ of dimension k with minimum distance $d < q^{k-1}$, which meet the Griesmer bound, have codewords of weight at least $d + p$ in subcodes, which contain codewords satisfying certain hypotheses on their supports.

1 Introduction

In this article, p always denotes a *prime* and q always denotes an arbitrary prime *power* (that can also be a prime). Let $\mathbb{F}_q^n$ denote the n-dimensional

*The first author acknowledges the support of the projects MTM2008-06620-C03-01 and MTM2005-08990-C02-01 of the Spanish Ministry of Science and Education and the project 2005SGR00256 of the Catalan Research Council.

†The second author acknowledges the hospitality and financial support of the *Centre de Recerca Matemàtica* of Catalonia.

vector space over the finite field with q elements $\mathbb{F}_q$. The *Hamming distance* or simply *distance* between two vectors is the number of coordinates in which they differ.

Definition 1.1 *A* q-ary linear code C *of* length n, dimension k *and* minimum distance d, *is a* k*-dimensional subspace of* $\mathbb{F}_q^n$ *in which the distance between any two distinct vectors is at least* d.

For more background on linear codes see [13] or [15].

Let G be a generator matrix for a linear code C of length n, dimension k and minimum distance d. In other words G is a $k \times n$ matrix of full rank with the property that

$$C = \left\{ xG \mid x \in \mathbb{F}_q^k \right\}.$$

Let S be the multi-set of columns of G. Since C has minimum distance d, for any non-zero vector x of $\mathbb{F}_q^k$ the inner product $\langle x|s \rangle$ is zero for at most $n-d$ elements $s \in S$. In other words if we consider S as a multi-subset of the points of $\mathrm{PG}(k-1,q)$ then every hyperplane is incident with at most $n-d$ points of S.

Definition 1.2 *If the generator matrix* G *has no two linear dependent columns (in other words if the dual minmum distance of the code* C *is at least three) then the multi-set* S *is a set. In this case the linear code* C *is called a* projective code.

Suppose that C is a projective code. The set B of points of $\mathrm{PG}(k-1,q)$ that are not points of S is a set of

$$|B| = |\mathrm{PG}(k-1,q)| - |S| = \frac{q^k-1}{q-1} - n \tag{1}$$

points with the property that every hyperplane is incident with at least

$$t = \frac{q^{k-1}-1}{q-1} - n + d = |B| - q^{k-1} + d \tag{2}$$

points of B.

Definition 1.3 *A* t-fold blocking set *with respect to the* hyperplanes *of* $\mathrm{PG}(k-1,q)$ *is a set of points* B *with the property that every hyperplane is incident with at least* t *points of* B.

Thus, a projective code of length n, dimension k and minimum distance d corresponds to a t-fold blocking set with respect to the hyperplanes of $\mathrm{PG}(k-1,q)$, where $t = \frac{q^{k-1}-1}{q-1} - n + d$.

Some authors prefer to use the word minihyper, which is defined as follows.

Definition 1.4 *An $\{f,t,k-1,q\}$-minihyper is a set M of f points of $\mathrm{PG}(k-1,q)$ with the property that every hyperplane is incident with at least t points of M.*

Thus, an $\{f,t,k-1,q\}$-minihyper is a t-fold blocking set with respect to hyperplanes of cardinality f.

2 Multiple blocking sets in two dimensions

In this section we review the known results about the minimal possible sizes of multiple blocking sets in $\mathrm{PG}(2,q)$ which we shall use subsequently.

Suppose that $1 \le t \le q$.

Proposition 2.1 *If B is a proper subset of the points of $\mathrm{PG}(2,q)$ and it is a t-fold blocking set then $|B| \ge t(q+1)$.*

Proof: Let $P \in \mathrm{PG}(2,q) \setminus B$ be a point not in the blocking set. There are $q+1$ lines through P and each lines contains at least t points of B (and these points are distinct). ■

Definition 2.2 *Let $\Delta_q(t)$ denote the maximum number such that a t-fold blocking set in $\mathrm{PG}(2,q)$ has at least $t(q+1)+\Delta_q(t)$ points.*

The following theorem comes from the results [1, Theorem 1.2, Theorem 1.3, Theorem 1.4] for $p > 3$ and is also valid for the cases $p = 2$ and $p = 3$.

Theorem 2.3 (Blokhuis) *Let B be a t-fold blocking set with respect to lines in $\mathrm{PG}(2,p)$ where p is an arbitrary prime. If $2 \le t \le p$ then*

$$|B| \ge tp + t + \min\left\{\frac{p+1}{2}, p-t\right\}.$$

In other words

$$\Delta_p(t) \ge \min\left\{\frac{p+1}{2}, p-t\right\}.$$

Furthermore, if $p = 7$ then $\Delta_7(2) \ge 5$, if $p = 11$ then $\Delta_{11}(2) \ge 7$ and $\Delta_{11}(3) \ge 7$, if $p = 13$ then $\Delta_{13}(2) \ge 8$ and $\Delta_{13}(3) \ge 8$, if $p = 17$ then $\Delta_{17}(2) \ge 10$ and $\Delta_{17}(3) \ge 10$, and if $p = 19$ then $\Delta_{19}(2) \ge 11$. ■

For results in the prime *power* case see [1], [7] and [6].

3 The Griesmer bound

The *(Hamming) weight* $w(x)$ of a vector $x \in \mathbb{F}_q^k$ is the number of non-zero coordinates of x.

Definition 3.1 *The* residual code *of C with respect to a vector x, denoted by* $\mathrm{Res}(C, x)$*, is the code of length $n - w(x)$ obtained from C by deleting all the coordinates where x is non-zero.*

The following proposition can be proved using the pigeon-hole principle, see for example [12, Lemma 5.7.3].

Proposition 3.2 *If x is a codeword of weight d then* $\mathrm{Res}(C, x)$ *is a $(k-1)$-dimensional code of length $n - d$ whose minimum distance is at least* $\left\lceil \frac{d}{q} \right\rceil$. ■

Using Proposition 3.2 one obtains the Griesmer bound

$$n \geq g(k, d) := \sum_{i=0}^{k-1} \left\lceil \frac{d}{q^i} \right\rceil, \tag{GB}$$

by considering the sequence of residual codes $C = C_0, C_1, \ldots, C_{k-1}$, where C_j is a $(k-j)$-dimensional code of length $n - \sum_{i=0}^{j-1} d^{(i)}$ with minimum distance $d^{(j)}$ which satisfies

$$d^{(j)} \geq \left\lceil \frac{d^{(j-1)}}{q} \right\rceil \geq \left\lceil \frac{d}{q^j} \right\rceil. \tag{3}$$

The bound follows by observing that the one-dimensional code C_{k-1} of length $n - \sum_{i=0}^{k-2} d^{(i)}$ has minimum distance is at least $d^{(k-1)}$. Note that if one of the residual codes C_j does not have length $g(k-j, \left\lceil \frac{d}{q^j} \right\rceil)$ then the codes C_m, with $0 \leq m \leq j$ have length at least $g(k-m, \left\lceil \frac{d}{q^m} \right\rceil) + 1$. In particular the code C has length at least $g(k, d) + 1$. ■

The following proposition is from [10].

Proposition 3.3 *If C is a k-dimensional code of length $g(k, d) + t$ and $d \leq sq^{k-1}$ then a column of a generator matrix of C is appears as a column at most $s + t$ times.*

Proof: Suppose that C has a generator matrix G with a column which appears at least $s+t+1$ times. We can assume that this column is $(1, 0, \ldots, 0)^t$ and that it appears in the first $s+t+1$ columns. The $(k-1) \times (g(k, d) - s - 1)$ matrix obtained by deleting the first row and the first $s+t+1$ columns of G

generates a $(k-1)$-dimensional code of length $g(k,d)-s-1$ and minimum distance at least d. Thus, applying the Griesmer bound and $sq^{k-1} \geq d$ we have

$$g(k,d)-s-1 \geq g(k-1,d) = g(k,d) - \left\lceil \frac{d}{q^{k-1}} \right\rceil \geq g(k,d)-s,$$

a contradiction. ■

Corollary 3.4 *If C is k-dimensional code with minimum distance $d \leq q^{k-1}$, that meets the Griesmer bound, in other words of length $g(k,d)$, then no generator matrix for C has repeated columns. In other words C is a projective code.* ■

The purpose of this article is to show that for many values of $d < q^{k-1}$ there is no code that meets the Griesmer bound. Similar results have been obtained before, for instance in [9] the following theorem is proved.

Theorem 3.5 *If, for a fixed k and d, either*

1. *k is odd and $q^{k-1} - 2q^{(k-1)/2} - q + 1 \leq d \leq q^{k-1} - 2q^{(k-1)/2}$, or*
2. *k is even and $q^{k-1} - q^{k/2} - q^{k/2-1} - q + 1 \leq d \leq q^{k-1} - q^{k/2} - q^{k/2-1}$*

then

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

Our improvements to the Griesmer bound apply in the case $q = p$ is prime. We shall see that it is possible to prove that for about $\frac{3}{8}$-th's of values of $d < p^{k-1}$ there is no k-dimensional linear code meeting the Griesmer bound, see Sections 4 and 8. Moreover, in Section 8, we show that if there is a linear code with minimum distance d which meets the Griesmer bound then certain subcodes (which contain codewords satisfying a property on their supports) contain codewords of weight at least $d+p$.

In Sections 5, 6 and 7 we shall also prove some results relating to multiple blocking sets with respect to hyperplanes in $\mathrm{PG}(k-1,q)$. Some of these will be used in Section 8.

4 Improvements to the Griesmer bound

The following result is a consequence of Theorem 2.3. Let p be a prime.

Corollary 4.1 *A set A of n points in* $\mathrm{PG}(2,p)$ *with the property that every hyperplane (line) is incident with at most $r \leq p-1$ points of A satisfies*

$$n \leq \max\left\{(r-1)p+1, (r-1)p+r-\frac{(p+1)}{2}\right\}. \qquad \blacksquare$$

Let $d = \sum_{i=0}^{k-2} d_i p^i$ be the p-ary expansion of d.

Theorem 4.2 *If, for a fixed k and d, p^{k-3} divides $d < p^{k-1} - 2p^{k-2}$ and $d_{k-3} \geq \max\{\frac{p+1}{2}, p - d_{k-2}\}$ then*

$$n \geq g(k,d) + 1 = 1 + \sum_{i=0}^{k-1} \left\lceil \frac{d}{p^i} \right\rceil.$$

Proof: Let us assume there is a code C meeting the Griesmer bound with minimum distance $d^{(0)} = d = d_{k-2}p^{k-2} + d_{k-3}p^{k-3}$. We form a sequence of residual codes with minimum distance $d^{(i)} = d^{(i-1)}/p = d/p^i$ by choosing a codeword of weight $d^{(i-1)}$ in the previous code in the sequence. The sequence of codes descends to a 3-dimensional code C' with minimum distance $d' = d_{k-2}p + d_{k-3}$. Moreover, since C meets the Griesmer bound all the residual codes also meet the Griesmer bound. In particular C' meets the Griesmer bound.

By Proposition 3.3, C' is a projective code. It has length

$$n' = d' + \left\lceil \frac{d'}{p} \right\rceil + 1, \tag{4}$$

which gives $n' = d_{k-2}(p+1) + d_{k-3} + 2$ if $d_{k-3} \neq 0$ and $n' = d_{k-2}(p+1) + 1$ if $d_{k-3} = 0$.

As discussed in the introduction, the columns of a generator matrix of a three-dimensional projective code of length n' and minimum distance d', form a set A of n' points with the property that every line is incident with at most $n' - d'$ points of A. By Corollary 4.1

$$n' \leq \max\left\{(n'-d'-1)p+1, (n'-d'-1)p+n'-d'-\frac{(p+1)}{2}\right\}. \tag{5}$$

Substituting $n' = d_{k-2}(p+1) + d_{k-3} + 2$ gives the condition that either $d_{k-2} + d_{k-3} \leq p-1$ or $d_{k-3} \leq (p-1)/2$ and substituting $n' = d_{k-2}(p+1)+1$, for the case $d_{k-3} = 0$, gives the condition $d_{k-2} = 0$.

Therefore, if $d_{k-2} + d_{k-3} \geq p$ and $d_{k-3} \geq (p+1)/2$ then we have a contradiction. $\blacksquare$

The following theorem deals with the case that p^{k-3} does not divide d. Note that we cannot prove the above by simply applying Theorem 4.3 below to the punctured code, since such a proof would not be valid for the case $k = 3$.

Theorem 4.3 *If, for a fixed k and d, p^{k-3} does not divide $d < p^{k-1} - 2p^{k-2}$ and $d_{k-3} \geq \max\left\{\frac{p-1}{2}, p-1-d_{k-2}\right\}$ then*

$$n \geq g(k,d) + 1 = 1 + \sum_{i=0}^{k-1} \left\lceil \frac{d}{p^i} \right\rceil .$$

Proof: Let us assume there is a code C meeting the Griesmer bound with minimum distance $d^{(0)} = d$. We form a sequence of residual codes with minimum distance $d^{(i)} = \left\lceil d^{(i-1)}/q \right\rceil = \lceil d/q^i \rceil$ by choosing a codeword of weight $d^{(i-1)}$ in the previous code in the sequence. The sequence of codes descends to a 3-dimensional code C' with minimum distance $d' = d_{k-2}p + d_{k-3} + 1$ meeting the Griesmer bound.

By Proposition 3.3, C' is a projective code. It has length

$$n' = d' + \left\lceil \frac{d'}{p} \right\rceil + 1 \tag{6}$$

which gives $n' = d_{k-2}(p+1) + d_{k-3} + 3$ if $d_{k-3} \neq p-1$ and $n' = (d_{k-2} + 1)(p+1) + 1$ if $d_{k-3} = p-1$.

Since C' is a projective code, we can apply Corollary 4.1 which implies

$$n' \leq \max\left\{(n'-d'-1)p+1, (n'-d'-1)p + n' - d' - \frac{(p+1)}{2}\right\}. \tag{7}$$

Substituting $n' = d_{k-2}(p+1) + d_{k-3} + 3$ gives the condition that either $d_{k-2} + d_{k-3} \leq p-2$ or $d_{k-3} \leq (p-3)/2$ and substituting $n' = d_{k-2}(p+1)+1$ gives the condition $d_{k-2} \leq -1$.

Therefore, if $d_{k-2} + d_{k-3} \geq p-1$ and $d_{k-3} \geq (p-1)/2$ then we have a contradiction. ■

We shall consider further improvements to the Griesmer bound in Section 8, which will include the case $d_{k-2} = p-2$.

5 Multiple blocking sets in three dimensions

In this section, suppose that $1 \leq t \leq q^2 + q$ and define t_0 and t_1 by $t = t_1(q+1) + t_0$, where $0 \leq t_i \leq q$. If $t_1 = q$ then $t_0 = 0$ since $t \leq q^2 + q$.

Lemma 5.1 *Suppose that $B \subseteq \mathrm{PG}(3,q)$ is a t-fold blocking set with respect to planes and suppose that there exists a line ℓ such that $0 \leq |B \cap \ell\,| = r \leq q$. Then $|B| \geq qt + t_1 + t_0 + q(t_1 - r)$.*

Proof: Consider the $q+1$ projective planes through the line ℓ and consider the affine planes arising from these projective planes removing the line ℓ. Each such affine planes is incident with at least $t-r$ points of $B \setminus \ell$ and these affine planes are disjoint. So $|B| \geq (q+1)(t-r)+r = qt+t_1+t_0+q(t_1-r)$. ■

Lemma 5.2 *Let $B \subseteq \mathrm{PG}(3,q)$ be a t-fold blocking set with respect to planes and let Π be an arbitrary t-secant plane. The set $B \cap \Pi$ is not a (t_1+1)-fold blocking set with respect to the lines of Π.*

Proof: Suppose to the contrary that $B \cap \Pi$ is a (t_1+1)-fold blocking set in $\Pi \cong \mathrm{PG}(2,q)$. By Proposition 3.1, $t_1(q+1)+t_0 = |B \cap \Pi| \geq (q+1)(t_1+1)$, and $t_0 \geq q+1$, that is a contradiction. ■

The following theorem follows from special cases of Theorem 2.1 and Theorem 2.5 in Hamada [11]. We include a proof since it is short.

Theorem 5.3 *Let $B \subseteq \mathrm{PG}(3,q)$ be a t-fold blocking set with respect to planes such that there exists a t-secant plane Π. If*

$$|B| \leq qt + t_1 + t_0 + q - 1$$

then

$$|B| \geq qt + t_1 + t_0.$$

Moreover, B is a t_1-fold blocking set with respect to lines and every t-secant plane contains a t_1-secant line.

Proof: If there exists a (t_1-1)-secant line ℓ then Lemma 5.1 gives $|B| \geq qt + t_1 + t_0 + q$. (If there exist an r-secant line, $r < t_1 - 1$, then Lemma 5.1 gives a better lower bound.) Lemma 5.2 implies that B is not a (t_1+1)-fold blocking set with respect to the lines of the t-secant planes, thus each t-secant plane has to contain an r-secant line, where $r \leq t_1$, and thus Lemma 5.1 gives $|B| \geq qt + t_1 + t_0$ ■

We will extend Theorem 5.3 to higher dimensions in Theorem 6.4.

Corollary 5.4 *Let $B \subseteq \mathrm{PG}(3,q)$ be a t-fold blocking set with respect to planes such that there exists a t-secant plane Π. Then*

$$|B| \geq qt + t_1 + t_0 \qquad ■$$

Theorem 5.5 *Let $B \subseteq \mathrm{PG}(3,q)$ be a t-fold blocking set with respect to planes such that there exists a t-secant plane Π. If $t_1 \geq 1$ and $t_0 \leq \Delta_q(t_1) - 1$ then*

$$|B| \geq qt + t_1 + t_0 + q$$

Proof: $|B \cap \Pi| = t = (q+1)t_1 + t_0$. If $t_0 \leq \Delta_q(t_1) - 1$ then $B \cap \Pi$ cannot be a t_1-fold blocking set with respect to the lines of Π, and thus, B cannot be a t_1-fold blocking set with respect to lines. Now use Theorem 5.3. ■

Remark 5.6 *If $t_1 = 0$ then $t = t_0 \leq q$ and thus, the union of t lines among of the elements of an arbitrary* spread (of lines) *is a t-fold blocking set (with respect to planes) that meets the bound in Corollary 5.4.* ■

6 Multiple blocking sets in higher dimensions

In this section let $\delta \geq 4$ denote the dimension of the finite projective space $\mathrm{PG}(\delta,q)$ or $\mathrm{PG}(\delta,p)$. Following Hamada [11], let $1 \leq t \leq \frac{q^\delta-1}{q-1} - 1$ be represented in the form

$$t = \sum_{i=0}^{\delta-2} t_i \frac{q^{i+1}-1}{q-1} = t_{\delta-2}\frac{q^{\delta-1}-1}{q-1} + \cdots + t_1(q+1) + t_0 \tag{8}$$

where $0 \leq t_i \leq q$ for each i and if $t_j = q$ then $t_0 = t_1 = \cdots = t_{j-1} = 0$. The last condition makes the representation of t unique. This representation of t has the following property.

$$qt + \sum_{i=1}^{\delta-1} t_{i-1} = \sum_{i=1}^{\delta-1} t_{i-1}\frac{q^{i+1}-1}{q-1} \tag{9}$$

Similarly, let $0 \leq r \leq \frac{q^{\delta+1}-1}{q-1} - 1$ be represented in the form

$$r = \sum_{i=0}^{\delta-1} r_i \frac{q^{i+1}-1}{q-1} = r_{\delta-1}\frac{q^{\delta}-1}{q-1} + \cdots + r_1(q+1) + r_0 \tag{10}$$

where $0 \leq r_i \leq q$ for each i and if $r_j = q$ then $r_0 = r_1 = \cdots = r_{j-1} = 0$. This representation of r has the the following properties,

$$r = \sum_{i=0}^{\delta-1} r_i \frac{q^{i+1}-1}{q-1} = q\left(\sum_{i=1}^{\delta-1} r_i \frac{q^{i}-1}{q-1}\right) + \sum_{i=0}^{\delta-1} r_i, \tag{11}$$

$$r - qt - \sum_{i=1}^{\delta-1} t_{i-1} = r_0 + \sum_{i=1}^{\delta-1} (r_i - t_{i-1}) \frac{q^{i+1}-1}{q-1}. \tag{12}$$

The following lemma describes another property of these representations of t and r, which will be needed to extend Hamada's theorem [11, Theorem 2.5] to Theorem 6.4.

Lemma 6.1 *If there exists a $j \in \{1, \ldots, \delta-1\}$ such that $r_j \leq t_{j-1} - 1$ and $r_i = t_{i-1}$ for all $i > j$ then*

$$\sum_{i=1}^{\delta-1} (r_i - t_{i-1}) \frac{q^i - 1}{q-1} \leq -1 \quad \textit{and also} \quad r_0 + \sum_{i=1}^{\delta-1} (r_i - t_{i-1}) \frac{q^{i+1}-1}{q-1} \leq -1. \tag{13}$$

Similarly, if there exists a $j \in \{1, \ldots, \delta-1\}$ such that $r_j \geq t_{j-1} + 1$ and $r_i = t_{i-1}$ for all $i > j$ then

$$\sum_{i=1}^{\delta-1} (r_i - t_{i-1}) \frac{q^i - 1}{q-1} \geq 1 \quad \textit{and also} \quad r_0 + \sum_{i=1}^{\delta-1} (r_i - t_{i-1}) \frac{q^{i+1}-1}{q-1} \geq 1. \tag{14}$$

Proof: In the first case

$$\sum_{i=1}^{\delta-1} (r_i - t_{i-1}) \frac{q^i - 1}{q-1} \leq -\frac{q^j - 1}{q-1} + \sum_{i=1}^{j-1} r_i \frac{q^i - 1}{q-1} \leq -1,$$

since

$$\sum_{i=1}^{j-1} r_i \frac{q^i - 1}{q-1} \leq \frac{q^j - 1}{q-1} - 1.$$

Moreover

$$r_0 + \sum_{i=1}^{\delta-1} (r_i - t_{i-1}) \frac{q^{i+1}-1}{q-1}$$

$$\leq -\frac{q^{j+1}-1}{q-1} + r_0 + \sum_{i=1}^{j-1} r_i \frac{q^{i+1}-1}{q-1} = -\frac{q^{j+1}-1}{q-1} + \sum_{i=0}^{j-1} r_i \frac{q^{i+1}-1}{q-1} \leq -1,$$

since

$$\sum_{i=0}^{j-1} r_i \frac{q^{i+1}-1}{q-1} \leq \frac{q^{j+1}-1}{q-1} - 1.$$

The other case is similar. ■

Lemma 6.2 *Let $B \subseteq \mathrm{PG}(\delta, q)$ be an r-fold blocking set with respect to hyperplanes for which there is an r-secant hyperplane $\Pi_{\delta-1}$. If $B \cap \Pi_{\delta-1}$ is a t-fold blocking set with respect to the hyperplanes of $\Pi_{\delta-1}$ and there exists a t-secant hyperplane $\Pi_{\delta-2}$ of $\Pi_{\delta-1}$ then*

$$|B| \geq qr + \sum_{i=0}^{\delta-1} r_i + q\left(\sum_{i=1}^{\delta-1}(r_i - t_{i-1})\frac{q^i-1}{q-1}\right) \tag{15}$$

Proof: Consider the $q+1$ hyperplanes intersecting each other in the t-secant 2-codimensional space $\Pi_{\delta-2}$ and partitioning the points of $\mathrm{PG}(\delta, q) \setminus \Pi_{\delta-2}$.

$$|B| \geq (q+1)(r-t) + t = qr + r - qt =$$

$$qr + q\left(\sum_{i=1}^{\delta-1} r_i \frac{q^i-1}{q-1}\right) + \sum_{i=0}^{\delta-1} r_i - q\left(\sum_{i=1}^{\delta-1} t_{i-1}\frac{q^i-1}{q-1}\right)$$

using Equation (11). ■

Definition 6.3 *If $(s_n, \ldots, s_1)$ is an arbitrary n-tuple then let the expression $[s_n, \ldots, s_1]$ mean the following sum*

$$[s_n, \ldots, s_1] = \sum_{i=1}^{n} s_i \frac{q^i-1}{q-1}.$$

Let N be defined as j if $t_j = q$ and $\delta - 2$ if no such j exists.

In [11, Theorem 2.5] Hamada proves the following for the main case $N = \delta - 2$.

Theorem 6.4 *Let $B \subseteq \mathrm{PG}(\delta, q)$ be a t-fold blocking set with respect to hyperplanes for which there exists a t-secant hyperplane $\Pi_{\delta-1}$ of $\mathrm{PG}(\delta, q)$. If*

$$|B| \leq qt + \sum_{i=0}^{\delta-2} t_i + q - 1$$

then

$$|B| \geq qt + \sum_{i=0}^{\delta-2} t_i$$

and for each $j = 0, \ldots, N$ the set B is a $[t_{\delta-2}, \ldots, t_j]$-fold blocking set with respect to $(\delta - j - 1)$-dimensional subspaces. Moreover, for each $[t_{\delta-2}, \ldots, t_j]$-secant $(j+1)$-codimensional subspace $\Pi_{\delta-j-1}$ there exists a sequence $\Pi_{\delta-2-N} < \cdots < \Pi_{\delta-j-1}$ of subspaces, each a hyperplane of the following one, such that for each $i = j, \ldots, N+1$ we have $|\Pi_{\delta-i-1} \cap B| = [t_{\delta-2}, \ldots, t_i, t_{i-1}]$.

Proof: If $\delta = 3$ then the theorem follows from Theorem 5.3. By induction on δ suppose that the theorem is true for $\mathrm{PG}(\delta, q)$ and let $B \subseteq \mathrm{PG}(\delta+1, q)$ be an r-fold blocking set with respect to hyperplanes and let $\Pi_\delta \cong \mathrm{PG}(\delta, q)$ be an arbitrary r-secant hyperplane of $\mathrm{PG}(\delta+1, q)$. Let t be such that $B \cap \Pi_\delta$ is a t-fold blocking set with respect to the hyperplanes of Π_δ and there exists a t-secant hyperplane $\Pi_{\delta-1} \cong \mathrm{PG}(\delta-1, q)$ of Π_δ. By induction we know that

$$r = |B \cap \Pi_\delta| \geq qt + \sum_{i=0}^{\delta-2} t_i \tag{16}$$

and thus

$$r - qt - \sum_{i=0}^{\delta-2} t_i = r_0 + \sum_{i=1}^{\delta-1} (r_i - t_{i-1}) \frac{q^{i+1} - 1}{q - 1} \geq 0. \tag{17}$$

If there exists an index $j \in \{1, \ldots, \delta - 1\}$ such that $r_j \neq t_{j-1}$ then let j be the largest such index. If $r_j \leq t_{j-1} - 1$ then (13) in Lemma 6.1 says that

$$r_0 + \sum_{i=1}^{\delta-1} (r_i - t_{i-1}) \frac{q^{i+1} - 1}{q - 1} \leq -1, \text{ that contradicts (17).}$$

If $r_j \geq t_{j-1} + 1$ then (14) in Lemma 6.1 says

$$\left(\sum_{i=1}^{\delta-1} (r_i - t_{i-1}) \frac{q^i - 1}{q - 1} \right) \geq 1,$$

and using (15) in Lemma 6.2 we get

$$|B| \geq \left(qr + \sum_{i=0}^{\delta-1} r_i \right) + q \left(\sum_{i=1}^{\delta-1} (r_i - t_{i-1}) \frac{q^i - 1}{q - 1} \right) \geq qr + \sum_{i=0}^{\delta-1} r_i + q.$$

Otherwise, for each $i = 1, \ldots, \delta - 1$ we have $r_i = t_{i-1}$ and Lemma 6.2 implies

$$|B| \geq qr + \sum_{i=0}^{\delta-1} r_i.$$

For each $j = 1, \ldots, \delta$, we have $[t_{\delta-2}, \ldots, t_{\delta-1-j}] = [r_{\delta-1}, \ldots, r_{\delta-j}]$.

If $r_0 \leq q - 1$ then $|B \cap \Pi_\delta| = r \leq qt + \sum_{i=0}^{\delta-1} t_i + q - 1$ and thus, by induction we have that for each $j = 1, \ldots, \delta - 1$ the set $B \cap \Pi_\delta$ is a $[t_{\delta-2}, \ldots, t_{\delta-1-j}]$-fold blocking set with respect to j-dimensional subspaces and for each $[t_{\delta-2}, \ldots, t_{\delta-1-j}]$-secant j-dimensional subspace Π_j there exists a sequence $\ell = \Pi_1 < \cdots < \Pi_{j-1} < \Pi_j$ of subspaces, each a hyperplane of the following one, such that for each $i = 1, \ldots, j$ we have $|\Pi_i \cap B| = [t_{\delta-2}, \ldots, t_{\delta-1-i}]$. ■

The following is from Hamada [11, Theorem 2.2].

Corollary 6.5 *If $B \subseteq \mathrm{PG}(\delta, q)$ is a $t = [t_{\delta-2}, \ldots, t_0]$-fold blocking set with respect to hyperplanes such that there exists a t-secant hyperplane $\Pi < \mathrm{PG}(\delta, q)$ then*

$$|B| \geq [t_{\delta-2}, \ldots, t_1, t_0, 0] = qt + \sum_{i=0}^{\delta-2} t_i \qquad \blacksquare$$

The following appears to be new.

Theorem 6.6 *Let $B \subseteq \mathrm{PG}(\delta, q)$ be a t-fold blocking set with respect to hyperplanes such that there exists a t-secant hyperplane. If $t_{\delta-4}, \ldots, t_1, t_0 \leq q-1$ and $t_{\delta-2} \geq 1$ and $t_{\delta-3} \leq \Delta_q(t_{\delta-2}) - 1$ then*

$$|B| \geq [t_{\delta-2}, \ldots, t_1, t_0, q] = qt + \sum_{i=0}^{k-2} t_i + q.$$

Proof: Suppose that $|B| \leq qt + \sum_{i=0}^{k-2} t_i + q - 1$. By Theorem 6.4, B is a $t_{\delta-2}$-fold blocking set with respect to lines and, since $N = \delta - 2$, there is a plane Π_2 $(i = \delta - 3)$ with the property that

$$|B \cap \Pi_2| = [t_{\delta-2}, t_{\delta-3}, t_{\delta-4}].$$

By Theorem 5.5,

$$|B \cap \Pi_2| \geq [t_{\delta-2}, t_{\delta-3}, q],$$

a contradiction. $\blacksquare$

7 Multiple blocking sets in the prime case

Theorem 5.5 and Theorem 6.6 have the following consequence using the bounds for $\Delta_p(t)$ given by Theorem 2.3.

Corollary 7.1 *Let p be a* prime *and let $B \subseteq \mathrm{PG}(\delta, p)$ be a t-fold blocking set with respect to hyperplanes such that there exists a t-secant hyperplane. Suppose that either $\delta = 3$ or $\delta \geq 4$ and $t_{\delta-4}, \ldots, t_1, t_0 \leq p-1$. If $t_{\delta-2} \geq 2$ and $t_{\delta-3} \leq \min\left\{\frac{p-1}{2}, p-1-t_{\delta-2}\right\}$ then*

$$|B| \geq [t_{\delta-2}, \ldots, t_0, p] = pt + \sum_{i=0}^{\delta-2} t_i + p.$$

Furthermore, the bound holds if $p = 7$, $t_{\delta-2} = 2$ and $t_{\delta-3} \leq 4$, $p = 11$, $t_{\delta-2} = 2$ or 3 and $t_{\delta-3} \leq 6$, $p = 13$, $t_{\delta-2} = 2$ or 3 and $t_{\delta-3} \leq 7$, $p = 17$, $t_{\delta-2} = 2$ or 3 and $t_{\delta-3} \leq 9$, or $p = 19$, $t_{\delta-2} = 2$ and $t_{\delta-3} \leq 10$. $\blacksquare$

We shall use of series of lemmas to prove the same bound for $|B|$ in roughly half the cases when $t_{\delta-2} = 1$.

The following lemma can be deduced directly from [14, Theorem 3.14].

Lemma 7.2 *Let $B \subseteq \mathrm{PG}(\delta, p)$ be a blocking set with respect to lines. If $|B| < 3(p^{\delta-1}+1)/2$ then B contains a hyperplane.* ■

The following can be deduced from [2, Theorem 2.2].

Lemma 7.3 *If $t < p$ then a t-fold blocking set with respect to affine planes of $\mathrm{AG}(3, p)$ contains at least $(t+2)p - 2$ points.* ■

Theorem 7.4 *Let $B \subseteq \mathrm{PG}(\delta, p)$ be a $[1, t_{\delta-3}, \ldots, t_0]$-fold blocking set with respect to hyperplanes and $\delta \geq 3$. If $t_i \leq p-1$ for all $i = 0, \ldots, \delta-3$, $t_{\delta-3} \neq 0$ and*

$$\sum_{i=0}^{\delta-3} t_i(p^{i+2}-1) < \frac{(p-3)}{2}(p^{\delta-1}-1) - (p-1)^2$$

then

$$|B| \geq tp + \sum_{i=0}^{\delta-2} t_i + p.$$

Proof: Suppose that $|B| \leq tp + \sum_{i=0}^{\delta-2} t_i + p - 1$.

By Theorem 6.4, B is 1-fold blocking set of $\mathrm{PG}(\delta, p)$ with respect to lines. By assumption

$$|B| \leq tp + \sum_{i=0}^{\delta-2} t_i + p - 1 = \frac{p^\delta - 1}{p-1} + \sum_{i=0}^{\delta-3} t_i \frac{(p^{i+2}-1)}{p-1} + p - 1$$

$$< \frac{p^\delta - 1}{p-1} + \frac{(p-3)(p^{\delta-1}-1)}{2(p-1)} = \frac{3p^{\delta-1}-1}{2},$$

and so, by Lemma 7.2, B contains a hyperplane Π.

By Theorem 6.4 the set B is a $(p+1+t_{\delta-3})$-fold blocking set with respect to planes. Therefore, $B \setminus \Pi$ is $t_{\delta-3}$-fold blocking set with respect to planes in each affine three dimensional subspace $\Sigma \setminus \Pi$. Let Ω be a plane of H. In each of the $p^{\delta-3}$ affine subspaces $\Sigma \setminus \Pi$, where Σ contains Ω and is not contained in Π,

$$|(B \cap \Sigma) \setminus \Pi| \geq (t_{\delta-3}+2)p - 2.$$

Hence

$$|B| \geq p^{\delta-3}(t_{\delta-3}p + 2p - 2) + \frac{p^\delta - 1}{p-1} > tp + \sum_{i=0}^{\delta-2} t_i + p.$$

■

The following was proved by Blokhuis in [5].

Lemma 7.5 *Suppose that the polynomial $f(X) = g(X)X^p + h(X)$ is a product of linear polynomials of $\mathbb{F}_p[X]$ and that the degree of g and h is at most $(p-1)/2$. Either $f(X) = g(X)(X^p - X)$ or $f(X) = g(X)(X^p + c)$ for some $c \in \mathbb{F}_p$.* ■

The following is a generalisation of Blokhuis' Theorem, Theorem 2.3 to $\delta \geq 3$. In what follows we assume that $[t_{\delta-2}, \ldots, t_2, t_1 + 1] = t_1 + 1$ and $[t_{\delta-2}, \ldots, t_2] = 0$ if $\delta = 3$.

Theorem 7.6 *Let $\delta \geq 3$ and suppose that $B \subseteq \mathrm{PG}(\delta, p)$ is a t-fold blocking set with respect to hyperplanes and that $t_0 \geq 1$.*

If there exists a $[t_{\delta-2}, \ldots, t_2, t_1 + 1]$-secant $(\delta - 2)$-dimensional subspace, contained in a t-secant hyperplane but not contained in any hyperplane incident with at least $p + t$ points of B, then

$$|B| \geq pt + \sum_{i=0}^{\delta-2} t_i + \min\left\{\frac{p+1}{2}, p - t_0\right\}.$$

Proof: Note that $t_0 \geq 1$ implies that $p - 1 \geq t_1$.

Let Ω, the hyperplane defined by the equation $X_0 = 0$, be a t-secant to B. Let Σ, the co-dimension two subspace defined $X_0 = X_1 = 0$, be a $[t_{\delta-2}, \ldots, t_2, t_1 + 1]$-secant not contained in any hyperplane incident with at least $p + t$ points of B.

Assume that $|B| = tp + \sum_{i=0}^{\delta-2} t_i + m$ and that $m \leq p - t_0 - 1$. We shall prove that $m \geq (p+1)/2$.

By Theorem 6.4, if $\delta \geq 4$ then $B \cap \Sigma$ is a $[t_{\delta-2}, \ldots, t_3, t_2]$-fold blocking set of the hyperplanes of Σ. Moreover, since

$$|B \cap \Sigma| = [t_{\delta-2}, \ldots, t_2, t_1 + 1] \leq [t_{\delta-2}, \ldots, t_3, t_2 + 1, 0] - 1$$

there is a hyperplane, Π of Σ, which is a $[t_{\delta-2}, \ldots, t_3, t_2]$-secant to B.

If $\delta = 3$ then let Π be a point not in B.

Let Π be defined by the equation $X_0 = X_1 = X_2 = 0$.

Let x_0, x_1 be elements of $\mathbb{F}_p$. The hyperplanes $x_0X_0 + x_1X_1 + X_2 = 0$ are incident with at least $r = t - [t_{\delta-2}, \ldots, t_3, t_2]$ points of $B \setminus \Sigma$, since Π is a $[t_{\delta-2}, \ldots, t_3, t_2]$-secant to B. Thus the polynomial

$$f(X_0, X_1) = \prod_{a \in B \setminus \Sigma} (a_0X_0 + a_1X_1 + a_2)$$

has a zero of multiplicity at least r at every $(x_0, x_1) \in \mathbb{F}_p^2$.

By Bruen [8], there are polynomials g_j of degree at most $|B \setminus \Sigma| - rp$ such that

$$f(X_0, X_1) = \sum_{j=0}^{r} (X_0^p - X_0)^{r-j} (X_1^p - X_1)^j g_j(X_0, X_1).$$

The degree of g_j is at most

$$tq + \sum_{i=0}^{\delta-2} t_i + m - [t_{\delta-2}, \ldots, t_2, t_1 + 1] - tq + [t_{\delta-2}, \ldots, t_3, t_2]q = m + t_0 - 1.$$

Let $f^*(X_0)$ be the polynomial which are the terms of highest degree occurring in f with $X_1 = 1$. Define g_j^* similarly. The polynomial

$$f^*(X_0) = \prod_{a \in B \setminus \Sigma} (a_0 X_0 + a_1)$$

is of degree $|B| - t$, since Ω is a t-secant.

Let $s = \sum_{i=1}^{\sigma-2} t_i p^{i-1} = [t_{\delta-2}, \ldots, t_1] - [t_{\delta-2}, \ldots, t_2]$, and so $r - s = t - [t_{\delta-2}, \ldots, t_1]$. Then

$$|B| - t = tp + \sum_{i=0}^{\delta-2} t_i + m - t = (r - s)p + m.$$

The hyperplane $X_1 = 0$ is incident with at least

$$t - [t_{\delta-2}, \ldots, t_1] - 1 = r - s - 1 = sp + t_0 - 1$$

points of $B \setminus \Sigma$, and so X_0^{sp} divides f^*. Hence, we have that

$$f^*(X_0) = \prod_{a \in B \setminus \Sigma} (a_0 X_0 + a_1) = \sum_{j=s}^{r-s} X_0^{(r-j)p} g_j^*(X_0), \tag{18}$$

where the degree of $g_s^* = m$ and for $j = s+1, \ldots, r-s$ the degree of g_j^* is at most $m + t_0 - 1 \leq p - 2$.

Every hyperplane containing Σ is incident with at least $t - [t_{\delta-2}, \ldots, t_1 + 1] = r - s - 1$ points of $B \setminus \Sigma$ and so $(X_0^q - X_0)^{r-s-1}$ divides $f^*(X)$.

Define $l(X_0)$, a polynomial of degree at most $p - 1$, by the identity

$$f^*(X_0) = (X_0^p - X_0)^{r-s-1} (X_0^p g_s^* + l(X_0) + g_{r-s}^* / (-X_0)^{t_0 - 1}).$$

Note that X_0^{sp+p} divides $X_0^{r-s-1} l(X_0)$, or in other words $X_0^{p-t_0+1}$ divides $l(X_0)$.

The degree of g_s^* is m and the degree of $g_{r-s}^*/(-X_0)^{t_0-1}$ is at most m. Note that $r-s-1+m = t_0+m-1$ modulo p which is less than $p-2$ by assumption. Therefore, the terms of degree -1 modulo p in f^* come from $(X_0^q - X_0)^{sp+t_0-1} l(X_0)$. The coefficient of $X_0^{(ps+t_0-1-i)p+p-1}$, for $i = 0, \dots t_0-1$ is

$$(-1)^i \binom{t_0-1}{i} l_{p-i-1},$$

where l_i is the coefficient of X_0^i in $l(X_0)$. Equation (18) implies f^* has no terms of degree -1 modulo p, hence $l_{p-1-i} = 0$. Therefore, $l(X_0) = 0$.

By Lemma 7.5, the polynomial $X_0^p g_s^* + g_{r-s}^*/(-X_0)^{t_0-1}$, is equal to $(X_0^p - X_0)g_s^*$, $(X_0^p - c)g_s^*$ for some $c \in \mathbb{F}_p$, or $m \geq (p+1)/2$. The first case cannot occur since the degree of g_s^* is at least the degree of $g_{r-s}^*/(-X_0)^{t_0-1}$. The second case does not occur since we assumed that Σ is not contained in any hyperplane with at least $p+t$ points of B. Hence, $m \geq (p+1)/2$. ■

8 Further improvements to the Griesmer bound

Let C be a q-ary linear code of length n, dimension k and minimum distance $d < q^{k-1}$ meeting the Griesmer bound, in other words

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

Write $d = \sum_{i=s}^{k-2} d_i q^i$, where $0 \leq d_i \leq q-1$ for $i = s, \dots, k-2$ and $d_s \neq 0$. Then

$$n = [d_{k-2}, \dots, d_0] + k - 1 - s.$$

As in the introduction, since C is a projective code we can construct a t-fold blocking set with respect to hyperplanes B of $\mathrm{PG}(k-1, q)$ where

$$t = \frac{q^{k-1}-1}{q-1} - n + d, \tag{19}$$

and

$$|B| = \frac{q^k-1}{q-1} - n = \frac{q^k-1}{q-1} - [d_{k-2}, \dots, d_0] - k + 1 + s.$$

Substituting for n in (19) gives

$$t = \frac{q^s-1}{q-1} + \sum_{j=s}^{k-2} (q-1-d_j) \frac{q^j-1}{q-1}.$$

As in the previous section, we write $t = \sum_{i=0}^{k-3} t_i \frac{q^{i+1}-1}{q-1}$, and conclude that if $s \neq 0$ then for $j = s, \ldots, k-3$

$$t_j = q - 1 - d_{j+1}, \tag{20}$$

that $t_{s-1} = q - d_s$ and $t_j = 0$ for $j \leq s-2$. If $s = 0$ then

$$t_j = q - 1 - d_{j+1}, \tag{21}$$

for $j = 0, \ldots, k-3$.

By careful calculation, substituting for t_j with the above, we have for $s \neq 0$

$$tq + \sum_{i=0}^{k-3} t_i = \frac{q^k - 1}{q-1} - k + s + 1 - \sum_{i=s}^{k-2} d_i \frac{q^{i+1}-1}{q-1} = \frac{q^k-1}{q-1} - n, \tag{22}$$

and for $s = 0$

$$tq + \sum_{i=0}^{k-3} t_i = \frac{q^k - 1}{q-1} - k - q + 1 - \sum_{i=1}^{k-2} d_i \frac{q^{i+1}-1}{q-1} = \frac{q^k-1}{q-1} - n + d_0 - q. \tag{23}$$

Now we can translate Theorem 7.4 and Theorem 7.6 into their corresponding results in terms of linear codes meeting the Griesmer bound.

The following is a corollary to Theorem 7.4, which extends Theorem 4.3.

Corollary 8.1 *Let p be prime and suppose that there is a k-dimensional linear code of length n and minimum distance $d < p^{k-1}$ over $\mathbb{F}_p$. If $k \geq 4$, $d_{k-2} = p-2$ and $p-2 \geq d_{k-3} \geq (p+3)/2$ then*

$$n \geq g(k,d) + 1 = 1 + \sum_{i=0}^{k-1} \left\lceil \frac{d}{p^i} \right\rceil.$$

Proof: The condition in Theorem 7.4 that $t_{\delta-3} \neq 0$ translates to $d_{k-3} \neq p-1$.

The condition

$$\sum_{i=0}^{\delta-3} t_i (p^{i+2} - 1) \leq \frac{(p-3)}{2}(p^{\delta-1} - 1) - (p-1)^2$$

translates to

$$\frac{(p+3)}{2}\left(\frac{p^{\delta-1}-1}{p-1}\right) + p + 2 - p^{s+2} \leq \sum_{i=s+1}^{k-3} d_i \frac{p^{i+1}-1}{p-1}.$$

Therefore, if $d_{k-3} \geq (p+3)/2$ and $s \neq 0$ then

$$|B| = \frac{q^k - 1}{q-1} - n \geq \frac{q^k - 1}{q-1} - n + q,$$

which is clearly a contradiction. Thus, there is no code meeting the Griesmer bound for these values of d and k.

If $d_{k-3} \geq (p+3)/2$ and $s = 0$ then

$$|B| = \frac{q^k - 1}{q-1} - n \geq \frac{q^k - 1}{q-1} - n + d_0 - q + q,$$

which implies $d_0 = 0$ and therefore $s \geq 1$, also a contradiction. ■

An m-secant hyperplane of B corresponds to a codeword of weight $n - (q^{k-1} - 1)/(q-1) + m$. An m-secant $(\delta - 2)$-dimensional subspace of B corresponds to a pair of codewords c_1, c_2 with support

$$|sup(c_1) \cup sup(c_2)| = n - \frac{q^{k-2} - 1}{q-1} + m.$$

In the latter case, if $m = [t_{\delta-2}, \ldots, t_2, t_1 + 1]$ and $s = 0$ or $s = 1$ then one can check by direct calculation using (20) and (21) that

$$|sup(c_1) \cup sup(c_2)| = d + \left\lceil \frac{d}{q} \right\rceil + 1.$$

The following is a corollary to Theorem 7.6, which generalizes the case $k = 3$ in Theorem 4.2. To be able to apply Theorem 7.6 we need that $t_0 \geq 1$ which implies that $s \leq 1$.

Corollary 8.2 *Let p be prime and suppose that there is a k-dimensional linear code of length n and minimum distance $d < p^{k-1}$ over $\mathbb{F}_p$. Suppose that $k \geq 4$ and either $d_1 \leq p-2$ and $d_0 \geq \max((p+1)/2, p - d_1)$, or $d_0 = 0$ and $d_1 \neq 0$. If there are codewords c_1 and c_2 such that*

$$|sup(c_1) \cup sup(c_2)| = d + \left\lceil \frac{d}{p} \right\rceil + 1,$$

the codeword c_1 has weight d, and all codewords in $\langle c_1, c_2 \rangle$ have weight less than $d + p$, then

$$n \geq g(k,d) + 1 = 1 + \sum_{i=0}^{k-1} \left\lceil \frac{d}{p^i} \right\rceil.$$

Proof: By Theorem 7.6 we have that the t-fold blocking set B that corresponds to the code meeting the Griesmer bound satisfies

$$|B| \geq tp + \sum_{i=0}^{\delta-2} t_i + \min\left(\frac{p+1}{2}, p - t_0\right). \tag{24}$$

If $s = 0$, in other words $d_0 \neq 0$ this, together with (23), gives

$$p - d_0 \geq \min\left(\frac{p+1}{2}, d_1 + 1\right),$$

which contradicts the assumption.

If $s = 1$ then $d_1 \neq 0$ and (24) together with (22) gives $0 \geq \min\left(\frac{p+1}{2}, d_1 + 1\right)$, a contradiction. ■

There are examples of linear codes which meet the Griesmer bound and whose minimum distance satisfies the above conditions. For these codes it follows that if there are codewords c_1 and c_2 such that

$$|sup(c_1) \cup sup(c_2)| = d + \left\lceil \frac{d}{p} \right\rceil + 1,$$

and c_1 has weight d, then there is a codeword in $\langle c_1, c_2 \rangle$ that has weight $d+p$.

For example, an ovoid O in $\mathrm{PG}(3, q)$ is a set of $q^2 + 1$ points which has the property that every hyperplane is incident with at most $q + 1$ points of O. The 4-dimensional code generated by the matrix whose columns are the points of O is of length $q^2 + 1$ and has minimum distance $q^2 - q$. Thus, $d_0 = 0$ and $d_1 = q - 1$. Corollary 8.2 says that (in the prime case) if there are codewords c_1 and c_2 such that $|sup(c_1) \cup sup(c_2)| = p^2$ and the weight of c_1 is $p^2 - p$, then there is a codeword, which we can assume is c_2 of weight p^2. This, in terms of the ovoid, simply states that every tangent line is contained in a tangent plane.

We now apply Corollary 8.2 to codes whose residual codes satisfy the hypothesis.

Theorem 8.3 *Let C be a k-dimensional linear code over $\mathbb{F}_p$ with minimum distance $d < p^{k-1}$ which meets the Griesmer bound. Suppose there are codewords $c_1, \ldots, c_m$, where $2 \leq m \leq k - 2$, with the property that for $j = 1, \ldots, m - 1$*

$$|\cup_{i=1}^{j} sup(c_i)| = \sum_{i=0}^{j-1} \left\lceil \frac{d}{p^i} \right\rceil$$

and

$$|\cup_{i=1}^{m} sup(c_i)| = \sum_{i=0}^{m-1} \left\lceil \frac{d}{p^i} \right\rceil + 1.$$

If any of the following occur,

1. p^{m-2} *does not divide* d *and* $d_{m-2} \geq \max(\frac{p-1}{2}, p - d_{m-1} - 1)$ *and* $d_{m-2} \neq p-1$,
2. p^{m-2} *does not divide* d *and* $d_{m-2} = p-1$ *and* $d_{m-1} \neq p-1$,
3. p^{m-2} *divides* d *and* $d_{m-2} \geq \max(\frac{p+1}{2}, p - d_{m-1})$,
4. p^{m-2} *divides* d *and* $d_{m-2} = 0$ *and* $d_{m-1} \neq 0$,

then there is a codeword in $\langle c_1, \ldots, c_m \rangle$ *of weight at least* $d + p$.

Proof: Let $C = C_0$ and consider the sequence of residual codes defined iteratively by $C_i = Res(C_{i-1}, c_i)$, for $i = 1, \ldots, m$. Let c^* denote the reduced codeword in C_{m-2} of a codeword c in C.

By hypothesis the codeword c^*_{m-1} has weight $\left\lceil \frac{d}{p^{m-2}} \right\rceil$ and

$$|sup(c^*_{m-1}) \cup sup(c^*_m)| = \left\lceil \frac{d}{p^{m-2}} \right\rceil + \left\lceil \frac{d}{p^{m-1}} \right\rceil + 1.$$

Since C is a code attaining the Griesmer bound, the mininum distance of C_{m-2} is $\left\lceil \frac{d}{p^{m-2}} \right\rceil$.

The hypothesis on d in Corollary 8.2 is satisfied in precisely the four cases listed, so applying Corollary 8.2 we conclude that there is a codeword c^* in C_{m-2} which has weight at least $\left\lceil \frac{d}{p^{m-2}} \right\rceil + p$.

We shall now construct iteratively a sequence of codewords x_i of C_i of weight at least $\left\lceil \frac{d}{p^i} \right\rceil + p$ for $i = m-2, m-3, \ldots, 0$. Let $x_{m-2} = c^*$. Let y_i be a codeword of C_i which reduces to x_{i+1} when we construct the residual code $C_{i+1} = Res(C_i, c_{i+1})$. For some $\lambda \in \mathbb{F}_p$ the codewords λc_{i+1} and y_i agree in at most

$$\frac{1}{q} \left\lceil \frac{d}{p^i} \right\rceil \leq \left\lceil \frac{d}{p^{i+1}} \right\rceil$$

coordinates. Thus, for this λ, the codeword $x_i = y_i - \lambda c_{i+1}$ has weight at least

$$\left\lceil \frac{d}{p^i} \right\rceil - \left\lceil \frac{d}{p^{i+1}} \right\rceil + \left\lceil \frac{d}{p^{i+1}} \right\rceil + p.$$

The codeword $x_0 \in C$ has weight at least $d + p$ and is in the subspace $\langle c_1, \ldots, c_m \rangle$. ■

9 Acknowledgements

We would like to thank the anonymous referees for their careful reading and suggestions, they were greatly appreciated.

References

[1] S. Ball, Multiple blocking sets and arcs in finite planes, *J. London Math. Soc.*, **54** (1996) 581–593.

[2] S. Ball, On intersection sets in Desarguesian affine spaces, *European J. Combin.*, **21** (2000) 441–446.

[3] S. Ball and A. Blokhuis, On the size of a double blocking set in $\mathrm{PG}(2, q)$, *Finite Fields and their Applications*, **2** (1996) 125–137.

[4] S. Ball and J. W. P. Hirschfeld, Bounds on (n, r)-arcs and their application to linear codes, *Finite Fields Appl.*, **11** (2005) 326–336.

[5] A. Blokhuis, On the size of a blocking set in $PG(2, p)$, *Combinatorica*, **14** (1994) 111–114.

[6] A. Blokhuis, L. Lovász, L. Storme and T. Szőnyi, On multiple blocking sets in Galois-planes, *Adv. Geom.*, **7** (2007) 39–53.

[7] A. Blokhuis, L. Storme and T. Szőnyi, Lacunary polynomials, multiple blocking sets and Baer-subplanes, *J. London Math. Soc.*, **60** (1999) 321–332.

[8] A. A. Bruen, Polynomial multiplicities over finite fields and intersection sets, *J. Combin. Theory Ser. A*, **60** (1992) 19–33.

[9] E. J. Cheon and T. Maruta, On the minimum length of some linear codes, *Des. Codes Cryptogr.*, **43** (2007) 123–135.

[10] S. Dodunekov amd J. Simonis, Optimal linear codes, unpublished manuscript.

[11] N. Hamada, A characterization of some $[n, k, d; q]$-codes meeting the Griesmer bound using a minihyper in a finite projective geometry, *Discrete Math.*, **116** (1993) 229–268.

[12] S. Ling, C. Xing, *Coding Theory, A First Course*, Cambridge, 2004.

[13] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*, North-Holland, 1977.

[14] T. Szőnyi and Zs. Weiner, Small blocking sets in higher dimensions, *Journal of Combinatorial Theory*, Series A, **95** (2001) 88–101.

[15] J. H. van Lint, *An Introduction to Coding Theory*, Second Edition, Springer, Berlin, 1992.