A BOUND FOR THE MAXIMUM WEIGHT OF A LINEAR CODE

SIMEON BALL AND AART BLOKHUIS

ABSTRACT. It is shown that the parameters of a linear code over $\mathbb{F}_q$ of length n, dimension k, minimum weight d and maximum weight m satisfy a certain congruence relation. In the case that $q = p$ is a prime, this leads to the bound $m \leq (n-d)p - e(p-1)$, where $e \in \{0, 1, \ldots, k-2\}$ is maximal with the property that

$$\binom{n-d}{e} \not\equiv 0 \pmod{p^{k-1-e}}.$$

Thus, if C contains a codeword of weight n then $n \geq d/(p-1) + d + e$.

The results obtained for linear codes are translated into corresponding results for (n,t)-arcs and t-fold blocking sets of $\mathrm{AG}(k-1,q)$. The bounds obtained in these spaces are better than the known bounds for these geometrical objects for many parameters.

1. INTRODUCTION

A *linear code* C is a k-dimensional subspace of $\mathbb{F}_q^n$, where $\mathbb{F}_q$ denotes the finite field with q elements. We say that C has *length* n and *dimension* k. The weight of a vector is the number of non-zero coordinates and we denote by d the minimum non-zero weight of C. The *Hamming distance* between two vectors u and v is the number of coordinates in which they differ. It is a simple matter to observe that the minimum distance between any two vectors of C is d, the minimum weight of C. For more on linear codes, see [8] or [11].

Date: 8 February 2013.

This research was initiated while the authors were visiting the Institute for Mathematical Sciences, National University of Singapore in 2011. The visit was supported by the Institute. The first author also acknowledges the support of the project MTM2008-06620-C03-01 of the Spanish Ministry of Science and Education and the project 2009-SGR-01387 of the Catalan Research Council. The second author was partially supported by ERC Advanced Research Grant no 267165 (DISCONV).

Let $q = p^h$, where p is a prime. In Section 5 we shall prove that if there is a linear code of length n, dimension k, minimum distance d and maximum weight $m \geq n - d + 1$ then for all $\epsilon \geq 1$, the coefficient of $X^{(n-d)q-m+\epsilon}$ in

$$(X-1)^{-m}(X^p-1)^{(n-d)q/p}$$

is divisible by q^{k-1}.

In Section 6 we shall prove that when $q = p$ this leads to the bound

$$m \leq (n-d)p - e(p-1), \tag{1.1}$$

where $e \in \{0, 1, \ldots, k-2\}$ is maximal with the property that

$$\binom{n-d}{e} \not\equiv 0 \pmod{p^{k-1-e}}.$$

Hence, if C contains a codeword of weight n then

$$n \geq d/(p-1) + d + e. \tag{1.2}$$

In Section 7 we translate the bounds obtained to bounds for (n, t)-arcs and t-fold blocking sets of hyperplanes in $\mathrm{AG}(k-1, q)$, the Desarguesian affine space.

We begin, however, in Section 2 with a discussion of the usefulness of these results and make a comparison with some known bounds.

2. Some discussion of the bounds

Let us first consider the bound (1.1) on the maximum weight of a codeword in a linear code over $\mathbb{F}_p$. Imagine one wants to construct a 3-dimensional code of length $n = 145$ and minimum distance $d = 133$ over $\mathbb{F}_{13}$. Since

$$\binom{12}{1} \not\equiv 0 \pmod{13}$$

the maximum weight of a codeword in such a code, according to (1.1) is

$$m \leq 12.13 - 12 = 144,$$

so there is no codeword of weight 145. A linear code with these parameters was found by Braun et al. [2], however the maximum weight of a codeword in this code is 141. This does not undermine the usefulness of (1.1) in this case because knowing that there is no codeword of weight 145 can help in when one wants to construct such a code. A popular method for constructing linear codes is to use anti-codes [8,

Section 17.6]. This is equivalent to finding a *t-fold blocking set* B of $\mathrm{PG}(k-1,q)$, a set of points with the property that every hyperplane of $\mathrm{PG}(k-1,q)$ contains at least t points of B and some hyperplane contains exactly t points of B. One writes down a generator matrix whose columns consist of all the points of $\mathrm{PG}(k-1,q)$ taken once and then remove the columns which belong to B. If the bound (1.1) implies $m < n$ then one cannot remove all the points on a hyperplane, in other words the t-fold blocking set B does not contain a hyperplane.

We are not aware of any examples of linear codes where $m < n$ and the bound (1.1) is acheived apart from the following almost trivial codes.

The even weight code over $\mathbb{F}_2$ where n is odd, $k = n-1$ and $d = 2$. Since $\binom{n}{2} \not\equiv 0 \mod 2$, we can put $e = k-2$ and then (1.1) gives $m \leq 2(k-1) - (k-2) = k < n$ and the maximum weight is k for this code. The other example is the 2-dimensional MDS code where $n = p+1$ and $d = p$. Then (1.1) gives $m \leq p < n$ and again the bound is obtained.

Now consider a linear code C with a codeword of weight n over a prime field. Thus we have the bound (1.2). As with all bounds for a linear code, the fact that we have three parameters n, k and d (we suppose q is fixed), we may consider the bound as a bound for one of them when we fix the other two parameters.

Let us consider a linear code over $\mathbb{F}_2$ with $d = 7$ and $k = 12$. If there is a code of length $n = 22$ then, since $\binom{15}{10} = 1 \mod 2$, we can put $e = k-2 = 10$ and then (1.2) implies $n \geq 24$, a contradiction. Hence $n \geq 23$ and indeed the binary Golay code is such a code of length 23.

As a further example, consider a linear code over $\mathbb{F}_3$ with $d = 6$ and $k = 6$. If there is a code of length $n = 11$ then, since $\binom{5}{4} = 2 \mod 3$, we can put $e = k-2 = 4$ and then (1.2) implies $n \geq 13$, a contradiction. Hence $n \geq 12$ and indeed the extended ternary Golay code is such a code of length 12.

However, the bound is probably best used in the following way. If we try to extend a linear code then we should try and increase the minimum distance too (since otherwise we cannot correct nor detect any more errors and there is no reason to extend) so it is natural to fix $r = n - d$ and k. Now, once they are fixed e is determined and (1.2) becomes an upper for n (or equivalently d).

By writing $d = \sum_{i=a}^{k-2} d_i p^i < p^{k-1}$, $d_a \neq 0$, the p-ary expansion of d we can compare (1.2) to the Griesmer bound ([6]) which states that for a linear code of length n,

dimension k and minimum distance d over $\mathbb{F}_p$,

$$n \geq \sum_{i=0}^{k-1} \lceil d/p^i \rceil.$$

We have

$$d/(p-1) + d + e - \sum_{i=0}^{k-1} \lceil d/p^i \rceil = (\sum_{i=a}^{k-2} d_i)/(p-1) + e + 1 + a - k.$$

Since e depends on $n-d$ and k (and so not directly on d), this can be positive, and improve on the Griesmer bound, but can also be negative and therefore not. Note, we reiterate that the bound (1.2) is only valid for linear codes over a prime field that contain a codeword of weight equal to its length, whereas the Griesmer bound is valid for all linear codes.

Codes which contain a codeword of weight equal to its length arise in a number of contexts. For example in [8, Section 19.6], they count the number of such binary linear codes C which are *weakly self-dual*, i.e. $C \subseteq C^\perp$ and conclude that many such codes exist. They also appear in the program GUAVA [5, Section 5.1] in the operation **AugmentedCode(C)**, where the all-one vector is added to the rows of a generator matrix of a linear code C in order to increase the dimension of the code. They also appear when we construct a linear code from an anti-code using a t-fold blocking set which contains a hyperplane of $\mathrm{PG}(k-1,q)$.

Finally, we mention the Plotkin bound [9] which applies to all codes where $d \geq n(q-1)/q$, in other words when the relative minimum distance is large. As we shall see in Section 4 all linear codes which contain a codeword of weight equal to its length satisfy $n \leq (n-d)q$ and so $d \leq n(q-1)/q$, i.e. the relative minimum distance is bounded above for such codes.

To prove (1.1) and (1.2) we shall use some very basic properties of complex characters, which we review in the next section.

3. Group characters

Let G be the additive group of $\mathbb{F}_q^{k-1}$ and denote by $\hat{G} = \{\chi_u \mid u \in G\}$ the multiplicative group of characters, so

$$\chi_u(x) = e^{2\pi i \mathrm{Tr}(x \cdot u)/p},$$

where $q = p^h$ for some prime p, Tr is the trace function from $\mathbb{F}_q$ to $\mathbb{F}_p$ and $x \cdot u$ is the standard inner product.

LEMMA 3.1. *Let $g(x) = \sum_{\chi \in \hat{G}} c_\chi \chi(x)$, where $c_\chi \in \mathbb{Z}$. If $g(x) = 0$ for all $x \in G \setminus \{0\}$, then q^{k-1} divides $g(0)$.*

Proof. We have

$$g(0) = \sum_{x \in G} g(x) = \sum_{x \in G} \sum_{\chi \in \hat{G}} c_\chi \chi(x) = \sum_{\chi \in \hat{G}} c_\chi \sum_{x \in G} \chi(x) = c_{\chi_0} |G|,$$

since $\sum_{x \in G} \chi(x) = 0$ unless $\chi = \chi_0$ in which case it is $|G|$. □

4. Linear codes containing a codeword of weight equal to its length

Let C be a linear code of length n, dimension k and minimum distance d which contains a codeword of weight n. Let A be a $k \times n$ generator matrix for C, so that $C = \{xA \mid x \in \mathbb{F}_q^k\}$, whose k-th row is a codeword of weight n. Let S be the multi-set of n vectors of $\mathbb{F}_q^k$ which are the columns of A. For any $x = (x_1, \ldots, x_k) \in \mathbb{F}_q^k$, the vector xA has at least d non-zero coordinates and so it has at most $n - d$ zero coordinates. Hence, there are at most $n - d$ vectors $(s_1, \ldots, s_k) \in S$ with the property that

$$x_1 s_1 + \cdots + x_k s_k = 0.$$

Therefore, there are at most $n - d$ vectors in S on the hyperplane of $\mathbb{F}_q^k$ defined by the equation

$$x_1 X_1 + \cdots + x_k X_k = 0.$$

Multiplying $u \in S$ by a non-zero scalar does not affect this property, so we can assume that the k-th coordinate of each of the vectors in S is 1. Thus, we can consider S as a subset of $\mathrm{AG}(k-1, q)$. As we have seen, every hyperplane of $\mathrm{AG}(k-1, q)$ contains at most $n - d$ points of S.

Now, fix an $x \in \mathbb{F}_q^{k-1}$, $x \neq 0$ and consider the q hyperplanes of $\mathrm{AG}(k-1, q)$ defined by the equation

$$x_1 X_1 + \cdots + x_{k-1} X_{k-1} = \alpha,$$

where $\alpha \in \mathbb{F}_q$. Each of these hyperplanes contains at most $n - d$ points of S, which has size n, and so $n \leq (n - d)q$.

The following theorem suggests that in general there is a much better bound.

THEOREM 4.1. *Let C be a linear code of length n, dimension k and minimum distance d over $\mathbb{F}_q$, where $q = p^h$ and p is prime. If C contains a codeword of weight n then, for all $\epsilon \geq 1$ and $\gamma \geq n - d$, the coefficient of $X^{\gamma q - n + \epsilon}$ in*

$$(X-1)^{-n}(X^p-1)^{\gamma q/p}$$

is divisible by q^{k-1}.

Proof. Let

$$f(X,x) = \prod_{u \in S}(X - \chi_u(x)),$$

so that it is a polynomial whose coefficients are complex valued functions, and for every $x \in G$ this defines a polynomial $f(X,x) \in \mathbb{C}[X]$. Let

$$g(X,x) = \sum_{j=0}^{\infty} g_j(x) X^j$$

be defined by $f(X,x)g(X,x) = 1$ and note that

$$g_j(x) = \sum_{\chi \in \hat{G}} c_\chi \chi(x),$$

for some $c_\chi \in \mathbb{Z}$. Furthermore, for some $\gamma \geq n - d$, define

$$h(X,x) = (X^p - 1)^{\gamma q/p} g(X,x)$$

and so

$$f(X,x)h(X,x) = (X^p-1)^{\gamma q/p}.$$

For $x_0 \in \mathbb{F}_q^{k-1}$, $x_0 \neq 0$, and $\alpha \in \mathbb{F}_q$, there are at most $n - d$ points $u \in S$ such that $x_0 \cdot u = \alpha$. Thus, the multi-set $\{\chi_u(x_0) \mid u \in S\}$ contains each p-th root of unity repeated at most $(n-d)q/p$ times. This implies that $f(X,x_0)$ divides $(X^p-1)^{\gamma q/p}$ and so $h(X,x_0)$ is a polynomial, and it is a polynomial of degree $\gamma q - n$. Therefore, for all $\epsilon \geq 1$, the coefficient of $X^{\gamma q - n + \epsilon}$ in $h(X,x_0)$ is zero. Hence, the function

$$\sum_{r=0}^{\lfloor (\gamma q - n + \epsilon)/p \rfloor} (-1)^r \binom{\gamma q/p}{r} g_{\gamma q - n + \epsilon - rp}(x)$$

is zero, for all $x = x_0 \neq 0$.

By Lemma 3.1,

$$\sum_{r=0}^{\lfloor(\gamma q-n+\epsilon)/p\rfloor}(-1)^r\binom{\gamma q/p}{r}g_{\gamma n-n+\epsilon-rp}(0)\equiv 0 \pmod{q^{k-1}},$$

and so the coefficient of $X^{\gamma q-n+\epsilon}$ in $h(X,0)$ is divisible by q^{k-1}.

It only remains to note that since $f(X,0)=(X-1)^n$, we have

$$h(X,0)=(X-1)^{-n}(X^p-1)^{\gamma q/p}.$$

□

5. A condition on the parameters of a linear code

Theorem 4.1 has the following corollary.

Corollary 5.1. *Let C be a linear code of length n, dimension k, minimum distance d and maximum weight m over $\mathbb{F}_q$, where $q=p^h$ and p is prime. If $m\geq n-d+1$ then, for all $\epsilon\geq 1$ and $\gamma\geq n-d$, the coefficient of $X^{\gamma q-m+\epsilon}$ in*

$$(X-1)^{-m}(X^p-1)^{\gamma q/p}$$

is divisible by q^{k-1}.

Proof. The code C is shortened to a code of length m, dimension k and minimum distance d' (where $m-d'\leq n-d$) containing a codeword of length m. Apply Theorem 4.1 to the shortened code. □

We introduce a sum $\pi_{\ell,m}$ which will allow us to exploit this congruence. Let Δ be the set of p-th roots of unity and define

$$\pi_{\ell,m}=\sum_{\delta\in\Delta}(\delta X-1)^{-m}(X^p-1)^{\ell q/p}.$$

The coefficient of X^{rp} in $\pi_{n-d,m}$ is p times the coefficient of X^{rp} in

$$(X-1)^{-m}(X^p-1)^{(n-d)q/p},$$

for all $r\in\mathbb{N}$. Therefore, if we can calculate the exact number of times p divides the coefficients of $\pi_{n-d,m}$ then we can use Corollary 5.1 to obtain a bound for m.

We will use the following lemma.

LEMMA 5.2. *For $\ell \geq 1$,*

$$\pi_{\ell,m} = \sum_{t=1}^{q-1} \sum_{i=\lceil t/p \rceil}^{q/p} \binom{q/p}{i} \binom{ip}{t} (-1)^{q/p-i} \pi_{\ell-1,m-t} + \pi_{\ell-1,m-q}.$$

Proof. For all $\delta \in \Delta$, using the binomial theorem,

$$(X^p - 1)^{q/p} = \sum_{i=0}^{q/p} (-1)^{q/p-i} \binom{q/p}{i} X^{ip} = \sum_{i=0}^{q/p} \binom{q/p}{i} (1 + (\delta X - 1))^{ip} (-1)^{q/p-i}$$

$$= \sum_{i=0}^{q/p} \sum_{t=0}^{ip} \binom{q/p}{i} \binom{ip}{t} (-1)^{q/p-i} (\delta X - 1)^t = \sum_{t=0}^{q} \sum_{i=\lceil t/p \rceil}^{q/p} \binom{q/p}{i} \binom{ip}{t} (-1)^{q/p-i} (\delta X - 1)^t.$$

Note that $0 = (1 + (-1))^{q/p} = \sum_{i=0}^{q/p} \binom{q/p}{i} (-1)^i$, so we have that

$$(X^p - 1)^{q/p} = (\delta X - 1)^q + \sum_{t=1}^{q-1} \sum_{i=\lceil t/p \rceil}^{q/p} \binom{q/p}{i} \binom{ip}{t} (-1)^{q/p-i} (\delta X - 1)^t$$

Since

$$\pi_{\ell,m} = \sum_{\delta \in \Delta} (\delta X - 1)^{-m} (X^p - 1)^{\ell q/p} = \sum_{\delta \in \Delta} (\delta X - 1)^{-m} (X^p - 1)^{(\ell-1)q/p} (X^p - 1)^{q/p},$$

the lemma follows. □

We can repeatedly apply Lemma 5.2, reducing the first subindex by one and reducing the second subindex successively by t_1, t_2, …, t_ℓ. By setting s to be the number of these t_j's that are not equal to q we can write this reduction as in the following lemma.

LEMMA 5.3.

$$\pi_{n-d,m} = \sum_{s=0}^{n-d} \binom{n-d}{s} \sum_{t_1,\ldots,t_s \in \{1,\ldots,q-1\}} c_{t_1} \ldots c_{t_s} \pi_{0,m-(t_1+\ldots+t_s)-(n-d-s)q},$$

where

$$c_t = \sum_{i=\lceil t/p \rceil}^{q/p} \binom{q/p}{i} \binom{ip}{t} (-1)^{q/p-i}.$$

In general it seems difficult to calculate the exact number of times p divides c_t and so be able to apply Corollary 5.1. However, in the case $q = p$ this is easily done, since for $0 < t < q = p$,

$$c_t = \binom{p}{t}(-1)^{q/p-1}.$$

This is what we shall use in the following section.

6. Linear codes over a prime field

THEOREM 6.1. *Let C be a linear code of length n, dimension k, minimum distance d and maximum weight m over $\mathbb{F}_p$, where p is prime. Then*

$$m \leq (n-d)p - e(p-1),$$

where $e \in \{0, 1, \ldots, k-2\}$ is maximal with the property that

$$\binom{n-d}{e} \not\equiv 0 \pmod{p^{k-1-e}}.$$

Proof. By shortening the code C if necessary, which may possibly decrease $n - d$, we can suppose that $m = (n-d)p - e(p-1) + 1$.

If $m \leq n - d$ then, since $e \leq k - 2$, we have $n - d \geq (n-d)p - (k-2)(p-1) + 1$ and so $k - 1 > n - d$, which contradicts the Singleton bound [10]. Hence, in this case there is nothing to prove.

If $m \geq n - d + 1$ then by Corollary 5.1, for all $\epsilon \geq 1$ the coefficient of $X^{e(p-1)+\epsilon-1}$ in

$$(X-1)^{-m}(X^p-1)^{n-d},$$

is zero modulo p^{k-1}.

As mentioned before, the coefficient of X^{rp} in $\pi_{n-d,m}$ is p times the coefficient of X^{rp} in

$$(X-1)^{-m}(X^p-1)^{n-d},$$

for all $r \in \mathbb{N}$. Choose ϵ so that p divides $e(p-1)+\epsilon-1$ and note that the coefficient of $X^{e(p-1)+\epsilon-1}$ in $\pi_{n-d,m}$ is zero modulo p^k.

Consider the terms in the sum in Lemma 5.3.

If $m-(t_1+\cdots+t_s)-(n-d-s)p \leq 0$ then $\pi_{0,m-(t_1+\cdots+t_s)-(n-d-s)p}$ is a polynomial and moreover it is a polynomial of degree

$$e(p-1)-sp-1+\sum_{j=1}^{s} t_j \leq e(p-1)-s-1,$$

and so has no term of degree $e(p-1)+\epsilon-1$.

If $s \leq e-1$ then $m-(t_1+\cdots+t_s)-(n-d-s)p \leq 0$ and so $\pi_{0,m-(t_1+\cdots+t_s)-(n-d-s)p}$ has no term of degree $e(p-1)+\epsilon-1$.

If $s \geq e+1$ then since p divides c_{t_j} for all $j=1,\ldots,s$, $\binom{n-d}{s} \equiv 0 \bmod p^{k-1-s}$ by hypothesis, and all coefficients of $\pi_{0,m-(t_1+\cdots+t_s)-(n-d-s)p}$ are divisible by p, all terms in the sum in Lemma 5.3 are zero modulo p^k.

If $s=e$ and $m-(t_1+\cdots+t_s)-(n-d-s)p \geq 1$ then $-(t_1+\cdots+t_s)+s \geq 0$ and so $t_j=1$ for all $j=1,\ldots,s$.

Thus, the coefficient of $X^{e(p-1)-1+\epsilon}$ in $\pi_{n-d,m}$ is the coefficient of $X^{e(p-1)-1+\epsilon}$ in

$$\binom{n-d}{e} c_1^e \pi_{0,1},$$

and since $c_1=p$ and the coefficient of $X^{e(p-1)-1+\epsilon}$ in $\pi_{0,1}$ is $p(-1)^{e(p-1)-1+\epsilon}$, it is not zero modulo p^k, a contradiction. □

7. (n,r)-arcs and t-fold blocking sets of $\mathrm{AG}(s,q)$

An (n,t)-*arc* in $\mathrm{AG}(s,q)$ is a set S of points with the property that any hyperplane contains at most t points of S and some hyperplane contains exactly t points of S. Reversing the construction of Section 4, the code generated by the $(s+1)\times n$ matrix whose columns are the vectors in S and where the $(s+1)$-th row is the all one vector is linear code of length n, dimension $s+1$ and minimum distance at least $n-t$. Therefore, Corollary 5.1 has the following corollary.

Corollary 7.1. *If there is an (n,t)-arc in $AG(s,q)$, where $q=p^h$ and p is prime, then for all $\epsilon \geq 1$ the coefficient of $X^{tq-n+\epsilon}$ in*

$$(X-1)^{-n}(X^p-1)^{tq/p}$$

is divisible by q^{k-1}.

And Theorem 6.1 has the following corollary.

COROLLARY 7.2. *If there is an (n,t)-arc in $AG(s,p)$, where p is prime, then*

$$n \le (t-e)p + e,$$

where $e \in \{0,1,\ldots,s-1\}$ is maximal with the property that

$$\binom{t}{e} \not\equiv 0 \pmod{p^{s-e}}.$$

A *t-fold blocking set of hyperplanes* in $\mathrm{AG}(s,q)$ is a set B of points of $\mathrm{AG}(s,q)$ with the property that every hyperplane contains at least t points of B and some hyperplane contains exactly t points of B. The complement of B is a $(q^s-|B|, q^{s-1}-t)$-arc of $\mathrm{AG}(s,q)$. Hence, the above corollaries imply the following for t-fold blocking sets.

COROLLARY 7.3. *If B is a t-fold blocking set of $AG(s,q)$, where $q = p^h$ and p is prime, then for all $\epsilon \in \mathbb{N} = \{1,2,\ldots\}$ the coefficient of $X^{|B|-tq+\epsilon}$ in*

$$(X-1)^{|B|-q^s}(X^p-1)^{(q^{s-1}-t)q/p}$$

is divisible by q^s.

And in the case that q is prime we have the following corollary.

COROLLARY 7.4. *If B is a t-fold blocking set of $AG(s,p)$, where p is prime, then*

$$|B| \ge tp + e(p-1),$$

where $e \in \{0,1,\ldots,s-1\}$ is maximal with the property that

$$\binom{-t}{e} \not\equiv 0 \pmod{p^{s-e}}.$$

These bound should be compared with the following bounds.

The bound of Bruen [4]

$$|B| \ge (t+s-1)(q-1)+1,$$

is a general lower bound, which improves on the trivial $|B| \ge tq$ for $t \le (s-1)(q-1)$. This bound had been obtained previously for $t=1$ by Jamison [7] and Brouwer and Schrijver [3].

The bound from [1], which was proven there for $t < q$, states that

$$|B| \geq tq + (s-1)(q-1)$$

provided that

$$\binom{-s}{t-1} \not\equiv 0 \pmod{p}.$$

For many parameters Corollary 7.3 will allow one to calculate a better lower bound than these previously known bounds, as Corollary 7.4 indicates in the case q is prime. Indeed, for q prime the bound

$$|B| \geq tq + (s-1)(q-1)$$

extends to all t provided that

$$\binom{-t}{s-1} = (-1)^{s+t}\binom{-s}{t-1} \not\equiv 0 \pmod{p},$$

which improves on Bruen's bound by $t-1$.

8. Acknowledgement

We would like to thank the referee who made various suggestions and helpful comments, most of Section 2 is due to him/her.

References

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

[2] M. Braun, A. Kohnert and A. Wassermann, Construction of (n, r)-arcs in PG$(2, q)$, *Innov. Incidence Geom.*, **1** (2005) 133-141.

[3] A. E. Brouwer and A. Schrijver, The blocking number of an affine space, *J. Combin. Theory Ser. A*, **24** (1978) 251–253.

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

[5] Guava Manual, `http://www.math.rwth-aachen.de/~Greg.Gamble/gap4r3/pkg/guava/htm/CHAP005.htm`

[6] J. H. Griesmer, A bound for error-correcting codes, *IBM J. Res. Develop.*, **4** (1960) 532–542.

[7] R. Jamison, Covering finite fields with cosets of subspaces, *J. Combin. Theory Ser. A*, **22** (1977) 253–266.

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

[9] M. Plotkin, Binary codes with specified minimum distance, *IRE Transactions on Information Theory*, **6** 445–450 (1960).
[10] R.C. Singleton, Maximum distance q-nary codes, *IEEE Trans. Inf. Theory*, **10**, (1964), 116–118.
[11] J. H. van Lint, *An Introduction to Coding Theory*, Third edition, Springer-Verlag, 1998.

Simeon Ball
Departament de Matemàtica Aplicada IV,
Universitat Politècnica de Catalunya, Jordi Girona 1-3, Mòdul C3, Campus Nord,
08034 Barcelona, Spain
simeon@ma4.upc.edu

Aart Blokhuis
Department of Mathematics and Computing Science,
Eindhoven University of Technology, P.O. Box 513
5600MB Eindhoven, The Netherlands
aartb@win.tue.nl