An empty interval in the spectrum of small weight codewords in the code from points and k-spaces of $\mathrm{PG}(n, q)$

M. Lavrauw L. Storme P. Sziklai* G. Van de Voorde †

July 9, 2008

Abstract

Let $\mathrm{C}_k(n, q)$ be the p-ary linear code defined by the incidence matrix of points and k-spaces in $\mathrm{PG}(n, q)$, $q = p^h$, p prime, $h \geq 1$. In this paper, we show that there are no codewords of weight in $]\frac{q^{k+1}-1}{q-1}, 2q^k[$ in $\mathrm{C}_k(n, q) \setminus \mathrm{C}_{n-k}(n, q)^\perp$ which implies that there are no codewords with this weight in $\mathrm{C}_k(n, q) \setminus \mathrm{C}_k(n, q)^\perp$ if $k \geq n/2$. In particular, for the code $\mathrm{C}_{n-1}(n, q)$ of points and hyperplanes of $\mathrm{PG}(n, q)$, we exclude all codewords in $\mathrm{C}_{n-1}(n, q)$ with weight in $]\frac{q^n-1}{q-1}, 2q^{n-1}[$. This latter result implies a sharp bound on the weight of small weight codewords of $\mathrm{C}_{n-1}(n, q)$, a result which was previously only known for general dimension for q prime and $q = p^2$, with p prime, $p > 11$, and in the case $n = 2$, for $q = p^3$, $p \geq 7$.

1 Introduction

Let $\mathrm{PG}(n, q)$ denote the n-dimensional projective space over the finite field $\mathbb{F}_q$ with q elements, where $q = p^h$, p prime, $h \geq 1$, and let $\mathrm{V}(n + 1, q)$ denote the underlying vector space. Let θ_n denote the number of points in $\mathrm{PG}(n, q)$, i.e., $\theta_n = (q^{n+1} - 1)/(q - 1)$.

We define the incidence matrix $A = (a_{ij})$ of points and k-spaces in the projective space $\mathrm{PG}(n, q)$, $q = p^h$, p prime, $h \geq 1$, as the matrix whose rows are indexed by the k-spaces of $\mathrm{PG}(n, q)$ and whose columns are indexed by the points of $\mathrm{PG}(n, q)$, and with entry

$$a_{ij} = \begin{cases} 1 & \text{if point } j \text{ belongs to } k\text{-space } i, \\ 0 & \text{otherwise.} \end{cases}$$

The p-ary linear code of points and k-spaces of $\mathrm{PG}(n, q)$, $q = p^h$, p prime, $h \geq 1$, is the $\mathbb{F}_p$-span of the rows of the incidence matrix A. We denote this code by $\mathrm{C}_k(n, q)$. The *support* of a codeword c, denoted by *supp*(c), is the set of all non-zero positions of c. The *weight* of c is the number of non-zero positions of

*This author was partially supported by OTKA T-049662, T-067867 and Bolyai grants.

†This author's research was supported by the Institute for the Promotion of Innovation through Science and Technology in Flanders (IWT-Vlaanderen).

c and is denoted by $wt(c)$. Often we identify the support of a codeword with the corresponding set of points of $\mathrm{PG}(n,q)$. We let (c_1, c_2) denote the scalar product in $\mathbb{F}_p$ of two codewords c_1, c_2 of $\mathrm{C}_k(n,q)$. Furthermore, if T is a set of points of $\mathrm{PG}(n,q)$, then the incidence vector of this set is also denoted by T. The dual code $\mathrm{C}_k(n,q)^\perp$ is the set of all vectors orthogonal to all codewords of $\mathrm{C}_k(n,q)$, hence

$$\mathrm{C}_k(n,q)^\perp = \{v \in V(\theta_n, p) || (v,c) = 0,\ \forall c \in \mathrm{C}_k(n,q)\}.$$

It is easy to see that $c \in \mathrm{C}_k(n,q)^\perp$ if and only if $(c,K)=0$ for all k-spaces K of $\mathrm{PG}(n,q)$.

In [4] and [5], we excluded codewords of small weight in $\mathrm{C}_{n-1}(n,q)$, resp. $\mathrm{C}_k(n,q) \setminus \mathrm{C}_k(n,q)^\perp$, corresponding to linear small minimal blocking sets, which implied Result 1 and Result 2.

Result 1. [4] *The only possible codewords c of $\mathrm{C}_{n-1}(n,q)$ of weight in $]\theta_{n-1}, 2q^{n-1}[$ are the scalar multiples of non-linear minimal blocking sets, intersecting every line in* $1 \pmod p$ *points.*

Result 2. [5] *For $k \geq n/2$, the only possible codewords c of $\mathrm{C}_k(n,q)\setminus \mathrm{C}_k(n,q)^\perp$ of weight in $]\theta_k, 2q^k[$ are scalar multiples of non-linear minimal k-blocking sets of $\mathrm{PG}(n,q)$, intersecting every line in* $1 \pmod p$ *or zero points.*

Remark 3. *It is believed (and conjectured, see [7]) that all small minimal blocking sets are linear. If that conjecture is true, then Result 1 eliminates all possible codewords of $\mathrm{C}_{n-1}(n,q)$ of weight in $]\theta_{n-1}, 2q^{n-1}[$, and Result 2 eliminates all codewords of $\mathrm{C}_k(n,q) \setminus \mathrm{C}_k(n,q)^\perp$ of weight in $]\theta_k, 2q^k[$ if $k \geq n/2$.*

In this article, we improve on Result 1 and Result 2 by showing that there are no codewords in $\mathrm{C}_k(n,q) \setminus \mathrm{C}_{n-k}(n,q)^\perp$, $q=p^h$, p prime, $p>5$, $h \geq 1$, in the interval $]\theta_k, 2q^k[$, which implies that there are no codewords in the interval $]\theta_k, 2q^k[$ in $\mathrm{C}_k(n,q) \setminus \mathrm{C}_k(n,q)^\perp$ if $k \geq n/2$. Using the results of [5], we show that there are no codewords in $\mathrm{C}_k(n,q)$, $q=p^h$, p prime, $h \geq 1$, $p>7$, with weight in $]\theta_k, (12\theta_k+6)/7[$.

In the case that $k=n-1$, we show that there are no codewords in $\mathrm{C}_{n-1}(n,q)$ in the interval $]\theta_{n-1}, 2q^{n-1}[$. This interval is sharp: codewords of minimum weight in $\mathrm{C}_{n-1}(n,q)$ have been characterized as scalar multiples of incidence vectors of hyperplanes (see [1, Proposition 5.7.3]), and codewords of weight $2q^{n-1}$ can be obtained by taking the difference of the incidence vectors of two hyperplanes.

2 Blocking sets

A *blocking set* of $\mathrm{PG}(n,q)$ is a set K of points such that each hyperplane of $\mathrm{PG}(n,q)$ contains at least one point of K. A blocking set K is called *trivial* if it contains a line of $\mathrm{PG}(n,q)$. These blocking sets are also called 1*-blocking sets* in [2]. In general, a k*-blocking set* K in $\mathrm{PG}(n,q)$ is a set of points such that any $(n-k)$-dimensional subspace intersects K. A k-blocking set K is called *trivial* if there is a k-dimensional subspace contained in K. If an $(n-k)$-dimensional space contains exactly one point of a k-blocking set K in $\mathrm{PG}(n,q)$, it is called a *tangent* $(n-k)$*-space* to K, and a point P of K is called *essential* when it belongs to a tangent $(n-k)$-space of K. A k-blocking set K is called *minimal* when no proper subset of K is also a k-blocking set, i.e., when each point of K is essential. A k-blocking set is called *small* if it contains less than $3(q^k+1)/2$ points.

In order to define a *linear* k-blocking set, we introduce the notion of a Desarguesian spread.

By field reduction, the points of $\mathrm{PG}(n,q)$, $q=p^h$, p prime, $h \geq 1$, correspond to $(h-1)$-dimensional subspaces of $\mathrm{PG}((n+1)h-1,p)$, since a point of $\mathrm{PG}(n,q)$ is a 1-dimensional vector space over $\mathbb{F}_q$, and so an h-dimensional vector space over $\mathbb{F}_p$. In this way, we obtain a partition $\mathcal{D}$ of the point set of $\mathrm{PG}((n+1)h-1,p)$ by $(h-1)$-dimensional subspaces. In general, a partition of the point set of a projective space by subspaces of a given dimension k is called a *spread*, or a *k-spread* if we want to specify the dimension. The spread we have obtained here is called a *Desarguesian spread*. Note that the Desarguesian spread satisfies the property that each subspace spanned by two spread elements is again partitioned by spread elements. In fact, it can be shown that if $n \geq 2$, this property characterises a Desarguesian spread [6].

Definition 4. *Let U be a subset of $\mathrm{PG}((n+1)h-1,p)$ and let $\mathcal{D}$ be a Desarguesian $(h-1)$-spread of $\mathrm{PG}((n+1)h-1,p)$, then $\mathcal{B}(U)=\{R \in \mathcal{D} || U \cap R \neq \emptyset\}$.*

Analogously to the correspondence between the points of $\mathrm{PG}(n,q)$ and the elements of a Desarguesian spread $\mathcal{D}$ in $\mathrm{PG}((n+1)h-1,p)$, we obtain the correspondence between the lines of $\mathrm{PG}(n,q)$ and the $(2h-1)$-dimensional subspaces of $\mathrm{PG}((n+1)h-1,p)$ spanned by two elements of $\mathcal{D}$, and in general, we obtain the correspondence between the $(n-k)$-spaces of $\mathrm{PG}(n,q)$ and the $((n-k+1)h-1)$-dimensional subspaces of $\mathrm{PG}((n+1)h-1,p)$ spanned by $n-k+1$ elements of $\mathcal{D}$. With this in mind, it is clear that any hk-dimensional subspace U of $\mathrm{PG}(h(n+1)-1,p)$ defines a k-blocking set $\mathcal{B}(U)$ in $\mathrm{PG}(n,q)$. A blocking set constructed in this way is called a *linear k-blocking set.* Linear k-blocking sets were first introduced by Lunardon [6], although there a different approach is used. For more on the approach explained here, we refer to [3].

3 Results

In [8], Szőnyi and Weiner proved the following result on small blocking sets.

Result 5. *[8, Theorem 2.7] Let B be a minimal blocking set of $\mathrm{PG}(n,q)$ with respect to k-dimensional subspaces, $q=p^h$, $p>2$ prime, $h \geq 1$, and assume that $|B| < 3(q^{n-k}+1)/2$. Then any subspace that intersects B, intersects it in $1 \pmod p$ points.*

In [5], we proved the following lemmas.

Result 6. *The support of a codeword $c \in \mathrm{C}_k(n,q)$ with weight smaller than $2q^k$, for which $(c,S) \neq 0$ for some $(n-k)$-space S, is a minimal k-blocking set in $\mathrm{PG}(n,q)$. Moreover, c is a scalar multiple of a certain incidence vector, and supp(c) intersects every $(n-k)$-dimensional space in $1 \pmod p$ points.*

Lemma 7. *Let $c \in C_k(n,q)$, then there exists a constant $a \in \mathbb{F}_p$ such that $(c,U)=a$, for all subspaces U of dimension at least $n-k$.*

In the same way as the authors do in [5, Theorem 19], one can prove Lemma 8, which shows that all minimal k-blocking sets of size less than $2q^k$ and intersecting every $(n-k)$-space in $1 \pmod{p}$ points, are small.

Lemma 8. *Let B be a minimal k-blocking set in $\mathrm{PG}(n,q)$, $n \geq 2$, $q = p^h$, p prime, $p > 5$, $h \geq 1$, intersecting every $(n-k)$-dimensional space in $1 \pmod{p}$ points. If $|B| \in]\theta_k, 2q^k[$, then*

$$|B| < \frac{3(q^k - q^k/p)}{2}.$$

Lemma 9. *Let B_1 and B_2 be small minimal $(n-k)$-blocking sets in $\mathrm{PG}(n,q)$. Then $B_1 - B_2 \in \mathrm{C}_k(n,q)^\perp$.*

Proof. It follows from Result 5 that $(B_i, \pi_k) = 1$ for all k-spaces π_k, $i = 1, 2$. Hence $(B_1 - B_2, \pi_k) = 0$ for all k-spaces π_k. This implies that $B_1 - B_2 \in \mathrm{C}_k(n,q)^\perp$. □

Lemma 10. *Let c be a codeword of $\mathrm{C}_k(n,q)$ with weight smaller than $2q^k$, for which $(c,S) \neq 0$ for some $(n-k)$-space S, and let B be a small minimal $(n-k)$-blocking set. Then supp(c) intersects B in $1 \pmod{p}$ points.*

Proof. Let c be a codeword of $\mathrm{C}_k(n,q)$ with weight smaller than $2q^k$, for which $(c,S) \neq 0$ for some $(n-k)$-space S. Lemma 9 shows that $(c, B_1 - B_2) = 0 = (c, B_1) - (c, B_2)$ for all small minimal $(n-k)$-blocking sets B_1 and B_2. Hence (c, B), with B a small minimal $(n-k)$-blocking set, is a constant. Result 6 shows that c is a codeword only taking values from $\{0, a\}$, so $(c, B) = a(supp(c), B)$, hence $(supp(c), B)$ is a constant too. Let B_1 be an $(n-k)$-space, then Result 6 shows that $(supp(c), B_1) = 1$. Since B_1 is a small minimal $(n-k)$-blocking set, the number of intersection points of *supp*(c) and B is equal to $1 \pmod{p}$ for any small minimal blocking set B. □

It follows from Lemma 7 that, for $c \in \mathrm{C}_k(n,q)$ and S an $(n-k)$-space, (c,S) is a constant. Hence, either $(c,S) \neq 0$ for all $(n-k)$-spaces S, or $(c,S) = 0$ for all $(n-k)$-spaces S. In this latter case, $c \in \mathrm{C}_{n-k}(n,q)^\perp$.

Theorem 11. *There are no codewords in $\mathrm{C}_k(n,q) \setminus \mathrm{C}_{n-k}(n,q)^\perp$ with weight in $]\theta_k, 2q^k[$, $q = p^h$, p prime, $p > 5$, $h \geq 1$.*

Proof. Let Y be a linear small minimal $(n-k)$-blocking set in $\mathrm{PG}(n,q)$. As explained in Section 2, Y corresponds to a set $\bar{Y} = \mathcal{B}(\pi)$ of $(h-1)$-dimensional spread elements intersecting a certain $(h(n-k))$-space π in $\mathrm{PG}(h(n+1)-1,p)$. Let c be a codeword of $\mathrm{C}_k(n,q) \setminus \mathrm{C}_{n-k}(n,q)^\perp$ with weight at most $2q^k - 1$. Result 6 and Lemma 8 show that *supp*(c) is a small minimal k-blocking set B. This blocking set B corresponds to a set $\bar{B}$ of $|B|$ spread elements in $\mathrm{PG}(h(n+1)-1,p)$. Since *supp*(c) and Y intersect in $1 \pmod{p}$ points (see Lemma 10), $\bar{B}$ and $\bar{Y}$ intersect in $1 \pmod{p}$ spread elements. Since all spread elements of $\bar{Y}$ intersect π, there are $1 \pmod{p}$ spread elements of $\bar{B}$ that intersect π.

But this holds for any $(h(n-k))$-space π' in $\mathrm{PG}(h(n+1)-1,p)$, since any $(h(n-k))$-space π' corresponds to a linear small minimal $(n-k)$-blocking set Y' in $\mathrm{PG}(n,q)$.

Let $\tilde{B}$ be the set of points contained in the spread elements of the set $\bar{B}$. Since a spread element that intersects a subspace of $\mathrm{PG}(h(n+1)-1,p)$ intersects it in 1 (mod p) points, $\tilde{B}$ intersects any $(h(n-k))$-space in 1 (mod p) points. Moreover, $|\tilde{B}| = |B| \cdot (p^h - 1)/(p-1) \leq 3(p^{hk} - p^{hk-1}) \cdot (p^h - 1)/(2(p-1)) < 3(p^{h(k+1)-1} + 1)/2$ (see Lemma 8). This implies that $\tilde{B}$ is a small $(h(k+1)-1)$-blocking set in $\mathrm{PG}(h(n+1)-1, p)$.

Moreover, $\tilde{B}$ is minimal. This can be proven in the following way. Let R be a point of $\tilde{B}$. Since B is a minimal k-blocking set in $\mathrm{PG}(n,q)$, there is a tangent $(n-k)$-space S through the point R' of $\mathrm{PG}(n,q)$ corresponding to the spread element $\mathcal{B}(R)$. Now S corresponds to an $(h(n-k+1)-1)$-space π' in $\mathrm{PG}(h(n+1)-1, p)$, such that $\mathcal{B}(R)$ is the only element of $\bar{B}$ in π'. This implies that through R, there is an $(h(n-k))$-space in π' containing only the point R of $\tilde{B}$. This shows that through every point of $\tilde{B}$, there is a tangent $(h(n-k))$-space, hence that $\tilde{B}$ is a minimal $(h(k+1)-1)$-blocking set.

Result 5 implies that $\tilde{B}$ intersects any subspace of $\mathrm{PG}(h(n+1)-1, p)$ in zero or 1 (mod p) points. This implies that a line is skew, tangent or entirely contained in $\tilde{B}$, hence $\tilde{B}$ is a subspace of $\mathrm{PG}(h(n+1)-1, p)$, with at most $3(p^{h(k+1)-1} + 1)/2$ points, intersecting every $(h(n-k))$-space. Moreover, it is the point set of a set of $|B|$ spread elements. Hence, $\bar{B}$ is the set of spread elements corresponding to a k-space in $\mathrm{PG}(n,q)$, so *supp*(c) has size θ_k. □

In [5], we determined a lower bound on the weight of the code $\mathrm{C}_k(n,q)^{\perp}$.

Result 12. *The minimum weight of* $\mathrm{C}_k(n,q)^{\perp}$ *is at least* $(12\theta_{n-k} + 2)/7$ *if* $p = 7$*, and at least* $(12\theta_{n-k} + 6)/7$ *if* $p > 7$.

Theorem 13. *There are no codewords in* $\mathrm{C}_k(n,q)$ *with weight in* $]\theta_k, (12\theta_k + 2)/7[$ *if* $p = 7$ *and there are no codewords in* $\mathrm{C}_k(n,q)$ *with weight in* $]\theta_k, (12\theta_k + 6)/7[$ *if* $p > 7$.

Proof. This follows immediately from Theorem 11 and Result 12. □

In [5], we proved the following result.

Result 14. *Assume that* $k \geq n/2$*. A codeword* c *of* $\mathrm{C}_k(n,q)$ *is in* $\mathrm{C}_k(n,q) \cap \mathrm{C}_k(n,q)^{\perp}$ *if and only if* $(c, U) = 0$ *for all subspaces* U *with* $\dim(U) \geq n-k$.

Corollary 15. *If* $k \geq n/2$*,* $\mathrm{C}_k(n,q) \setminus \mathrm{C}_{n-k}(n,q)^{\perp} = \mathrm{C}_k(n,q) \setminus \mathrm{C}_k(n,q)^{\perp}$.

Proof. It follows from Result 14 that $\mathrm{C}_k(n,q) \cap \mathrm{C}_{n-k}(n,q)^{\perp} = \mathrm{C}_k(n,q) \cap \mathrm{C}_k(n,q)^{\perp}$ if $k \geq n/2$. □

In [4], we proved the following result.

Result 16. *The minimum weight of* $\mathrm{C}_{n-1}(n,q) \cap \mathrm{C}_{n-1}(n,q)^{\perp}$ *is equal to* $2q^{n-1}$.

Theorem 11, Corollary 15, and Result 16 yield the following corollary, which gives a sharp empty interval on the size of small weight codewords of $\mathrm{C}_{n-1}(n,q)$, since θ_{n-1} is the weight of a codeword arising from the incidence vector of an $(n-1)$-space and $2q^{n-1}$ is the weight of a codeword arising from the difference of the incidence vectors of two $(n-1)$-spaces.

Corollary 17. *There are no codewords with weight in* $]\theta_{n-1}, 2q^{n-1}[$ *in the code* $\mathrm{C}_{n-1}(n,q)$.

In the planar case, this yields the following corollary, which improves on the results in [1].

Corollary 18. *There are no codewords with weight in* $]q+1, 2q[$ *in the code of points and lines of* $\mathrm{PG}(2,q)$.

In this case, the weight $q+1$ corresponds to the incidence vector of a line, and the weight $2q$ can be obtained by taking the difference of the incidence vectors of two different lines.

References

[1] E.F. Assmus, Jr. and J.D. Key. Designs and their codes. *Cambridge University Press*, 1992.

[2] A. Beutelspacher. Blocking sets and partial spreads in finite projective spaces. *Geom. Dedicata* **9** (1980), 130–157.

[3] M. Lavrauw. Scattered spaces with respect to spreads, and eggs in finite projective spaces. PhD Dissertation, Eindhoven University of Technology, Eindhoven, 2001. viii+115 pp.

[4] M. Lavrauw, L. Storme and G. Van de Voorde. On the code generated by the incidence matrix of points and hyperplanes in $\mathrm{PG}(n,q)$ and its dual. *Des. Codes Cryptogr.*, to appear.

[5] M. Lavrauw, L. Storme and G. Van de Voorde. On the code generated by the incidence matrix of points and k-spaces in $\mathrm{PG}(n,q)$ and its dual. *Finite Fields Appl.*, to appear.

[6] G. Lunardon. Normal spreads. *Geom. Dedicata* **75** (1999), 245–261.

[7] P. Sziklai. On small blocking sets and their linearity. *J. Combin. Theory, Ser. A*, to appear.

[8] T. Szőnyi and Zs. Weiner. Small blocking sets in higher dimensions. *J. Combin. Theory Ser. A* **95** (2001), no. 1, 88–101.

Address of the authors:

Michel Lavrauw, Leo Storme, Geertrui Van de Voorde:
Department of pure mathematics and computer algebra,
Ghent University
Krijgslaan 281-S22
9000 Ghent (Belgium)
{ml,ls,gvdvoorde}@cage.ugent.be
http://cage.ugent.be/ ∼ {ml,ls,gvdvoorde}

Peter Sziklai:
Department of Computer Science,
Eötvös Loránd University
Pázmány P. sétány 1/C
H-1117 Budapest (Hungary)
sziklai@cs.elte.hu
http://www.cs.elte.hu/∼sziklai