

Contents lists available at ScienceDirect

Journal of Combinatorial Theory, Series A

www.elsevier.com/locate/jcta



Note

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

Michel Lavrauw a,1, Leo Storme a, Peter Sziklai b,2, Geertrui Van de Voorde a,3

ARTICLE INFO

Article history: Received 9 July 2008 Available online 29 January 2009

Keywords:
Projective spaces
Linear Codes
Blocking sets
Small weight codewords

ABSTRACT

Let $C_k(n,q)$ be the p-ary linear code defined by the incidence matrix of points and k-spaces in PG(n,q), $q=p^h$, p prime, $h \geqslant 1$. In this paper, we show that there are no codewords of weight in the open interval $]\frac{q^{k+1}-1}{q-1}, 2q^k[$ in $C_k(n,q) \setminus C_{n-k}(n,q)^{\perp}$ which implies that there are no codewords with this weight in $C_k(n,q) \setminus C_k(n,q)^{\perp}$ if $k \ge n/2$. In particular, for the code $C_{n-1}(n,q)$ of points and hyperplanes of PG(n,q), we exclude all codewords in $C_{n-1}(n,q)$ with weight in the open interval $]\frac{q^n-1}{q-1}, 2q^{n-1}[$. This latter result implies a sharp bound on the weight of small weight codewords of $C_{n-1}(n,q)$, 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 $q = p^3$, $p \ge 7$ [K. Chouinard, On weight distributions of codes of planes of order 9, Ars Combin. 63 (2002) 3-13; V. Fack, Sz.L. Fancsali, L. Storme, G. Van de Voorde, J. Winne, Small weight codewords in the codes arising from Desarguesian projective planes, Des. Codes Cryptogr. 46 (2008) 25-43; M. Lavrauw, L. Storme, G. Van de Voorde, On the code generated by the incidence matrix of points and hyperplanes in PG(n,q) and its dual, Des. Codes Cryptogr. 48 (2008) 231–245; M. Lavrauw, L. Storme, G. Van de Voorde, On the code generated

^a Department of Pure Mathematics and Computer Algebra, Ghent University, Krijgslaan 281-S22, 9000 Ghent, Belgium

b Department of Computer Science, Eötvös Loránd University, Pázmány P. sétány 1/C, H-1117 Budapest, Hungary

E-mail addresses: ml@cage.ugent.be (M. Lavrauw), ls@cage.ugent.be (L. Storme), sziklai@cs.elte.hu (P. Sziklai), gvdvoorde@cage.ugent.be (G. Van de Voorde).

URLs: http://cage.ugent.be/~ml (M. Lavrauw), http://cage.ugent.be/~ls (L. Storme), http://www.cs.elte.hu/~sziklai (P. Sziklai), http://cage.ugent.be/~gvdvoorde (G. Van de Voorde).

¹ The research was supported by the Fund for Scientific Research, Flanders (FWO, Vlaanderen).

² Partially supported by OTKA T-049662, T-067867 and Bolyai grants.

³ The research was supported by the Institute for the Promotion of Innovation through Science and Technology in Flanders (IWT-Vlaanderen) and the Fund for Scientific Research, Flanders (FWO, Vlaanderen).

by the incidence matrix of points and k-spaces in PG(n, q) and its dual, Finite Fields Appl. 14 (2008) 1020–1038].

© 2009 Elsevier Inc. All rights reserved.

1. Definitions

Let 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, $h\geqslant 1$, and let V(n+1,q) denote the underlying vector space. Let θ_n denote the number of points in 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 PG(n, q), $q = p^h$, p prime, $h \ge 1$, as the matrix whose rows are indexed by the k-spaces of PG(n, q) and whose columns are indexed by the points of 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 PG(n,q), $q=p^h$, p prime, $h\geqslant 1$, is the \mathbb{F}_p -span of the rows of the incidence matrix A. We denote this code by $C_k(n,q)$. The support of a codeword c, denoted by supp(c), is the set of all non-zero positions of c. The support of a codeword with the corresponding set of points of 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 $C_k(n,q)$. Furthermore, if T is a set of points of PG(n,q), then the incidence vector of this set is also denoted by T. The dual code $C_k(n,q)^\perp$ is the set of all vectors orthogonal to all codewords of $C_k(n,q)$, hence

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

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

2. Previous results

The p-ary linear code of points and lines of PG(2,q), $q=p^h$, p prime, $h\geqslant 1$, is studied in [1, Chapter 6]. In [1, Proposition 5.7.3], the codewords of minimum weight of the code of points and hyperplanes of PG(n,q), $q=p^h$, p prime, $h\geqslant 1$, are determined. The first results on codewords of small weight in the p-ary linear code of points and lines in PG(2,p), p prime, were proved by McGuire and Ward [10], where they proved that there are no codewords of $C_1(2,p)$, p an odd prime, in the interval [p+2,3(p+1)/2]. This result was extended by Chouinard (see [3,4]) where he proves the following result.

Result 1. (See [3,4].) In the p-ary linear code arising from PG(2, p), p prime, there are no codewords with weight in the closed interval [p+2, 2p-1].

This result shows that there is a gap in the weight enumerator of the code $C_1(2, p)$ of points and lines in PG(2, p), p prime. In Corollary 21, Result 1 is extended to the code of points and k-spaces in PG(n, p), p prime, p > 5.

In the case where q is not a prime, we improve on results of [5,7,8], where the authors exclude codewords of small weight in $C_{n-1}(n,q)$, $q=p^h$, p prime, $h\geqslant 1$, respectively $C_k(n,q)\setminus C_k(n,q)^\perp$, $q=p^h$, p prime, $h\geqslant 1$, corresponding to linear small minimal blocking sets, which implied Results 2 and 3. For the definition of a blocking set, see the next section.

Result 2. (See [7, Corollary 3].) The only possible codewords c of $C_{n-1}(n,q)$, $q=p^h$, p prime, $h \ge 1$, of weight in the open interval $]\theta_{n-1}, 2q^{n-1}[$ are the scalar multiples of non-linear minimal blocking sets, intersecting every line in 1 (mod p) points.

Result 3. (See [8, Corollary 2].) For $k \ge n/2$, the only possible codewords c of $C_k(n,q) \setminus C_k(n,q)^{\perp}$, $q = p^h$, p prime, $h \ge 1$, of weight in the open interval $]\theta_k$, $2q^k[$ are scalar multiples of non-linear minimal k-blocking sets of PG(n,q), intersecting every line in 1 (mod p) or zero points.

Remark 4. It is believed (and conjectured, see [11, Conjecture 3.1]) that all small minimal blocking sets are linear. If that conjecture is true, then Result 2 eliminates all possible codewords of $C_{n-1}(n,q)$, $q=p^h$, p prime, $h\geqslant 1$, of weight in the open interval $]\theta_{n-1}, 2q^{n-1}[$, and Result 3 eliminates all codewords of $C_k(n,q)\setminus C_k(n,q)^{\perp}$, $q=p^h$, p prime, $h\geqslant 1$, of weight in the open interval $]\theta_k, 2q^k[$ if $k\geqslant n/2$.

In this article, we avoid the obstacle of this non-solved conjecture and improve on Results 2 and 3 by showing that there are no codewords in $C_k(n,q) \setminus C_{n-k}(n,q)^{\perp}$, $q=p^h$, p prime, p>5, $h\geqslant 1$, in the open interval $]\theta_k, 2q^k[$, which implies that there are no codewords in the open interval $]\theta_k, 2q^k[$ in $C_k(n,q) \setminus C_k(n,q)^{\perp}$ if $k\geqslant n/2$. Using the results of [8], we show that there are no codewords in $C_k(n,q)$, $q=p^h$, p prime, $h\geqslant 1$, p>7, with weight in the open interval $]\theta_k, (12\theta_k+6)/7[$.

In the case that k = n - 1, we show that there are no codewords in $C_{n-1}(n,q)$, $q = p^h$, p prime, $h \ge 1$, in the open interval $]\theta_{n-1}, 2q^{n-1}[$. These bounds are sharp: codewords of minimum weight in $C_{n-1}(n,q)$ 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.

3. Blocking sets

A blocking set of PG(n,q) is a set K of points such that each hyperplane of PG(n,q) contains at least one point of K. A blocking set K is called *trivial* if it contains a line of PG(n,q). These blocking sets are also called 1-blocking sets in [2]. In general, a k-blocking set K in 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 PG(n,q), it is called a *tangent* (n-k)-space to K, and a point K 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 PG(n,q), $q=p^h$, p prime, $h\geqslant 1$, correspond to (h-1)-dimensional subspaces of PG((n+1)h-1,p), since a point of 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 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.

Definition 5. Let \mathcal{D} be a Desarguesian (h-1)-spread of PG((n+1)h-1, p) as defined above. If U is a subset of PG((n+1)h-1, p), then we write $\mathcal{B}(U) = \{R \in \mathcal{D} \mid U \cap R \neq \emptyset\}$.

In analogy with the correspondence between the points of PG(n,q) and the elements of a Desarguesian spread \mathcal{D} in PG((n+1)h-1,p), we obtain the correspondence between the lines of PG(n,q) and the (2h-1)-dimensional subspaces of 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 PG(n,q) and the ((n-k+1)h-1)-dimensional subspaces of 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 PG(h(n+1)-1,p) defines a k-blocking set $\mathcal{B}(U)$ in 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 [9, Section 5], although there a different approach is used. For more on the approach explained here, we refer to [6, Chapter 1].

4. Results

In [12], Szőnyi and Weiner proved the following result on small blocking sets.

Result 6. (See [12, Theorem 2.7].) Let B be a minimal blocking set of PG(n, q) with respect to k-dimensional subspaces, $q = p^h$, p > 2 prime, $h \ge 1$, and assume that $|B| < 3(q^{n-k} + 1)/2$. Then any subspace that intersects B, intersects it in 1 (mod p) points.

In [8], Lavrauw et al. proved the following results.

Result 7. The support of a codeword $c \in C_k(n,q)$, $q = p^h$, p prime, $h \ge 1$, with weight smaller than $2q^k$, for which $(c,S) \ne 0$ for some (n-k)-space S, is a minimal k-blocking set in PG(n,q). Moreover, c is a scalar multiple of a certain incidence vector, and Supp(c) intersects every (n-k)-dimensional space in Supp(c) points.

Lemma 8. Let $c \in C_k(n, q)$, $q = p^h$, p prime, $h \ge 1$, 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 is done by the authors in [8, Theorem 19], one can prove Lemma 9, which shows that all minimal k-blocking sets of size less than $2q^k$ and intersecting every (n-k)-space in 1 (mod p) points, are small.

Lemma 9. Let B be a minimal k-blocking set in PG(n, q), $n \ge 2$, $q = p^h$, p prime, p > 5, $h \ge 1$, intersecting every (n - k)-dimensional space in 1 (mod p) points. If $|B| \in]\theta_k, 2q^k[$, then

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

Lemma 10. Let B_1 and B_2 be small minimal (n-k)-blocking sets in PG(n,q), $q=p^h$, p prime, $h \ge 1$. Then $B_1 - B_2 \in C_k(n,q)^{\perp}$.

Proof. It follows from Result 6 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 $B_1 - B_2 \in C_k(n, q)^{\perp}$. \square

Lemma 11. Let c be a codeword of $C_k(n,q)$, $q=p^h$, p prime, $h \ge 1$, with weight smaller than $2q^k$, for which $(c,S) \ne 0$ for some (n-k)-space S, and let B be a small minimal (n-k)-blocking set. Then supp(c) intersects B in D (mod D) points.

Proof. Let c be a codeword of $C_k(n,q)$ with weight smaller than $2q^k$, for which $(c,S) \neq 0$ for some (n-k)-space S. Lemma 10 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 7 shows that c is a codeword only taking values from $\{0,a\}$, so $(c,B)=a(\sup(c),B)$, hence $(\sup(c),B)$ is a constant too. Let B_1 be an (n-k)-space, then Result 7 shows that $(\sup(c),B_1)=1$. Since B_1 is a small minimal (n-k)-blocking set, the number of intersection points of (x) and (x) is equal to 1 (x) for any small minimal blocking set (x).

It follows from Lemma 8 that, for $c \in C_k(n,q)$ 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, $c \in C_{n-k}(n,q)^{\perp}$.

Theorem 12. There are no codewords in $C_k(n,q) \setminus C_{n-k}(n,q)^{\perp}$, $1 \le k \le n-1$, $2 \le n$, with weight in the open interval $]\theta_k, 2q^k[$, $q = p^h$, p prime, p > 5, $h \ge 1$.

Proof. Let Y be a linear small minimal (n-k)-blocking set in PG(n,q). As explained in Section 3, 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 PG(h(n+1)-1,p). Let c be a codeword of $C_k(n,q) \setminus C_{n-k}(n,q)^\perp$ with weight at most $2q^k-1$. Result 7 and Lemma 9 show that $\sup(c)$ is a small minimal k-blocking set p. This blocking set p corresponds to a set p of p spread elements in p of p intersect in 1 (mod p) points (see Lemma 11), p and p intersect in 1 (mod p) spread elements. Since all spread elements of p intersect p, there are 1 (mod p) spread elements of p that intersect p.

But this holds for any (h(n-k))-space π' in 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 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 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, $|\tilde{B}| = |B| \cdot (p^h - 1)/(p-1) \le 3(p^{hk} - p^{hk-1}) \cdot (p^h - 1)/(2(p-1)) < 3(p^{h(k+1)-1} + 1)/2$ (see Lemma 9). This implies that \tilde{B} is a small (h(k+1)-1)-blocking set in PG(h(n+1)-1,p).

Moreover, \tilde{B} is minimal. This can be proved in the following way. Let R be a point of \tilde{B} . Since B is a minimal k-blocking set in PG(n,q), there is a tangent (n-k)-space S through the point R' of PG(n,q) corresponding to the spread element $\mathcal{B}(R)$. Now S corresponds to an (h(n-k+1)-1)-space π' in PG(h(n+1)-1,p), such that $\mathcal{B}(R)$ is the only element of \tilde{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 6 implies that \tilde{B} intersects any subspace of PG(h(n+1)-1, p) in 1 (mod p) or zero points. This implies that a line is skew, tangent or entirely contained in \tilde{B} , hence \tilde{B} is a subspace of 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, \tilde{B} is the set of spread elements corresponding to a k-space in PG(n,q), so supp(c) has size θ_k . \square

In [8], Lavrauw et al. determined a lower bound on the weight of the code $C_k(n,q)^{\perp}$.

Result 13. The minimum weight of $C_k(n,q)^{\perp}$, $q=p^h$, p prime, $h \ge 1$, $2 \le n$, $1 \le k \le n-1$, 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 14. For $q = p^h$, p prime, $h \ge 1$, $2 \le n$, $1 \le k \le n-1$, there are no codewords in $C_k(n,q)$ with weight in the open interval $]\theta_k$, $(12\theta_k + 2)/7[$ if p = 7 and there are no codewords in $C_k(n,q)$ with weight in the open interval $]\theta_k$, $(12\theta_k + 6)/7[$ if p > 7.

Proof. This follows immediately from Theorem 12 and Result 13. \Box

In [8], the authors proved the following result.

Result 15. (See [8, Lemma 3].) Assume that $k \ge n/2$. A codeword c of $C_k(n,q)$ is in $C_k(n,q) \cap C_k(n,q)^{\perp}$ if and only if (c,U) = 0 for all subspaces U with $\dim(U) \ge n - k$.

Corollary 16. If $k \ge n/2$, $C_k(n,q) \setminus C_{n-k}(n,q)^{\perp} = C_k(n,q) \setminus C_k(n,q)^{\perp}$, $q = p^h$, p prime, $h \ge 1$.

Proof. It follows from Result 15 that $C_k(n,q) \cap C_{n-k}(n,q)^{\perp} = C_k(n,q) \cap C_k(n,q)^{\perp}$ if $k \ge n/2$. \square

In [7], the authors proved the following result.

Result 17. (See [7, Theorem 5].) The minimum weight of $C_{n-1}(n,q) \cap C_{n-1}(n,q)^{\perp}$ is equal to $2q^{n-1}$.

Result 18. (See [8, Theorem 12].) The minimum weight of $C_k(n, p)^{\perp}$, where p is a prime, is equal to $2p^{n-k}$, and the codewords of weight $2p^{n-k}$ are the scalar multiples of the difference of two (n-k)-spaces intersecting in an (n-k-1)-space.

Theorem 12, Corollary 16, and Result 17 yield the following corollary, which gives a sharp empty interval on the size of small weight codewords of $C_{n-1}(n,q)$, 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 19. There are no codewords with weight in the open interval $]\theta_{n-1}, 2q^{n-1}[$ in the code $C_{n-1}(n, q), q = p^h, p$ prime, $h \ge 1, p > 5$.

In the planar case, this yields the following corollary, which improves on the result of Chouinard mentioned in Result 1.

Corollary 20. There are no codewords with weight in the open interval]q + 1, 2q[in the p-ary linear code of points and lines of PG(2, q), $q = p^h$, p prime, $h \ge 1$, p > 5.

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.

Theorem 12 and Result 18 yield the following corollary, extending the result of Chouinard mentioned in Result 1 to general dimension.

Corollary 21. There are no codewords with weight in the open interval $]\theta_k, 2q^k[$ in the code $C_k(n, q), n \ge 2, 1 \le k \le n - 1, q$ prime, q > 5.

References

- [1] E.F. Assmus Jr., J.D. Key, Designs and Their Codes, Cambridge Univ. Press, 1992.
- [2] A. Beutelspacher, Blocking sets and partial spreads in finite projective spaces, Geom. Dedicata 9 (1980) 130-157.
- [3] K. Chouinard, Weight distributions of codes from planes, PhD thesis, University of Virginia, August 1998.
- [4] K. Chouinard, On weight distributions of codes of planes of order 9, Ars Combin. 63 (2002) 3-13.
- [5] V. Fack, Sz.L. Fancsali, L. Storme, G. Van de Voorde, J. Winne, Small weight codewords in the codes arising from Desarguesian projective planes, Des. Codes Cryptogr. 46 (2008) 25–43.
- [6] M. Lavrauw, Scattered spaces with respect to spreads, and eggs in finite projective spaces, PhD dissertation, Eindhoven Univ. of Technology, Eindhoven, 2001, viii+115 pp.
- [7] M. Lavrauw, L. Storme, G. Van de Voorde, On the code generated by the incidence matrix of points and hyperplanes in PG(n,q) and its dual, Des. Codes Cryptogr. 48 (2008) 231–245.
- [8] M. Lavrauw, L. Storme, G. Van de Voorde, On the code generated by the incidence matrix of points and k-spaces in PG(n, q) and its dual, Finite Fields Appl. 14 (2008) 1020–1038.
- [9] G. Lunardon, Normal spreads, Geom. Dedicata 75 (1999) 245-261.
- [10] G. McGuire, H. Ward, The weight enumerator of the code of the projective plane of order 5, Geom. Dedicata 73 (1) (1998) 63–77.
- [11] P. Sziklai, On small blocking sets and their linearity, J. Combin. Theory Ser. A 115 (7) (2008) 1167-1182.
- [12] T. Szőnyi, Zs. Weiner, Small blocking sets in higher dimensions, J. Combin. Theory Ser. A 95 (2001) 88–101.