On the (dual) code generated by the incidence matrix of points and hyperplanes in $PG(n, q)$

M. Lavrauw L. Storme G. Van de Voorde [*]

September 3, 2007

Abstract

In this paper, we study the p-ary linear code $C(PG(n, q))$, $q = p^h$, p prime, $h \geq 1$, generated by the incidence matrix of points and hyperplanes of a Desarguesian projective space $PG(n, q)$, and its dual code. We link the codewords of small weight of this code to blocking sets with respect to lines in $PG(n, q)$ and we exclude all possible codewords arising from small linear blocking sets.

We also look at the dual code of $C(PG(n, q))$ and we prove that finding the minimum weight of the dual code can be reduced to finding the minimum weight of the dual code of points and lines in $PG(2, q)$. We present an improved upper bound on this minimum weight and we show that we can drop the divisibility condition on the weight of the codewords in Sachar's lower bound [11].

1 Introduction

In this paper, we denote the n-dimensional projective space over the finite field of order q, where $q = p^h$, p prime, $h \geq 1$, by $PG(n, q)$. Let θ_n denote the number of points in $PG(n, q)$, i.e., $\theta_n = (q^{n+1} - 1)/(q - 1)$, and let $V(n + 1, q)$ denote the underlying vector space.

This research is a natural extension of the results on the p-ary linear code generated by points and lines of a projective plane $PG(2, q)$, with $q = p^h$, p prime, $h \geq 1$. The minimum weight and the nature of the minimum weight codewords of the p-ary linear codes generated by the incidence matrix of points and lines of projective planes, have been established in the 1960s, after Prange [9] and Rudolph [10] recognized that projective planes could be used to produce error-correcting codes. The codewords of minimal weight are the scalar multiples of the incidence vectors of the lines of $PG(2, q)$ [1, Theorem 6.3.1]. In [4], Chouinard investigates the codewords of small weight in this code. In particular, when q is prime, the following result is proven.

Theorem 1. *[4] (1) In the p-ary linear code arising from $PG(2, p)$, p prime, there are no codewords with weight in $[p + 2, 2p - 1]$.*

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

(2) The codewords of weight $2p$ in the p-ary linear code arising from $PG(2,p)$, p prime, are the scalar multiples of the differences of the incidence vectors of two lines of $PG(2,p)$.

In [5], this result was extended to codewords of larger weight in the following theorem.

Theorem 2. *[5] The only codewords c, with $0 < wt(c) \leq 2p + (p-1)/2$, in the p-ary linear code C arising from $PG(2,p)$, p prime, $p \geq 11$, are:*

- *codewords with weight $p+1$: the scalar multiples of the incidence vectors of the lines of $PG(2,p)$,*
- *codewords with weight $2p$: $\alpha(c_1 - c_2)$, c_1 and c_2 the incidence vectors of two distinct lines of $PG(2,p)$,*
- *codewords with weight $2p+1$: $\alpha c_1 + \beta c_2$, $\beta \neq -\alpha$, with c_1 and c_2 the incidence vectors of two distinct lines of $PG(2,p)$.*

Moreover, in [5], the first part of Theorem 1 was extended to $\mathbb{F}_{p^3}$.

Theorem 3. *[5] In the p-ary linear code of $PG(2,p^3)$, p prime, $p \geq 7$, there are no codewords with weight in the interval $[p^3+2, 2p^3-1]$.*

Remark 1. *The same result holds for $\mathbb{F}_{p^2}$, p prime, which can be deduced easily in the same way as the authors do in [5].*

Namely, it is known that a codeword of weight in $]p^2+1, 2p^2[$ in the p-ary linear code of $PG(2,p^2)$, p prime, is a scalar multiple of the incidence vector of a non-trivial minimal blocking set in $PG(2,p^2)$, p prime, intersecting every line in $1 \pmod p$ points [4], [5, Lemma 1]. The only such non-trivial minimal blocking sets are the Baer subplanes [14], but these are not codewords in the p-ary linear code of $PG(2,p^2)$ [1, Proposition 6.6.3].

Hence, we obtain the following result.

Theorem 4. *The p-ary linear code of $PG(2,p^2)$, p prime, does not have codewords with weight in $[p^2+2, 2p^2-1]$.*

Goal of the first section of this paper is to prove similar results for general dimension n and field order q.

We know that the smallest weight codewords in the p-ary linear code defined by the incidence matrix of points and hyperplanes of $PG(n,q)$, $q = p^h$, p prime, $h \geq 1$, are the scalar multiples of the incidence vectors of the hyperplanes of $PG(n,q)$ [1, Proposition 5.7.3]. We will study codewords of weight in $]\theta_{n-1}, 2q^{n-1}[$, and show that there is a gap in the weight enumerator of this code by excluding as many weights as possible in this interval. More precisely, we will show that there are no codewords with weight between the weight of a hyperplane and the symmetric difference of two hyperplanes for $q = p$ and $q = p^2$, $p > 11$, p prime. Corollary 4 proves the analogous statement of Theorem 1 (1) for general dimension. Extending the theorem for codes $C(PG(n,q))$, over an arbitrary finite field $\mathbb{F}_q$, is harder. Here we show that a codeword of weight in $]\theta_{n-1}, 2q^{n-1}[$ corresponds to a minimal blocking set in $PG(n,q)$, and we exclude all small linear blocking sets as codewords. We also prove that the weights of the codewords of weight in $]\theta_{n-1}, 2q^{n-1}[$ can only lie in a number of small intervals, and that there are no codewords with weight in $[3q^{n-1}/2, 2q^{n-1}[$. In this way, half of the interval is eliminated. If q is the square of a prime, this proves the statement of Remark 1 and Theorem 4 in general dimension.

The situation regarding the dual of the code generated by the incidence matrix of points and lines in $PG(2, q)$ is different. In this case, the minimum weight of the dual code is not known in general, although some bounds are given (see Assmus and Key [1] and Sachar [11]). We extend these results to general dimension by proving that the minimum weight of the dual code generated by the incidence matrix of points and hyperplanes in $PG(n, q)$ is equal to the minimum weight of the dual code generated by the incidence matrix of points and lines in $PG(2, q)$. Moreover, we present an improved upper bound on this minimum weight and we show that we can drop the divisibility condition on the weight of the codewords in Sachar's lower bound.

2 Small weight codewords in the code generated by the incidence matrix of points and hyperplanes in $PG(n, q)$

In this section, we investigate the codewords of small weight in the linear code generated by the incidence matrix of points and hyperplanes in $PG(n, q)$. We define the incidence matrix $A = (a_{ij})$ of the projective space $PG(n, q)$, $q = p^h$, p prime, $h \geq 1$, as the matrix whose rows are indexed by hyperplanes of the space and whose columns are indexed by points of the space, and with entry

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

The p-ary linear code C of the projective space $PG(n, q)$, $q = p^h$, p prime, $h \geq 1$, is the $\mathbb{F}_p$-span of the rows of the incidence matrix A. The support of a codeword c, denoted by $supp(c)$, is the set of all non-zero positions of c. We identify this set of positions with the set of corresponding points of $PG(n, q)$. Let c_P denote the symbol of the codeword c in the coordinate position corresponding to the point P. We denote the scalar product of two vectors v_1, v_2, calculated over $\mathbb{F}_p$, by (v_1, v_2).

The dual code $C^\perp$ is the set of all vectors orthogonal to all codewords of C, hence

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

From now on, we denote the p-ary linear code of points and hyperplanes of $PG(n, q)$, $q = p^h, p$ prime, $h \geq 1$, by C and its dual code by $C^\perp$. If we want to point out the dimension and field of the considered space, we write $C(PG(n, q))$ and $C(PG(n, q))^\perp$, respectively. For convenience of notation, we identify a space with its incidence vector, hence the symbol l stands for the line l or the incidence vector of l, depending on the context.

Lemma 1. *If U_1 and U_2 are subspaces of dimension at least 1 in $PG(n, q)$, then $U_1 - U_2 \in C^\perp$.*

Proof. For every subspace U_i of dimension at least 1 and every hyperplane H, $(H, U_i) = 1$, hence $(H, U_1 - U_2) = 0$, so $U_1 - U_2 \in C^\perp$. □

Note that in Lemma 1, $\dim U_1 \neq \dim U_2$ is allowed.

Lemma 2. *The scalar product (c, U), with $c \in C$ and U an arbitrary subspace of dimension at least 1, is a constant.*

Proof. Lemma 1 yields that $U_1 - U_2 \in C^\perp$, for all subspaces U_1, U_2 with $\dim(U_i) \geq 1$, hence $(c, U_1 - U_2) = 0$, so $(c, U_1) = (c, U_2)$. □

Lemma 3. *A codeword c is in $C \cap C^\perp$ if and only if $(c, U) = 0$ for all subspaces U with $\dim(U) \geq 1$.*

Proof. Let c be a codeword of $C \cap C^\perp$. Since $c \in C^\perp$, $(c, H) = 0$ for all hyperplanes H, Lemma 2 yields that $(c, U) = 0$ for all subspaces U with dimension at least 1.

Now suppose that $c \in C$ and $(c, U) = 0$ for all subspaces U with dimension at least 1. Applying this to a hyperplane yields that $c \in C \cap C^\perp$. □

Theorem 5. *The minimum weight of $C \cap C^\perp$ is equal to $2q^{n-1}$.*

Proof. It follows from Lemma 3 that the support of a codeword c in $C \cap C^\perp$ corresponds to a set of points such that every line contains zero or at least two of them. If $wt(c) < 2q^{n-1}$, then there is a line L containing exactly two points of *supp*(c). Suppose not, then all lines through a point $P \in$ *supp*(c) would have two extra intersection points with *supp*(c), which would imply that $wt(c) \geq 1 + 2\theta_{n-1}$, a contradiction.

Since the restriction of a hyperplane H to a plane π is a line (if $\pi \nsubseteq H$) or the sum of the lines of a pencil (if $\pi \subseteq H$), it follows that the restriction of the codeword c to a plane π is a codeword in the code $C(\pi)$ of points and lines in π.

In all planes π through L, *supp*(c) has at least two points and $(c, l) = 0$ for all lines l in π, so the restriction of c to π lies in $C(\pi) \cap C(\pi)^\perp$, which has minimum weight $2q$ (see [1]).

This implies that *supp*(c) has at least $\theta_{n-2}(2q-2)+2$ points which is equal to $2q^{n-1}$, a contradiction, so the minimum weight of $C \cap C^\perp$ is at least $2q^{n-1}$.

This minimum $2q^{n-1}$ can be obtained when we take the difference of two hyperplanes H_1 and H_2. This vector has weight $2q^{n-1}$, it is a codeword of C since it is a linear combination of hyperplanes, and it belongs to $C^\perp$ since $(H_1 - H_2, H)$=$(H_1, H) - (H_2, H) = 0$ for all hyperplanes H. □

Remark 2. *Proposition 2 of [2] yields the same statement for q prime. Moreover, for q prime, every codeword of weight $2q^{n-1}$ in $C \cap C^\perp$ is a scalar multiple of the difference of two hyperplanes of $PG(n, q)$.*

Lemma 4.

$$C \cap C^\perp = \langle H_1 - H_2 || H_1, H_2 \textit{ distinct hyperplanes of } PG(n,q) \rangle .$$

Proof. Put $A = \langle H_1 - H_2 || H_1, H_2$ distinct hyperplanes of $PG(n,q)\rangle$. Clearly $A \subseteq C \cap C^\perp$, since $(H, v) = (H, H_i) - (H, H_j) = 0$, for every hyperplane H of $PG(n, q)$, and for every $v = H_i - H_j \in A$. Moreover, since $\langle A \cup \{H_k\}\rangle$ contains each hyperplane, it follows that $\dim(C) - 1 \leq \dim(A) \leq \dim(C \cap C^\perp)$. The lemma now follows easily, since $C \cap C^\perp$ is not equal to C, as a hyperplane is not orthogonal to itself. □

Before we can link codewords of small weight to blocking sets, we need to prove that a small blocking set can be uniquely reduced to a minimal blocking set.

A *blocking set* (with respect to lines) of $PG(n,q)$ is a set B of points such that every line contains at least one point of B. A blocking set is called *minimal* if no proper subset of it is a blocking set. A blocking set is called *trivial* when it contains a hyperplane.

Lemma 5. *A point on a minimal blocking set B of size $q^{n-1}+k$, with $k < q^{n-1}$, in $PG(n,q)$ (w.r.t. lines) lies on at least $q^{n-1}-k$ tangent lines.*

Proof. For $n = 2$, the lemma immediately follows from Sziklai and Szőnyi [13, Proposition 2.8], [14]. We use this result to prove the lemma for general n.

A point R of B lies on at least one tangent line L. Take all the planes through L, call them $\pi_1, ..., \pi_{\theta_{n-2}}$. Let x_i be the number of points of B lying in π_i, different from the point R. Then

$$1 + \sum_{i=1}^{\theta_{n-2}} x_i = q^{n-1} + k.$$

Writing x_i as $2q - y_i$, we get

$$q^{n-1} + k = 1 + \sum x_i = 1 + \sum (2q - y_i) = 1 + 2q\theta_{n-2} - \sum y_i,$$

and hence

$$\sum y_i = 2q\theta_{n-2} - q^{n-1} + 1 - k.$$

Whenever $y_i > 1$, the number of points in the plane π_i is less than $2q$, and applying the result for $n = 2$, it follows that the point R lies on at least $y_i - 1$ tangent lines in π_i. So R lies on at least $y_i - 2$ tangent lines, different from L, in each plane π_i for which $y_i > 1$. It follows that the total number of tangent lines through R is at least

$$1 + \sum_{i|y_i>1} (y_i - 2).$$

We can rewrite this number as:

$$1 + \sum_{i=1}^{\theta_{n-2}} (y_i - 2) - \sum_{i|y_i \leq 1} (y_i - 2).$$

Using the fact that $\sum_{i|y_i \leq 1}(y_i - 2)$ is always negative, this yields that the number of tangent lines through R is at least

$$1 + 2q\theta_{n-2} - q^{n-1} - k + 1 - 2\theta_{n-2} =$$

$$q^{n-1} - k,$$

which proves the statement. □

Corollary 1. *Every blocking set B w.r.t. lines in $PG(n,q)$, of size smaller than $2q^{n-1}$, can be uniquely reduced to a minimal blocking set B'.*

Proof. Suppose that $|B| = q^{n-1} + k$, and let B' be a minimal blocking set contained in B, with $|B'| = q^{n-1} + k'$. A point in $B \backslash B'$ lies on zero tangent lines to B. By Lemma 5, a point P_1 of B' lies on at least $q^{n-1} - k'$ tangent lines to B'. There are $k - k'$ points in $B \backslash B'$, so P_1 lies on at least $q^{n-1} - k' - (k - k')$ tangent lines to B. Since $k < q^{n-1}$, P_1 lies on at least one tangent line to B. It follows that B' is the set of points of B, which lie on at least one tangent line to B, and hence, is uniquely determined. □

We are now ready to link codewords of small weight to blocking sets.

Lemma 6. *A codeword c of $C(PG(n,q))$, with weight $wt(c)$ smaller than $2q^{n-1}$, defines a minimal blocking set w.r.t. lines of $PG(n,q)$. Moreover, c is a codeword taking only values from $\{0, a\}$, for some $a \in \mathbb{F}_p^\star$, and supp(c) intersects every line in $1 \pmod p$ points.*

Proof. Take a codeword c with weight $wt(c) < 2q^{n-1}$, then according to Lemmas 2, 3 and Theorem 5, $(c, l) = a \neq 0$ for every line l. So *supp*(c) defines a blocking set B w.r.t. lines of $PG(n,q)$. We now show that this blocking set is minimal. Suppose that every line contains at least two points of the blocking set. Counting the points of B on all lines through a point not in B yields

$$|B| \geq 2\theta_{n-1},$$

a contradiction. So there is a point $R \in B$ lying on at least one tangent line l to B. This implies that $(c, l) = c_R = a \neq 0$. Since $(c, m) = a$ for all lines m (Lemma 2), we may conclude that for every necessary point R of the blocking set B defined by c, c_R equals $a \neq 0$.

By way of contradiction, suppose that c defines a non-minimal blocking set, and consider a point P_1 that is not necessary. If all θ_{n-1} lines through P_1 contain at least two extra points of B, then $|B| \geq 2\theta_{n-1} + 1 > 2q^{n-1}$, a contradiction. So there is a line P_1P_2 which has only P_1 and P_2 in common with B. Since B can be uniquely reduced to a minimal blocking set, see Corollary 1, the point P_2 is necessary, which implies that $c_{P_2} = a$. But $a = (c, P_1P_2) = c_{P_1} + c_{P_2} = a + c_{P_1}$, which implies that $c_{P_1} = 0$, contradicting $P_1 \in B$. This implies that B is minimal.

Since $(c, m) = a$ for all lines m, and $c_P = a$ for all points $P \in$ *supp*(c), it follows that *supp*(c) intersects every line in $1 \pmod p$ points. □

We give another proof for the following theorem proven in [1, Proposition 5.7.3], by using Lemma 6.

Corollary 2. *The minimum weight codewords of C are the scalar multiples of the incidence vectors of the hyperplanes of $PG(n,q)$.*

Proof. According to Lemma 6, a codeword of weight smaller than $2q^{n-1}$ is a scalar multiple of the incidence vector of a minimal blocking set with respect to lines. A result of Bose and Burton [3] shows that the minimum size of a blocking set with respect to lines in $PG(n,q)$ is equal to θ_{n-1}, and that this minimum is reached if and only if the blocking set is a hyperplane. □

The following lemmas are extensions of Lemmas 6.6.1 and 6.6.2 of Assmus and Key [1]. They will be used to exclude small non-trivial linear blocking sets as codewords.

Lemma 7. *A vector v of $V(\theta_n, p)$ taking only values from $\{0, a\}$, $a \in \mathbb{F}_p^\star$, is contained in $(C \cap C^\perp)^\perp$ if and only if $|supp(v) \cap H| \pmod{p}$ is independent of the hyperplane H of $PG(n, q)$.*

Proof. Let v be a vector in $(C \cap C^\perp)^\perp$, then $(v, H_1 - H_2) = 0$ since $C \cap C^\perp$ is generated by the differences of the hyperplanes (Lemma 4). We see that $(v, H) = a|supp(v) \cap H| \pmod{p}$ is independent of the choice of the hyperplane H and so is $|supp(v) \cap H| \pmod{p}$.

Conversely, if $|supp(v) \cap H|$ is constant $\pmod{p}$, then $(v, H) = a|supp(v) \cap H| \pmod{p}$. This implies that $(v, H_1 - H_2) = 0$ for all hyperplanes H_1, H_2, and hence $v \in (C \cap C^\perp)^\perp$. □

Lemma 8. *Let c,v be two vectors taking only values from $\{0, a\}$, $a \in \mathbb{F}_p^\star$, with $c \in C$, $v \in (C \cap C^\perp)^\perp$. If $|supp(c) \cap H| \equiv |supp(v) \cap H| \pmod{p}$ for every hyperplane H, then $|supp(c) \cap supp(v)| \equiv |supp(c)| \pmod{p}$.*

Proof. We know that $c \in C$, hence, according to Lemma 4, $(c, H_1 - H_2) = 0$ for all hyperplanes H_1, H_2, so $|supp(c) \cap H| \pmod{p}$ is independent of the hyperplane H. Since $(c - v, H) = (c, H) - (v, H) \equiv a|supp(c) \cap H| - a|supp(v) \cap H| \equiv 0 \pmod{p}$, for every hyperplane H, it follows that $c - v \in C^\perp$, and hence $(c - v, c) \equiv a^2|supp(c)| - a^2|supp(c) \cap supp(v)| \equiv 0 \pmod{p}$. This yields that $|supp(c)| \equiv |supp(c) \cap supp(v)| \pmod{p}$. □

As mentioned in the introduction, we will eliminate all so-called non-trivial *linear* blocking sets as the support of a codeword of C of small weight. In order to define a linear blocking set, we introduce the notion of a Desarguesian spread.

By what is sometimes called "field reduction", the points of $PG(n, q)$, $q = p^h$, p prime, 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 hence 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 if we want to specify the dimension, a *k-spread.* 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, see [8], that if the dimension of the ambient space is larger than twice the dimension plus one (i.e. $n \geq 2$), then this property characterises a Desarguesian spread.

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

Analogously to the correspondence between the points of $PG(n, q)$ 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 $\mathcal{D}$. With this in mind, it is clear that any $(nh - h)$-dimensional subspace U of $PG(nh + h - 1, p)$ defines a blocking set $\mathcal{B}(U)$ w.r.t. lines in $PG(n, q)$. A blocking set constructed in this way is called a *linear* blocking set. Linear blocking sets were first introduced by Lunardon [8], although there a different approach was used. For more on the approach explained here, we refer to [7].

Lemma 9. *If U is a subspace of $PG((n+1)h-1,q)$, then $|\mathcal{B}(U)| = 1 \pmod q$.*

Proof. Suppose that U is a subspace of $PG((n+1)h-1,q)$ of dimension r and let X_i be the number of spread elements intersecting U in a subspace of dimension i. Each point of U lies in a unique spread element, so

$$\sum_{i=0}^{r} X_i\theta_i = \theta_r \Leftrightarrow$$

$$\sum_{i=0}^{r} X_i q^{i+1} - \sum_{i=0}^{r} X_i = q^{r+1} - 1 \Leftrightarrow$$

$$q(\sum_{i=0}^{r} X_i q^i - q^r) = \sum_{i=0}^{r} X_i - 1.$$

The left hand side is divisible by q, so $\sum_{i=0}^{r} X_i = |\mathcal{B}(U)| = 1 \pmod q$. □

We put $N = h(n-1)$ throughout the following proofs. We call the linear blocking set B of $PG(n,q)$ defined by $\mathcal{B}(U_N)$, where U_N is an N-dimensional subspace of $PG(h(n+1)-1,p)$, a *small* linear blocking set. Such a small linear blocking set is always minimal. Our goal is to exclude the incidence vectors of small linear blocking sets as codewords of $C(PG(n,q))$.

Lemma 10. *Let U_N be an N-dimensional subspace of $PG(h(n+1)-1,p)$. Then the number of spread elements of $\mathcal{B}(U_N)$ intersecting U_N in exactly one point is at least $p^{hn-h} - p^{hn-h-2} - p^{hn-h-3} - \cdots - p^{hn-2h+1} - p^{hn-2h-2} - \cdots - p^{hn-3h+1} - p^{hn-3h-2} - \cdots - p^{h+1} - p^{h-2} - \cdots - p$.*

Proof. The set $\mathcal{B}(U_N)$ defines a blocking set B in $PG(n,q)$, $q = p^h$, p prime, $h \geq 1$, w.r.t. the lines. So $|\mathcal{B}(U_N)| = |B| \geq (q^n-1)/(q-1) = (p^{hn}-1)/(p^h-1)$ by Bose and Burton [3]. Suppose that there are exactly x spread elements of $\mathcal{B}(U_N)$ intersecting U_N in one point, then

$$\frac{p^{hn}-1}{p^h-1} \leq |B| \leq \frac{|U_N|-x}{p+1} + x.$$

Using that $|U_N| = (p^{N+1}-1)/(p-1)$ yields that $x \geq p^{hn-h} - p^{hn-h-2} - p^{hn-h-3} - \cdots - p^{hn-2h+1} - p^{hn-2h-2} - \cdots - p^{hn-3h+1} - p^{hn-3h-2} - \cdots - p^{h+1} - p^{h-2} - \cdots - p$. □

Remark 3. *It follows from Lemma 10 that the number of spread elements of $\mathcal{B}(U_N)$ intersecting U_N in exactly one point is at least $p^N - p^{N-1} + 1$. We will use this weaker bound.*

Lemma 11. *If there are $p^N - p^{N-1} + 1$ points R_i, $i = 1, \ldots, p^N - p^{N-1} + 1$, of a minimal blocking set B in $PG(n,q)$, for which it holds that every line through R_i is either a tangent line to B or is entirely contained in B, then B is a hyperplane of $PG(n,q)$.*

Proof. It is easy to see that a plane through a line R_iR_j, $i \neq j$, is either completely contained in B, or intersects B only in the line R_iR_j. There are at least $(p^N - p^{N-1})/p^h$ different lines R_1R_i, $i \neq 1$.

We prove that if $B \supset \pi_m$, $B \neq \pi_m$, for some m-dimensional space π_m through R_1, then $B \supseteq \pi_{m+1}$ for some $(m+1)$-dimensional space through π_m for all $m < n-1$.

If $B \supset \pi_m$, then there are still $(p^N - p^{N-1})/p^h - (p^{hm}-1)/(p^h-1)$ lines R_1R_j through R_1, but not in π_m, such that every plane through it intersects B in this line or lies completely in B. We can choose such a line R_1R_j if $m < n-1$ and $p^h > 2$. Then the space $\langle R_1R_j, \pi_m\rangle$ is clearly contained in B. By induction, we find a hyperplane π contained in B. Since B is minimal, $B = \pi$. □

Remark 4. *It follows from the proof of Lemma 11 that it is sufficient to find $n-1$ linearly independent points R_i such that every line through R_i is either a tangent line to B or is entirely contained in B, to prove that B is a hyperplane. Moreover, this bound is tight. If there are only $n-2$ linearly independent points for which this condition holds, we have the counterexample of a Baer cone, i.e. let B be the set of all lines connecting a point of a Baer subplane $\pi = PG(2,\sqrt{q})$ to the points of an $(n-3)$-dimensional subspace of $PG(n,q)$, skew to π.*

Lemma 12. *Let U_{N-1} be a fixed $(N-1)$-dimensional space in $PG(h(n+1)-1,p)$ and let U_N be an arbitrary N-dimensional space containing U_{N-1}. Then $\mathcal{B}(U_N)$ is entirely determined by U_{N-1} and two elements R_1, $R_2 \in \mathcal{B}(U_N)\backslash\mathcal{B}(U_{N-1})$.*

Proof. We may assume that $\mathcal{B}(U_{N-1}) \neq \mathcal{B}(U_N)$, since the theorem is obvious if $\mathcal{B}(U_{N-1}) = \mathcal{B}(U_N)$.

Suppose that $R_1, R_2 \in \mathcal{B}(U_N)\backslash\mathcal{B}(U_{N-1})$, $R_1 \neq R_2$. If $R_3 \in \mathcal{B}(U_N)\backslash\mathcal{B}(U_{N-1})$, $R_2 \neq R_3 \neq R_1$, then we claim that R_3 can be constructed only using elements of $\mathcal{B}(U_{N-1}) \cup \{R_1, R_2\}$. Clearly, R_i intersects U_N in a point P_i since R_1, R_2 and R_3 are elements of $\mathcal{B}(U_N)\backslash\mathcal{B}(U_{N-1})$. So $\langle P_1, P_3\rangle$ intersects U_{N-1} in a point P_4 which lies on a unique spread element R_4. Similarly, the spread element through $\langle P_2, P_3\rangle \cap U_{N-1}$ is called R_5.

Case 1: $P_3 \notin P_1P_2$. The spaces $\langle R_1, R_4\rangle$ and $\langle R_2, R_5\rangle$ are spanned by two elements of a Desarguesian spread, so they intersect in a spread element. The intersection of $\langle R_1, R_4\rangle$ with $\langle R_2, R_5\rangle$ certainly contains R_3. We can conclude that $R_3 = \langle R_1, R_4\rangle \cap \langle R_2, R_5\rangle$.

Case 2: $P_3 \in P_1P_2$. Take a spread element $R_6 \in \mathcal{B}(U_N)$ already constructed in Case 1. We can switch R_6 with R_2. Then $R_3 \notin \langle R_1, R_6\rangle$. So we can copy the proof of Case 1 to determine R_3 from R_1, R_6 and U_{N-1}. But R_6 was determined by R_1, R_2 and U_{N-1}, hence so is R_3. □

Theorem 6. *For every small linear blocking set B w.r.t. lines, not defining a hyperplane in $PG(n,p^h)$, there exists a small linear blocking set B' intersecting B in $2 \pmod p$ points.*

Proof. As we have seen before, a small linear blocking set B in $PG(n,p^h)$ corresponds to an N-dimensional space U_N in $PG(h(n+1)-1,p)$. We will construct a subspace U'_N that defines a second blocking set B' intersecting B in $2 \pmod p$ points.

There is a spread element R', lying in a $(2h-1)$-dimensional space spanned by two spread elements R_1 and R_2, $R_1, R_2 \in \mathcal{B}(U_N)$, where $R_1 \cap U_N$ is a point, such that R' does not intersect U_N. Suppose that for every R'_1 and R'_2 in $\mathcal{B}(U_N)$, where $R'_1 \cap U_N$ is a point, each spread element in $\langle R'_1, R'_2\rangle$ intersects U_N. Then $\mathcal{B}(U_N)$ defines a set B of points in $PG(n,q)$ such that every line through R'_1 is tangent to B in R'_1 or is entirely contained in B. But Remark 3 and Lemma 11 then imply that B is a hyperplane, a contradiction.

Choose an $(N-1)$-dimensional space $U_{N-1} \subset U_N$, such that $R_2 \in \mathcal{B}(U_{N-1})$ and $R_1 \notin \mathcal{B}(U_{N-1})$.

The elements R_1, R_2, R' define an $(h-1)$-regulus. Take a transversal line m to this $(h-1)$-regulus intersecting U_{N-1} in a point of $U_{N-1} \cap R_2$. Then $\langle m, U_{N-1}\rangle$ is an N-dimensional space U'_N, defining a blocking set B' of $PG(n,q)$.

Now $\mathcal{B}(U_N)$ and $\mathcal{B}(U'_N)$ have $\mathcal{B}(U_{N-1})$ and R_1 in common. So B and B' have at least $(1 \mod p) + 1$ points in common (see Lemma 9).

If $\mathcal{B}(U_N) \cap \mathcal{B}(U'_N)$ contains another spread element $R_3 \notin \mathcal{B}(U_{N-1})$, $R_3 \neq R_1$, then Lemma 12 implies that $\mathcal{B}(U_N) = \mathcal{B}(U'_N)$, contradicting $R' \in \mathcal{B}(U'_N) \backslash \mathcal{B}(U_N)$. It follows that the blocking sets B and B' of $PG(n,q)$ corresponding to U_N and U'_N intersect in $2 \pmod p$ points. □

Using this result, we exclude in Theorem 7 all small non-trivial linear blocking sets as codewords.

Theorem 7. *Let v be the incidence vector of a small non-trivial linear blocking set of points w.r.t. lines of $PG(n,q)$, then $v \notin C$.*

Proof. We know that $|supp(v)| = 1 \pmod p$. We know from Theorem 6 that there exists a linear minimal blocking set w such that $|supp(v) \cap supp(w)| \equiv 2 \pmod p$. Since $|supp(w) \cap H| \equiv 1 \pmod p$ for every hyperplane H (see Lemma 9), it follows that $w \in (C \cap C^\perp)^\perp$ (Lemma 7). Suppose that $v \in C$, then Lemma 8 implies that $|supp(v) \cap supp(w)| \equiv |supp(v)| \pmod p \equiv 1 \pmod p$, a contradiction. □

Together with Lemma 6, Theorem 7 gives the following corollary.

Corollary 3. *The only possible codewords c of C 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.*

Remark 5. *Amongst many of the leading researchers dealing with blocking sets, it is believed (and conjectured, see [12]) that all small minimal blocking sets are linear. If that conjecture is true, then Corollary 3 eliminates all possible codewords of weight in $]\theta_{n-1}, 2q^{n-1}[$. The cases in which the conjecture is proven (and relevant here) are mentioned below.*

In some cases, we can exclude non-linear blocking sets intersecting every line in $1 \pmod p$ points.

Lemma 13. *The only minimal blocking set B in $PG(n,p)$, with p prime, such that every line contains $1 \pmod p$ points of B, is a hyperplane.*

Proof. Let B be a blocking set in $PG(n,p)$ such that every line intersects B in $1 \pmod p$ points. If $B \supset PG(m,p)$, $B \neq PG(m,p)$, for some m, then $B \supseteq PG(m+1,p)$ since we can connect a point R' in $B \setminus PG(m,p)$ to all points of $PG(m,p)$. All these lines have to lie in B, so $PG(m+1,p) = \langle R', PG(m,p)\rangle \subset B$. There is always a line skew to $PG(m,p)$, with $m < n-1$, so we can always find a point $R' \in B \setminus PG(m,p)$ for $m < n-1$. This implies that the only possibility for a minimal blocking set B such that every line has $1 \pmod p$ points of B, is a hyperplane $PG(n-1,p)$. □

The next corollary, following from Lemma 13, extends the result of Chouinard (Theorem 1 (1)) to general dimension.

Corollary 4. *There are no codewords c, with $\theta_{n-1} < wt(c) < 2p^{n-1}$, in $C(PG(n,p))$, p prime.*

We turn our attention to minimal blocking sets B, with $|B| \in]\theta_{n-1}, 2q^{n-1}[$, in $PG(n,q)$, $q = p^h$, p prime, $h \geq 1$, such that every line contains 1 (mod p) points of B. Let e be the maximal integer for which B intersects every line in 1 (mod p^e) points. Then results of Sziklai prove that e is a divisor of h [12].

In [6, Corollary 5.2], it is proven that

$$|B| \geq q^{n-1} + \frac{q^{n-1}}{p^e+1} - 1.$$

We now derive the upper bound on $|B|$, based on [6, Theorem 5.3].

Theorem 8. *Let B be a minimal blocking set w.r.t. the lines of $PG(n,q)$, $q = p^h$, p prime, $h \geq 1$, intersecting every line in* 1 (mod p^e) *points, with e the maximal integer for which this is true, and assume that $|B| \in]\theta_{n-1}, 2q^{n-1}[$ and that $p^e > 2$.*

Then

$$|B| \leq q^{n-1} + \frac{2q^{n-1}}{p^e}.$$

Proof. Let $E = p^e$. Let τ_{1+iE} be the number of lines intersecting B in $1 + iE$ points. We count the number of lines, the number of pairs (R, l), with $R \in B$ and with l a line through R, and the number of triples (R, R', l), with R and R' distinct points of B and l a line passing through R and R'.

Then the following formulas are valid:

$$\begin{aligned} \sum_{i\geq 0} \tau_{1+iE} &= \frac{(q^{n+1}-1)(q^n-1)}{(q^2-1)(q-1)}, && (1) \\ \sum_{i\geq 0} (1+iE)\tau_{1+iE} &= |B|\left(\frac{q^n-1}{q-1}\right), && (2) \\ \sum_{i\geq 0} (1+iE)(1+iE-1)\tau_{1+iE} &= |B|(|B|-1). && (3) \end{aligned}$$

Then $\sum_{i\geq 0} i(i-1)E^2\tau_{1+iE} \geq 0$ implies that

$$|B|(|B|-1) - (1+E)|B|\left(\frac{q^n-1}{q-1}\right) + (1+E)\frac{(q^{n+1}-1)(q^n-1)}{(q^2-1)(q-1)} \geq 0.$$

Under the condition $2 < E$, this implies that

$$|B| \leq q^{n-1} + \frac{2q^{n-1}}{E} \quad \text{or that} \quad |B| \geq Eq^{n-1} + 1.$$

□

To exclude codewords in the code of $PG(n,p^2)$, with p a prime, we can use the following theorem of Weiner which implies that every small minimal blocking set in $PG(n,p^2)$ is linear.

Theorem 9. *[15] A non-trivial minimal blocking set of $PG(n,p^2)$, $p > 11$, p prime, with respect to k-spaces and of size less than $3(p^{2(n-k)}+1)/2$ is a $(t, 2((n-k)-t-1))$-Baer cone with as vertex a t-space and as base a $2((n-k)-t-1)$-dimensional Baer subgeometry, where* $\max\{-1, n-2k-1\} \leq t < n-k-1$.

Theorem 9, together with Theorem 8, yields the following corollary.

Corollary 5. *There are no codewords c, with $wt(c) \in]\theta_{n-1}, 2q^{n-1}[$, in $C(PG(n,q))$, $q = p^2$, $p > 11$, p prime.*

For general $q = p^h$, p prime, $h \geq 3$, Theorem 8 implies that the weights of possible codewords c in C, with $wt(c) \in]\theta_{n-1}, 2q^{n-1}[$, corresponding to non-linear blocking sets intersecting every line in 1 (mod p^e) points, with e the maximal integer for which this is true, must belong to certain small intervals.

In particular, we exclude all the codewords with weight in $[3q^{n-1}/2, 2q^{n-1}[$; in this way, excluding half of the interval $]\theta_{n-1}, 2q^{n-1}[$.

Corollary 6. *There are no codewords c in $C(PG(n,q))$, $q = p^h$, p prime, $p > 3$, $h \geq 3$, with weight in $[3q^{n-1}/2, 2q^{n-1}[$.*

3 Minimum weight codewords in the dual code generated by the incidence matrix of points and hyperplanes of $PG(n,q)$

In this section, we consider codewords $c \in C(PG(n,q))^\perp$, $q = p^h$, p prime, $h \geq 1$, with $C(PG(n,q))$ the p-ary linear code generated by the incidence matrix of points and hyperplanes in $PG(n,q)$, $q = p^h$, p prime, $h \geq 1$. This means that $(c, H) = 0$ for all hyperplanes H of $PG(n,q)$, since a codeword in $C^\perp$ is orthogonal to all the rows of the generator matrix of C.

For every hyperplane H,

$$\sum_{P \in supp(c) \cap H} c_P = 0.$$

Denote the minimum distance of a linear code C by $d(C)$. Note that $d(C^\perp) \leq 2q$ since the difference of the incidence vectors of two intersecting lines is a codeword of $C^\perp$.

Lemma 14. *For each $n \geq 2$, the following holds:*

$$d(C(PG(n,q))^\perp) \geq d(C(PG(n-1,q))^\perp) \geq \cdots \geq d(C(PG(2,q))^\perp).$$

Proof. Let c be a codeword of $C(PG(n,q))^\perp$ of minimum weight, and let R be a point of $PG(n,q) \backslash supp(c)$, with R on a tangent line to $supp(c)$, and let H be a hyperplane of $PG(n,q)$ not containing R. For each point $P \in H$, define $c'_P = \sum c_{P_i}$, with P_i the points of $supp(c)$ on the line $\langle R, P \rangle$, and let c' denote the vector with coordinates c'_P, $P \in H$. Note that $c' \neq 0$, since R lies on a tangent line to $supp(c)$.

Then it easily follows that $c' \in C(PG(n-1,q))^{\perp}$, and $supp(c')$ is contained in the projection of $supp(c)$ from the point R onto the hyperplane $H = PG(n-1,q)$. Clearly, $|supp(c')| \leq |supp(c)|$.

Using this relation on a codeword c of minimum weight yields that $d(C(PG(n-1,q))^{\perp}) \leq d(C(PG(n,q))^{\perp})$. Continuing this process proves the statement. □

Remark 6. *We call the vector c' defined in the proof of Lemma 14, the projection of c.*

Theorem 10. *For each $n \geq 2$, $d(C(PG(n,q))^{\perp}) = d(C(PG(2,q))^{\perp})$.*

Proof. Embed $\pi = PG(2,q)$ in $PG(n,q)$, $n > 2$, and extend each codeword c of $C(\pi)^{\perp}$ to a vector $c^{(n)}$ of $V(\theta_n,p)$ by putting a zero at each point $P \in PG(n,q)\backslash\pi$. Since the all one vector of $V(\theta_2,p)$ is a codeword of $C(PG(2,q))$, it follows that $\sum_{P\in\pi} c_P^{(n)} = 0$ for each $c^{(n)}$.

This implies that $(c^{(n)},H) = 0$, for each hyperplane H of $PG(n,q)$ which contains π. If a hyperplane H of $PG(n,q)$ does not contain π, then $(c^{(n)},H) = (c, H \cap \pi) = 0$, since $(c,l) = 0$, for each line l of π.

It follows that $c^{(n)}$ is a codeword of $C(PG(n,q))^{\perp}$ of weight equal to the weight of c, which implies that $d(C(PG(n,q))^{\perp}) \leq d(C(PG(2,q))^{\perp})$. Regarding Lemma 14, this yields that $d(C(PG(n,q))^{\perp}) = d(C(PG(2,q))^{\perp})$. □

Lemma 15. *Let B be a set in $PG(n,q)$, with $\dim\langle B\rangle \geq 3$, such that if a point R in $PG(n,q)\backslash B$ lies on at least one secant line to B, then it does not lie on tangent lines to B, then $|B| \geq 3q$.*

Proof. We first prove the following result. When we take two secants l_1, l_2 through R, then the plane $\langle l_1, l_2\rangle$ contains at least $q + \max\{a_1, a_2\}$ points of B, where $a_i = |l_i \cap B|$. Take a point $S \in B$ on $l_1\backslash l_2$. Then every line in $\langle l_1, l_2\rangle$ through S must be a secant line to B; else if it lies on a tangent line l, $l \cap l_2$ is a point not in B lying on a tangent line and a secant line to B, which is a contradiction. So $|B \cap \langle l_1, l_2\rangle| \geq q + a_1$, and similarly, $|B \cap \langle l_1, l_2\rangle| \geq q + a_2$.

Now R lies on at least three non-coplanar secants to B, since $\dim\langle B\rangle \geq 3$. Now

$$|\langle l_1, l_2\rangle \cap B| \geq q + \max\{a_1, a_2\},$$
$$|\langle l_1, l_3\rangle \cap B| \geq q + \max\{a_1, a_3\},$$
$$|\langle l_2, l_3\rangle \cap B| \geq q + \max\{a_2, a_3\},$$

with $a_i = |l_i \cap B|$.

So $|B| \geq (q + \max\{a_1, a_2\}) + (q + \max\{a_1, a_3\}) + (q + \max\{a_2, a_3\}) - (a_1 + a_2 + a_3)$, because we counted the points lying on $l_i \cap B$ twice. It follows that $|B| \geq 3q$. □

Theorem 11. *Let c be a codeword of $C(PG(n,q))^{\perp}$, $n \geq 3$, of minimal weight, then $supp(c)$ is contained in a plane of $PG(n,q)$.*

Proof. The difference of two intersecting lines clearly belongs to the dual code and has weight $2q$, so we may assume that $wt(c) \leq 2q$.

Assume that $\dim\langle supp(c)\rangle \geq 3$; using Lemma 15, we find a point R lying on a tangent line to $supp(c)$ and lying on at least one secant line to $supp(c)$. It follows from Theorem 10 that $wt(c) = d(C(PG(n,q))^\perp) = d(C(PG(n-1,q))^\perp) = d(C(PG(2,q))^\perp)$.

Since R lies on at least one secant line and at least one tangent line to $supp(c)$, the projection c', of c from R, has weight smaller than $wt(c)$.

But then c' is a non-zero codeword of $C(PG(n-1,q))^\perp$ satisfying $0 < wt(c') \leq wt(c) - 1 < d(C(PG(n-1,q))^\perp)$, a contradiction. □

In Theorem 11, we reduced the problem of finding the minimum weight of the dual of the code generated by points and hyperplanes in $PG(n,q)$ to finding the minimum weight of the dual of the code generated by points and lines in $PG(2,q)$. This means that we can use the known results about this latter code.

From [1, Theorem 6.4.2], we get the following bound on the minimum weight d of $C(PG(2,q))^\perp$, with $q = p^h, p$ prime, $h \geq 1$:

$$q + p \leq d \leq 2q,$$

with equality at the lower bound for $p = 2$.

Using this bound, together with Theorem 11, yields the following three theorems.

Theorem 12. *The minimum weight of $C(PG(n,p))^\perp$, p prime, is equal to $2p$.*

Theorem 13. *The minimum weight of $C(PG(n,2^h))^\perp$ is equal to $2^h + 2$.*

Theorem 14. *If d is the minimum weight of $C(PG(n,q))^\perp$, $q = p^h$, p prime, then*

$$q + p \leq d \leq 2q.$$

We conclude this manuscript by improving on Theorem 14. We summarize the improved bounds on the minimum weight of $C(PG(n,q))^\perp$ in Table 1 at the end of this section.

In Theorem 5, it was proven that the minimum weight of $C \cap C^\perp$ is equal to $2q^{n-1}$. We now show that the minimum weight of $C^\perp$ is smaller than $2q$ under certain conditions.

Theorem 15. *Let B be a minimal blocking set in $PG(2,q)$ of size $q+k$, with $k < (q+3)/2$, of Rédei-type (i.e. there exists a k-secant L). Then the difference of the incidence vectors of B and L is a codeword of $C(PG(2,q))^\perp$ with weight $2q+1-k$.*

Proof. If $k < (q+3)/2$, then B is a small minimal blocking set, hence every line intersects B in $1 \pmod{p}$ points (see [14]). Let c_1 be the incidence vector of B and let c_2 be the incidence vector of L. Then $(c_1 - c_2, m) = (c_1, m) - (c_2, m) = 0$ for all lines m, hence $c_1 - c_2$ is a codeword of $C(PG(2,q))^\perp$, with weight $2q + 1 - k$. □

We can use this theorem to lower the upper bound on the possible minimum weight of codewords of $C(PG(2,q))^\perp$. Let $q = p^h$, let e be a divisor of h with $1 < e < h$, then we have the following linear blocking set

$$B = \left\{(1, x, x^{p^e}) || x \in \mathbb{F}_{p^h}\right\} \cup \left\{(0, x, x^{p^e}) || x \in \mathbb{F}_{p^h}, x \neq 0\right\}.$$

The size of such a blocking set is $q + \frac{q-1}{p^e-1}$. The second part belongs to a line L which is a $\frac{q-1}{p^e-1}$-secant, so the weight of the codeword arising from the difference of the incidence vectors of B and L is equal to $2q + 1 - \frac{q-1}{p^e-1}$.

Corollary 7. *For $q = p^h$, p prime, $h \geq 1$, $d(C(PG(2,q))^\perp) \leq 2q + 1 - (q - 1)/(p - 1)$.*

Remark 7. *In [2, p. 130], the authors write that they have no examples of codewords of $C^\perp$ with weight smaller than $2q$, where q is odd. Theorem 15 provides numerous examples of such codewords for even and odd q.*

The following result of Sachar [11] states a lower bound on the minimum weight of $C^\perp$.

Theorem 16. *[11] Let c be a codeword of minimum weight of $C(PG(2,q))^\perp$, $q = p^h$, p prime, and suppose that $p \nmid wt(c)$. If $p = 5$, then $wt(c) \geq 4(2q+3)/5$, and if $p > 5$, then $wt(c) \geq (12q + 18)/7$.*

We give an alternative proof for the second part of Theorem 16, with a small change in the case $p = 7$, which has as convenience that the condition $p \nmid wt(c)$ is not necessary.

In this alternative proof, we use the following lemma of Sachar.

Lemma 16. *[11, Proposition 2.2] Suppose that there are $2m$ different non-zero symbols used in the codeword $c \in C(PG(2,q))^\perp$. Then $wt(c) \geq q + \frac{2m-1}{2m+1}q + \frac{6m}{2m+1}$.*

Theorem 17. *Let c be a codeword of minimum weight of $C(PG(2,q))^\perp$, $q = p^h$, p prime, $h \geq 1$. If $p = 7$, then $wt(c) \geq (12q + 6)/7$, and if $p > 7$, then $wt(c) \geq (12q + 18)/7$.*

Proof. Let c be a codeword of minimum weight of $C^\perp$ and suppose that $wt(c) < (12q+18)/7$. Then it follows from Lemma 16 that there are at most four different non-zero symbols used in the codeword c. Since through every point of $supp(c)$, there is a 2-secant, it is easy to see that the number of non-zero symbols used in c must be even, and that the non-zero symbols in c occur in pairs $\{a, -a\}$.

Suppose first that there are exactly two non-zero symbols used in c, say 1 and -1. Suppose that the symbol -1 occurs the least, say y times. Let X_S be the number of 2-secants through a point S of $supp(c)$. Let R be a point of $supp(c)$ for which $c_R = 1$. At most y of the lines through R contain a point R' of $supp(c)$ with $c_{R'} = -1$, so at least $q+1-y$ of those lines only contain points R' of $supp(c)$ with $c_{R'} = 1$. Since $(c, l) = 0$ for all lines l, such lines contain 0 (mod p) points of $supp(c)$. Then

$$wt(c) \geq (q + 1 - y)(p - 1) + y + 1.$$

If $wt(c) < (12q + 6)/7$, then $y < (6q + 3)/7$, and this implies that

$$q + 1 > (q + 4)p/7 + 1;$$

a contradiction if $p = 7$. If $wt(c) < (12q + 18)/7$, then $y < (6q + 9)/7$, and this implies that

$$q \geq (q - 2)p/7;$$

a contradiction if $p > 7$.

Assume now that there are four non-zero symbols, say $1, -1, a, -a$, in c. We can copy the arguments of the proof of Sachar [11] to obtain the stated lower bound. □

Using Theorem 11, together with Theorem 17, proves that the following result holds.

Theorem 18. *Let c be a codeword of minimum weight of $C(PG(n,q))^\perp$, $q = p^h$, p prime, $h \geq 1$. If $p = 7$, then $wt(c) \geq (12q + 7)/7$, and if $p > 7$, then $wt(c) \geq (12q + 18)/7$.*

We summarize the results on the minimum weight of $C(PG(n,q))^\perp$ in the following table.

p	h	d
2	h	$2^h + 2$
p	1	$2p$
7	h	$(12q + 7)/7 \leq d \leq 2q + 1 - (q - 1)/(p - 1)$
$p > 7$	h	$(12q + 18)/7 \leq d \leq 2q + 1 - (q - 1)/(p - 1)$

Table 1: The minimum weight d of $C(PG(n,q))^\perp$, $q = p^h$, p prime, $h \geq 1$

References

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

[2] B. Bagchi and S.P. Inamdar. Projective Geometric Codes. *J. Combin. Theory, Ser. A* **99** (2002), 128–142.

[3] R.C. Bose and R.C. Burton. A characterization of flat spaces in a finite geometry and the uniqueness of the Hamming and the MacDonald codes. *J. Combin. Theory* **1** (1966), 96–104.

[4] K. Chouinard. Weight distributions of codes from planes (PhD Thesis, University of Virginia) (August 1998).

[5] V. Fack, Sz. Fancsali, L. Storme, G. Van de Voorde, and J. Winne. Small Weight Codewords in Codes arising from Desarguesian Projective Planes. *Des. Codes Cryptogr.*, accepted.

[6] S. Ferret, L. Storme, P. Sziklai, and Zs. Weiner. A t (mod p) result on multiple $(n - k)$-blocking sets in PG(n,q). (In preparation).

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

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

[9] E. Prange. The use of coset equivalence in the analysis and decoding of group codes. Electronics Research Directorate, Air Force Cambridge Research Center, June 1959.

[10] L.D. Rudolph. A class of majority logic decodable codes. *IEEE Trans. Inform. Theory* **13** (1967), 305–307.

[11] H. Sachar. The F_p span of the incidence matrix of a finite projective plane. *Geom. Dedicata* **8** (1979), 407–415.

[12] P. Sziklai. On small blocking sets and their linearity. *J. Combin. Theory, Ser. A*, submitted.

[13] P. Sziklai and T. Szőnyi. Blocking sets and algebraic curves. *Rend. Circ. Mat. Palermo* **51** (1998), 71–86.

[14] T. Szőnyi. Blocking sets in Desarguesian affine and projective planes. *Finite Fields Appl.* **3** (1997), 187–202.

[15] Zs. Weiner. Small point sets of $PG(n, \sqrt{q})$ intersecting every k-space in 1 modulo $\sqrt{q}$ points. *Innov. Incidence Geom.* **1** (2005), 171–180.

Address of the authors:

Ghent University, Dept. of Pure Mathematics and Computer Algebra, Krijgslaan 281-S22, 9000 Ghent, Belgium

Michel Lavrauw:	ml@cage.ugent.be	http://cage.ugent.be/∼ml
Leo Storme:	ls@cage.ugent.be	http://cage.ugent.be/∼ls
Geertrui Van de Voorde:	gvdvoorde@cage.ugent.be	