On the code generated by the incidence matrix of points and \( k \)-spaces in \( PG(n, q) \) and its dual

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

December 21, 2013

Abstract

In this paper, we study the \( p \)-ary linear code \( C_k(n, q) \), \( q = p^h \), \( p \) prime, \( h \geq 1 \), generated by the incidence matrix of points and \( k \)-dimensional spaces in \( PG(n, q) \). For \( k \geq n/2 \), we link codewords of \( C_k(n, q) \setminus C_k(n, q)^\perp \) of weight smaller than \( 2q^k \) to \( k \)-blocking sets. We first prove that such a \( k \)-blocking set is uniquely reducible to a minimal \( k \)-blocking set, and exclude all codewords arising from small linear \( k \)-blocking sets. For \( k < n/2 \), we present counterexamples to lemmas valid for \( k \geq n/2 \). Next, we study the dual code of \( C_k(n, q) \) and present a lower bound on the weight of the codewords, hence extending the results of Sachar [12] to general dimension.

1 Introduction

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, \( h \geq 1 \), and let \( V(n + 1, q) \) denote the underlying vector space. Let \( \theta_n \) denote the number of points in \( PG(n, q) \), i.e., \( \theta_n = (q^{n+1} - 1)/(q - 1) \). 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 [3]. 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 when a \( k \)-dimensional subspace is contained in \( K \). The smallest non-trivial \( k \)-blocking sets are characterized as cones with a \( (k - 2) \)-dimensional vertex \( \pi_{k-2} \) and a non-trivial 1-blocking set of minimum cardinality in a plane, skew to \( \pi_{k-2} \), of \( PG(n, q) \) as base curve [3] [8]. 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 \( P \) 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 lot of attention has been paid to blocking sets in the Desarguesian plane \( PG(2, q) \), and to \( k \)-blocking sets in \( PG(n, q) \). It follows from results of Sziklai

\[ \text{This author’s research was supported by the Institute for the Promotion of Innovation through Science and Technology in Flanders (IWT-Vlaanderen).} \]
[13], Szönyi [14], and Szönyi and Weiner [15] that every minimal $k$-blocking set $K$ in $PG(n, q)$, $q = p^h$, $p$ prime, $h \geq 1$, of size smaller than $3(q^{n-k} + 1)/2$, intersects every subspace in zero or in 1 (mod $p$) points. If $e$ is the largest integer such that $K$ intersects every space in zero or 1 (mod $p^e$) points, then $e$ is a divisor of $h$. This implies, for instance, that the cardinality of a minimal blocking set, of size smaller than $3(q+1)/2$, in $PG(2, q)$ can only lie in a number of intervals, each of which corresponds to a divisor $e$ of $h$.

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, $h \geq 1$, 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 $C$ of points and $k$-spaces of $PG(n, q)$, $q = p^h$, $p$ prime, $h \geq 1$, is the $F_p$-span of the rows of the incidence matrix $A$. From now on, we denote this code by $C_k$, or, if we want to specify the dimension and order of the ambient space, 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 weight of $c$ is the number of non-zero positions of $c$ and is denoted by $wt(c)$. Often we identify the support of a codeword with the corresponding set of points of $PG(n, q)$. We let $c_P$ denote the symbol of the codeword $c$ in the coordinate position corresponding to the point $P$, and let $(c_1, c_2)$ denote the scalar product in $F_p$ of two codewords $c_1, c_2$ of $C$. Furthermore, if $T$ is a subspace of $PG(n, q)$, then the incidence vector of this subspace is also denoted by $T$. The dual code $C^\perp$ is the set of all vectors orthogonal to all codewords of $C$, hence

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

This means that for all $c \in C^\perp_k$ and all $k$-spaces $K$ of $PG(n, q)$, we have $(c, K) = 0$. In [10], the $p$-ary linear code $C_{n-1}(n, q)$, $q = p^h$, $p$ prime, $h \geq 1$, was discussed. The main goal of this paper is to prove similar results for the $p$-ary linear code $C_k(n, q)$ defined by the incidence matrix of points and $k$-spaces of $PG(n, q)$, $q = p^h$, $p$ prime, $h \geq 1$. More precisely, in [10], the following results are proven.

**Result 1.** (see also [3, Proposition 5.7.3]) The minimum weight codewords of $C_{n-1}(n, q)$ are the scalar multiples of the incidence vectors of the hyperplanes.

**Result 2.** There are no codewords with weight in the interval $[\theta_{n-1}, 2q^{n-1}]$ in $C_{n-1}(n, q)$, if $q$ is prime, or if $q = p^2$, $p > 11$ prime.

**Result 3.** The only possible codewords of $C_{n-1}(n, q)$, with weight in the interval $[\theta_{n-1}, 2q^{n-1}]$, are the scalar multiples of non-linear minimal blocking sets.

**Result 4.** The minimum weight of $C_{n-1}(n, q) \cap C_{n-1}(n, q)^\perp$ is equal to $2q^{n-1}$.

**Result 5.** If $c$ is a codeword of $C_{n-1}(n, q)^\perp$ of minimal weight, then $supp(c)$ is contained in a plane of $PG(n, q)$.

Theorem [16](2) and Theorem [17] extend Result 1 and the first part of Result 2 to general dimension. However, the generalization of the second part of Result
2 in Theorem[13] and the generalization of Result 3 in Theorem[10,11] are weaker, due to the lack of a generalization of Result 4 in the case where \( q \) is not a prime. In Theorem[11] Result 5 is generalized.

In the study of codewords \( c \in C_k(n, q) \) of weight smaller than \( 2q^k \), we distinguish the cases \( c \in C_k(n, q) \setminus C_k(n, q) \setminus C_k(n, q) \) and \( c \in C_k(n, q) \cap C_k(n, q) \). In the first case, for \( k \geq n/2 \), \( \supp(c) \) defines a \( k \)-blocking set of \( PG(n, q) \). We eliminate the small linear \( k \)-blocking sets as possible codewords, if \( k \geq n/2 \). One of the results we need regarding \( k \)-blocking sets, is the unique reducibility property of \( k \)-blocking sets, of size smaller than \( 2q^k \), to a minimal \( k \)-blocking set. We derive this property in the next section.

2 A unique reducibility property for \( k \)-blocking sets in \( PG(n, q) \) of size smaller than \( 2q^k \)

In [14], algebraic curves are associated to blocking sets in \( PG(2, q) \), in order to prove the following result.

Result 6. [14] Szőnyi] If \( K \) is a blocking set in \( PG(2, q) \) of cardinality \( |K| \leq 2q \), then \( K \) can be reduced in a unique way to a minimal blocking set.

In this section, we extend this result to general \( k \)-blocking sets in \( PG(n, q) \), \( n \geq 3 \), by associating an algebraic hypersurface to a blocking set in \( PG(n, q) \).

Let \( K \) be a blocking set in \( PG(n, q) \), \( n \geq 3 \), with \( |K| \leq 2q - 1 \). Suppose that the coordinates of the points are \((x_0, \ldots, x_n)\), where \( X_n = 0 \) defines the hyperplane at infinity \( H_\infty \), and let \( U \) be the set of affine points of \( K \). Let \( |K| = q + k + N \), \( N \geq 1 \), where \( N \) is the number of points of \( K \) in \( H_\infty \), Furthermore we assume that \((0, \ldots, 0, 1, 0) \in K \). The hyperplanes not passing through \((0, \ldots, 0, 1, 0) \) have equations \( m_0X_0 + \cdots + m_{n-2}X_{n-2} - X_{n-1} = 0 \) and they intersect \( H_\infty \) in the \((n-2)\)-dimensional space \( X_n = m_0X_0 + \cdots + m_{n-2}X_{n-2} - X_{n-1} = 0 \). We call the \((n-1)\)-tuple \( \vec{m} = (m_0, \ldots, m_{n-2}) \) the slope of the hyperplane. We also identify a slope \( \vec{m} \) with the corresponding subspace \( \sum_{j=0}^{n-2} m_jX_j \leq X_{n-1} = 0 \) of dimension \( n - 2 \) at infinity.

Definition 1. Define the Rédei polynomial of \( U \) as

\[
H(X, X_0, \ldots, X_{n-2}) = \prod_{(a_0, \ldots, a_{n-1}) \in U} (X + a_0X_0 + \cdots + a_{n-2}X_{n-2} - a_{n-1}) = X^{q+k} + h_1(X_0, \ldots, X_{n-2})X^{q+k-1} + \cdots + h_{n+k}(X_0, \ldots, X_{n-2}).
\]

For all \( j = 1, \ldots, q + k \), \( \deg h_j \leq j \). For simplicity of notations, we will also write \( H(X, X_0, \ldots, X_{n-2}) \) as \( H(X, \bar{X}) \).

Definition 2. Let \( C \) be the affine hypersurface, of degree \( k \), of \( AG(n, q) \), defined by

\[
f(X, \bar{X}) = X^k + h_1(\bar{X})X^{k-1} + \cdots + h_k(\bar{X}) = 0.
\]

Theorem 1. (1) For a fixed slope \( \vec{m} \) defining an \((n - 2)\)-dimensional subspace at infinity not containing a point of \( K \), the polynomial \( X^q - X \) divides \( H(X, \vec{m}) \). Moreover, if \( k < q - 1 \), then \( H(X, \vec{m})/(X^q - X) = f(X, \vec{m}) \) and \( f(X, \vec{m}) \) splits into linear factors over \( \mathbb{F}_q \).
(2) For a fixed slope \( \bar{m} = (m_0, \ldots, m_{n-2}) \), the element \( x \) is an \( r \)-fold root of \( H(X, \bar{m}) \) if and only if the hyperplane with equation \( m_0X_0 + \cdots + m_{n-2}X_{n-2} - X_{n-1} + x = 0 \) intersects \( U \) in exactly \( r \) points.

(3) If \( k < q-1 \) and \( \bar{m} \) defines an \((n-2)\)-dimensional subspace at infinity not containing a point of \( K \), such that the line \( X_0 = m_0, \ldots, X_{n-2} = m_{n-2} \) intersects \( f(X, \bar{X}) \) at \((x, m_0, \ldots, m_{n-2})\) with multiplicity \( r \), then the hyperplane with equation \( m_0X_0 + \cdots + m_{n-2}X_{n-2} - X_{n-1} + x = 0 \) intersects \( K \) in exactly \( r+1 \) points.

**Proof.** (1) For every \( X = b \), the hyperplane \( m_0X_0 + \cdots + m_{n-2}X_{n-2} - X_{n-1} + b = 0 \) contains at least one point of \( \bar{m} \). So \( X - b \) is a factor of \( H(X, \bar{m}) \).

If \( k < q-1 \), then \( H(X, \bar{m}) = X^{q+k} + h_1(\bar{m})X^{q+k-1} + \cdots + h_{q+k}(\bar{m}) = (X^k + h_1(\bar{m})X^{k-1} + \cdots + h_k(\bar{m}))(X^q - X) = f(X, \bar{m})(X^q - X) \).

Since \( H(X, \bar{m}) \) splits into linear factors over \( \mathbb{F}_q \), this is also true for \( f(X, \bar{m}) \).

(2) The multiplicity of a root \( X = x \) is the number of linear factors in the product defining \( H(X, \bar{m}) \) that vanish at \((x, \bar{m})\). This is the number of points of \( U \) lying on the hyperplane \( m_0X_0 + \cdots + m_{n-2}X_{n-2} - X_{n-1} + x = 0 \).

(3) The slope \((m_0, \ldots, m_{n-2})\) defines an \((n-2)\)-dimensional subspace at infinity not containing a point of \( K \). If the intersection multiplicity is \( r \), then \( x \) is an \((r+1)\)-fold root of \( H(X, \bar{m}) \). Hence, the result follows from (1) and (2).

**Remark 1.** By induction on the dimension, one can construct an \((n-2)\)-dimensional subspace \( \alpha \) skew to \( K \). Since \(|K| \leq 2q-1 \), \( K \) has a tangent hyperplane because all hyperplanes through \( \alpha \) must contain at least one point of \( K \).

Assume that \( X_n = 0 \) is a tangent hyperplane to \( K \) in the point \((0, \ldots, 0, 1, 0)\). The following theorem links the problem of minimality of the blocking set \( K \) to that of the problem of finding linear factors of the affine hypersurface \( C : f(X, \bar{X}) = 0 \).

**Theorem 2.** (1) If a point \( P = (a_0, \ldots, a_{n-1}) \in U \) is not essential, then the linear factor \( a_0X_0 + \cdots + a_{n-2}X_{n-2} - a_{n-1} + X \) divides \( f(X, \bar{X}) \).

(2) If the linear factor \( X + a_0X_0 + \cdots + a_{n-2}X_{n-2} - a_{n-1} \) divides \( f(X, \bar{X}) \), then \( P = (a_0, \ldots, a_{n-1}) \in U \) and this point is not essential.

**Proof.** (1) Consider an arbitrary slope \( \bar{m} = (m_0, \ldots, m_{n-2}) \). For this slope \( \bar{m} \), there are at least two points of \( K \) in the hyperplane \( m_0X_0 + \cdots + m_{n-2}X_{n-2} - X_{n-1} + b = 0 \) through \((a_0, \ldots, a_{n-1})\). Hence, by Theorem 1, the hyperplane \( \pi : a_0X_0 + \cdots + a_{n-2}X_{n-2} - a_{n-1} + X = 0 \) shares the point \((X, \bar{X}) = (a_{n-1} = (a_0m_0 + \cdots + a_{n-2}m_{n-2}), m_0, \ldots, m_{n-2}) \) with \( C \). Suppose that \( a_0X_0 + \cdots + a_{n-2}X_{n-2} - a_{n-1} + X \) does not divide \( f(X, \bar{X}) \), and let \( R \) be a point of the hyperplane \( \pi \) not lying in \( C \).

There are \( q^{n-2} + \cdots + q + 1 \) lines through \( R \) in the hyperplane \( \pi \), and none of them is contained in \( C \) since \( R \not\in C \). Since such lines contain at most \( k \) points of \( C \), \( \pi \) contains at most \( k(q^{n-2} + \cdots + q + 1) < (q-1)(q^{n-2} + \cdots + q + 1) = q^{n-1} - 1 \) points of \( C \). This is a contradiction since the number of possibilities for \( \bar{m} \) is \( q^{n-1} - 1 \), and each slope corresponds to a distinct point of \( \pi \cap C \).

(2) If this linear factor divides \( f(X, \bar{X}) \), then for all \( \bar{m} = (m_0, \ldots, m_{n-2}) \), the hyperplane with slope \( \bar{m} \) through \((a_0, \ldots, a_{n-1}) \) intersects \( U \) in at least two points (Theorem 1(3)). Here, we use that \( X_n = 0 \) is a tangent hyperplane to
that a \(k\)-blocking set \(B\) containment of \(\Pi\) in \(P\) is necessarily distinct) hyperplanes, it has dimension at least \(n\). By induction, it is possible to prove that there is a subspace \(\pi\) of dimension \(n - 2\) passing through \((a_0, \ldots, a_{n-1})\) and containing no points of \(K\) (cf. Remark \(\Pi\)). Consider all hyperplanes through \(\pi\). One of them passes through \((0, \ldots, 0, 1, 0)\); the other ones contain at least two points of \(K\). So \(|K| \geq 2q + 1\), which is false.

Hence, \(P = (a_0, \ldots, a_{n-1}) \in U\). Since all hyperplanes through \(P\), including those through \((0, \ldots, 0, 1, 0)\), contain at least two points of \(K\), the point \(P\) is not essential.

**Corollary 1.** A blocking set \(B\) of size smaller than \(2q\) in \(PG(n, q)\) is uniquely reducible to a minimal blocking set.

**Proof.** The non-essential points of \(B\) correspond to the linear factors over \(\mathbb{F}_q\) of the polynomial \(f(X, \bar{X})\), and this polynomial is uniquely reducible. \(\square\)

We will extend this unique reducibility property to blocking sets with respect to \(k\)-blocking sets.

**Theorem 3.** A \(k\)-blocking set in \(PG(n, q)\) of size smaller than \(2q^k\) is uniquely reducible to a minimal \(k\)-blocking set.

**Proof.** Embed \(PG(n, q)\) in \(PG(n, q^k)\). Let \(\pi\) be a hyperplane of \(PG(n, q^k)\). Let \(\pi^{i\ell} = (\langle x_0^{i\ell}, \ldots, x_n^{i\ell}\rangle)\) \(\forall (x_0, \ldots, x_n) \in \pi\). The space \(\pi \cap \pi^{1\ell} \cap \pi^{2\ell} \cdots \pi^{k-1}\) is the intersection of \(\pi\) with \(PG(n, q)\). Since it is the intersection of \(k\) (not necessarily distinct) hyperplanes, it has dimension at least \(n - k\). This implies that a \(k\)-blocking set \(B\) in \(PG(n, q)\) is also a 1-blocking set in \(PG(n, q^k)\). In Corollary \(\Pi\) it is proven that this latter blocking set is uniquely reducible to a minimal 1-blocking set \(B'\) in \(PG(n, q^k)\). Since every \((n - k)\)-dimensional space \(\Pi\) in \(PG(n, q)\) can be extended to a hyperplane in \(PG(n, q^k)\) that intersects \(PG(n, q)\) only in \(\Pi\) (straightforward counting), it is easy to see that the minimal blocking set \(B'\) in \(PG(n, q^k)\) is the unique minimal \(k\)-blocking set in \(PG(n, q)\) contained in \(B\). \(\square\)

## 3 The linear code generated by the incidence matrix of points and \(k\)-spaces in \(PG(n, q)\)

In this section, we investigate the codewords of small weight in the \(p\)-ary linear code generated by the incidence matrix of points and \(k\)-dimensional spaces, or for short \(k\)-spaces, in \(PG(n, q)\), \(q = p^h\), \(p\) prime, \(h \geq 1\).

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

**Proof.** For every subspace \(U_i\) of dimension at least \(n - k\) and every \(k\)-space \(K\), \((K, U_i) = 1\), hence \((K, U_1 - U_2) = 0\), so \(U_1 - U_2 \in C_k^+\). \(\square\)

Note that in Lemma \(\Pi\) \(\dim U_1 \neq \dim U_2\) is allowed.

**Lemma 2.** There exists a constant \(a \in \mathbb{F}_p\) such that \((c, U) = a\), for all subspaces \(U\) of dimension at least \(n - k\).
Proof. Lemma 1 yields $U_1 - U_2 \subseteq C_{k+1}^G$, for all subspaces $U_1, U_2$ with $\dim(U_i) > n - k$, hence $(c, U_1 - U_2) = 0$, so $(c, U_1) = (c, U_2)$.

Theorem 4. The support of a codeword $c \in C_k$ 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 $PG(n, q)$. Moreover, $c$ is a codeword taking only values from $\{0, a\}$, $a \in F_r^*$, and $\text{supp}(c)$ intersects every $(n - k)$-dimensional space in $1 \pmod{p}$ points.

Proof. If $c$ is a codeword with weight smaller than $2q^k$, and $(c, S) = a \neq 0$ for some $(n - k)$-space, then, according to Lemma 2, $(c, S) = a$ for all $(n - k)$-spaces $S$, so $\text{supp}(c)$ defines a $k$-blocking set $B$.

Suppose that every $(n - k)$-space contains at least two points of the $k$-blocking set $B$. Counting the number of incident pairs $(P \in B, (n - k)$-space through $P$) yields

$$|B| \left[ \begin{array}{c} n \\ n - k \end{array} \right] \geq \left[ \begin{array}{c} n + 1 \\ n - k + 1 \end{array} \right] 2.$$ 

Using $|B| < 2q^k$ gives a contradiction. So there is a point $R \in B$ on a tangent $(n - k)$-space. Since $c_R$ is equal to $a$, according to Lemma 2, $c_{R'} = a$ for every essential point $R'$ of $B$.

Suppose $B$ is not minimal, i.e. suppose there is a point $R \in B$ that is not essential. By induction on the dimension, we find an $(n - k - 1)$-dimensional space $\pi$ tangent to $B$ in $R$. If every $(n - k)$-space through $\pi$ contains two extra points of $B$, then $|B| > 2q^k$, a contradiction. Hence, there is an $(n - k)$-space $S$, containing besides $R$ only one extra point $R'$ of $\text{supp}(c)$, such that $(c, S) = c_R + c_{R'} = a$. But since $B$ is uniquely reducible to a minimal blocking set $B$ (see Theorem 3), $R'$ is essential, hence, $c_{R'} = a$. But this implies that $c_R = 0$, a contradiction. We conclude that the $k$-blocking set $B$ is minimal.

Since all the elements $R$ of $\text{supp}(c)$ have the coordinate value $c_R = a$, and since $(c, H) = a$ for every $(n - k)$-dimensional space $H$, necessarily $\text{supp}(c)$ intersects every $(n - k)$-dimensional space in $1 \pmod{p}$ points.

Theorem 5. Let $c$ be a codeword of $C_k(n, q)$, $q = p^h$, $p > 3$, with weight smaller than $2q^k$, for which $(c, S) \neq 0$ for some $(n - k)$-space $S$. Every subspace of $PG(n, q)$ that intersects $\text{supp}(c)$ in at least one point, intersects it in $1 \pmod{p}$ points.

Proof. It follows from Theorem 4 that a codeword $c$ of $C_k(n, q)$ with weight smaller than $2q^k$, for which $(c, S) \neq 0$ for some $(n - k)$-space $S$, is a minimal $k$-blocking set $B$ of $PG(n, q)$, intersecting any $(n - k)$-space in $1 \pmod{p}$ points. Using the same counting arguments as in the proof of Theorem 13 (with $E = p$), shows that

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

Substituting the values $|B| = 2q^k - 1$ and $|B| = 3(q^k + 1)/2$ in this inequality yields a contradiction for $p > 3$, hence $|B| < 3(q^k + 1)/2$. In [15, Theorem 2.7], it is proven that a subspace that intersects a minimal $k$-blocking set of size smaller than $3(q^k + 1)/2$ in at least 1 point, intersects it in $1 \pmod{p}$ points.
We emphasize that from now on, for some of the results, it is necessary to assume that \( k \geq n/2 \).

The following lemmas are extensions of the lemmas in [10]; we include the proofs to illustrate where the extra requirement \( k \geq n/2 \) arises.

**Lemma 3.** (See [10, Lemma 3]) Assume \( k \geq n/2 \). A codeword \( c \) of \( C_k \) is in \( C_k \cap C_k^\perp \) if and only if \( \langle c, U \rangle = 0 \) for all subspaces \( U \) with \( \dim(U) \geq n - k \).

**Proof.** Let \( c \) be a codeword of \( C_k \cap C_k^\perp \). Since \( c \in C_k^\perp \), \( \langle c, K \rangle = 0 \) for all \( k \)-spaces \( K \). Lemma 2 yields that \( \langle c, U \rangle = 0 \) for all subspaces \( U \) with dimension at least \( n - k \). The proof follows immediately.

**Remark 2.** If \( k < n/2 \), the lemma is false. Let \( c \) be \( K_1 - K_2 \), with \( K_1 \) and \( K_2 \) two skew-\( k \)-spaces. It is clear that \( c \in C_k \) and that \( \langle c, S \rangle = 0 \) for all \((n-k)\)-spaces \( S \). But \( c \notin C_k^\perp \) since \( \langle c, K_1 \rangle = 1 \). Note that the lemma is still valid in one direction: if \( c \in C_k \cap C_k^\perp \), then \( \langle c, S \rangle = 0 \) for all \((n-k)\)-spaces. For, let \( S \) be an \((n-k)\)-space, and let \( K_i, i = 1, \ldots, \theta_n - 2k \), be the \( \theta_n - 2k \) \( k \)-spaces through a fixed \((k-1)\)-space \( K' \) contained in \( S \). Since \( \langle c, K \rangle = 0 \) for all \( k \)-spaces \( K \), it follows that \( \langle c, S \rangle = \langle c, K_1 \setminus K' \rangle + \cdots + \langle c, K_{\theta_n - 2k} \setminus K' \rangle = 0 \).

**Lemma 4.** (See [10, Lemma 4]) For \( k \geq n/2 \),

\[
C_k \cap C_k^\perp = (K_1 - K_2)(K_1, K_2) \text{ distinct k-spaces in } PG(n, q).
\]

**Proof.** Put \( A = \{K_1 - K_2 \} \), \( K_1, K_2 \) distinct \( k \)-spaces in \( PG(n, q) \). Since \( k \geq n/2 \), two \( k \)-spaces \( K \) and \( K' \) of \( PG(n, q) \) intersect in \( 1 \) \( (mod p) \) points, so \( \langle K, K' \rangle = 1 \). Hence, \( A \subseteq C \cap C^\perp \), since \( \langle K, v \rangle = \langle K, K_1 \rangle - \langle K, K_2 \rangle = 1 - 1 = 0 \), for every \( k \)-space \( K \) of \( PG(n, q) \), and for every \( v = K_1 - K_2 \in A \).

Moreover, since \( \langle A \cup \{K_1\} \rangle \) contains each \( k \)-space, it follows that \( \dim(C) - 1 \leq \dim(\langle A \rangle) \leq \dim(C \cap C^\perp) \). The lemma now follows easily, since \( C \cap C^\perp \) is not equal to \( C \), as a \( k \)-space, with \( k \geq n/2 \), is not orthogonal to itself.

**Remark 3.** If \( k < n/2 \), the lemma is false, since \( K_1 - K_2 \notin C_k \cap C_k^\perp \), with \( K_1, K_2 \) two skew-\( k \)-spaces (see Remark 2).

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 non-trivial small linear blocking sets as codewords. The proofs are an extension of the proofs of Lemmas 7 and 8 of [10].

**Lemma 5.** For \( k \geq n/2 \), a vector \( v \in V(\theta_n, p) \) taking only values from \( \{0, a\} \), \( a \in F_p^* \), is contained in \( (C_k \cap C_k^\perp)^\perp \) if and only if \( |\text{supp}(v) \cap K| \) \( (mod p) \) is independent of the \( k \)-space \( K \) of \( PG(n, q) \).

**Remark 4.** If \( k < n/2 \), the lemma is false. Let \( v \) be a \( k \)-space. It follows that \( v \in (C_k \cap C_k^\perp)^\perp \) since \( v \in C_k = (C_k^\perp)^\perp \subseteq (C_k \cap C_k^\perp)^\perp \). But \( |\text{supp}(v) \cap K| = 0 \) \( (mod p) \) or \( 1 \) \( (mod p) \), depending on the \( k \)-space \( K \).

**Lemma 6.** Assume \( k \geq n/2 \) and let \( c, v \) be two vectors taking only values from \( \{0, a\} \), for some \( a \in F_p^* \), with \( c \in C_k \), \( v \in (C_k \cap C_k^\perp)^\perp \). If \( |\text{supp}(c) \cap K| = |\text{supp}(v) \cap K| \) \( (mod p) \) for every \( k \)-space \( K \), then \( |\text{supp}(c) \cap \text{supp}(v)| = |\text{supp}(c)| \) \( (mod p) \).
As mentioned in the introduction, we will eliminate all so-called non-trivial linear \( k \)-blocking sets as the support of a codeword of \( C \) of small weight. In order to define a linear \( k \)-blocking set, we introduce the notion of a Desarguesian spread.

By what is sometimes called “field reduction”, the points of \( \text{PG}(n, q) \), \( q = p^h \), \( p \) prime, \( h \geq 1 \), correspond to \((h - 1)\)-dimensional subspaces of \( \text{PG}(n + 1)h - 1, p \), since a point of \( \text{PG}(n, q) \) 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 \( \text{PG}(n + 1)h - 1, p \) 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 [11].

**Definition 3.** Let \( U \) be a subset of \( \text{PG}(n + 1)h - 1, p \) and let \( \mathcal{D} \) be a Desarguesian \((h - 1)\)-spread of \( \text{PG}(n + 1)h - 1, p \), then \( B(U) = \{ R \in \mathcal{D} | U \cap R \neq \emptyset \} \).

Analogously to the correspondence between the points of \( \text{PG}(n, q) \) and the elements of a Desarguesian spread \( \mathcal{D} \) in \( \text{PG}(n + 1)h - 1, p \), we obtain the correspondence between the lines of \( \text{PG}(n, q) \) and the \((2h - 1)\)-dimensional subspaces of \( \text{PG}(n + 1)h - 1, p \) spanned by two elements of \( \mathcal{D} \), and in general, we obtain the correspondence between the \((n - k)\)-spaces of \( \text{PG}(n, q) \) and the \(( (n - k + 1)h - 1)\)-dimensional subspaces of \( \text{PG}(n + 1)h - 1, p \) spanned by \( n - k + 1 \) elements of \( \mathcal{D} \). With this in mind, it is clear that any \( hk \)-dimensional subspace \( U \) of \( \text{PG}(h(n + 1) - 1, p) \) defines a \( k \)-blocking set \( B(U) \) in \( \text{PG}(n, q) \). A blocking set constructed in this way is called a linear \( k \)-blocking set. Linear \( k \)-blocking sets were first introduced by Lunardon [11], although there a different approach is used. For more on the approach explained here, we refer to [9].

The following lemmas, theorems, and remarks are proven in the same way as the authors do in [10].

**Lemma 7.** [10] **Lemma 9** If \( U \) is a subspace of \( \text{PG}(n + 1)h - 1, q \), then \( |B(U)| \equiv 1 \mod q \).

We put \( N = hk \) throughout the following results. We call a linear \( k \)-blocking set \( B \) of \( \text{PG}(n, q) \), \( q = p^h \), \( p \) prime, \( h \geq 1 \), defined by an \( N \)-dimensional space of \( \text{PG}(h(n + 1) - 1, p) \) a small linear \( k \)-blocking set.

**Lemma 8.** [10] **Lemma 10** Let \( U_N \) be an \( N \)-dimensional subspace of \( \text{PG}(h(n + 1) - 1, p) \). The number of spread elements of \( B(U_N) \) intersecting \( U_N \) in exactly one point is at least \( p_N - p_{N-2} - p_{N-3} - \ldots - p_{N-h+1} - p_{N-h-2} - \ldots - p_{N-2h+1} - p_{N-2h-2} - \ldots - p_{h+1} - p_{h-2} - \ldots - p \).

**Remark 5.** It follows from Lemma 8 that the number of spread elements of \( B(U_N) \) intersecting \( U_N \) in exactly one point is at least \( p_N - p_{N-1} + 1 \). We will use this weaker bound.

**Lemma 9.** [11] **Lemma 11** If there are \( p_N - p_{N-1} + 1 \) points \( R_i \) of a minimal \( k \)-blocking set \( B \) in \( \text{PG}(n, q) \), 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 \( k \)-space of \( \text{PG}(n, q) \).
Remark 6. It follows from the proof of Lemma 11 in [10] that it is sufficient to find \(k\) 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 \(k\)-space. Moreover, this bound is tight. If there are only \(k-1\) 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 \(\pi = \text{PG}(2, \sqrt{q})\) to the points of a \((k-2)\)-dimensional subspace of \(\text{PG}(n, q)\), skew to \(\pi\).

Lemma 10. [10] Lemma 12] Let \(U_{N-1}\) be a fixed \((N-1)\)-space in \(\text{PG}(h(n+1)−1, p)\) and let \(U_N\) be an arbitrary \(N\)-space containing \(U_{N-1}\). The set \(\mathcal{B}(U_N)\) is entirely determined by \(U_{N-1}\) and two elements \(R_1, R_2 \in \mathcal{B}(U_N)\setminus\mathcal{B}(U_{N-1})\).

Theorem 6. For every small linear \(k\)-blocking set \(B\), not defining a \(k\)-space in \(\text{PG}(n, p^h)\), there exists a small linear \(k\)-blocking set \(B'\) intersecting \(B\) in 2 \((\text{mod } p)\) points.

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

Choose a spread element \(R_1\) intersecting \(U_N\) in 1 point, say \(p_1\). The element \(R_1\) exists because of Lemma 5. Choose an \((N-1)\)-dimensional subspace \(U'_{N-1} \subseteq U_N\) not intersecting \(R_1\).

We can choose a spread element \(R_2 \in \mathcal{B}(U_{N-1})\) not lying in \(U_{N-1}\). Suppose that all elements of \(\mathcal{B}(U_{N-1})\) lie in \(U_{N-1}\). Then there are \(\theta_k\) elements in \(\mathcal{B}(U_{N-1})\) which intersect \(U_N\) in a point, so there are \(p^h\) elements in \(\mathcal{B}(U_N)\setminus\mathcal{B}(U_{N-1})\). Hence, there are in total \(\theta_k\) spread elements in \(\mathcal{B}(U_N)\), corresponding to a \(k\)-space in \(\text{PG}(n, p^h)\), since this is the only \(k\)-blocking set in \(\text{PG}(n, p^h)\) of size \(\theta_k\), a contradiction. So there is a spread element \(R_2 \in \mathcal{B}(U_{N-1})\) not contained in \(U_{N-1}\).

Suppose that for every \(R'_1\) with \(|R'_1 \cap U_N| = 1\), and \(R'_2\) in \(\mathcal{B}(U_{N-1})\), each spread element in \(\langle R'_1, R'_2 \rangle\) intersects \(U_N\). Then \(\mathcal{B}(U_N)\) defines a set of points in \(\text{PG}(n, q)\) such that every line through \(R'_1\) is tangent to \(B\) in \(R'_1\) or is entirely contained in \(B\). But Remark 5 and Lemma 9 imply that \(B\) is a \(k\)-space, a contradiction. So there is a spread element \(R'\), lying in a \((2h-1)\)-space spanned by two spread elements \(R_1, R_2, R_1 \in \mathcal{B}(U_N)\) is a point, and \(R_2 \in \mathcal{B}(U_{N-1})\) such that \(R'\) does not intersect \(U_N\).

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

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 \((1 \text{ mod } p)+1\) points in common (see Lemma 7).

If \(\mathcal{B}(U_N)\) contains another spread element \(R_3 \notin \mathcal{B}(U_{N-1})\), \(R_3 \neq R_1\), then Lemma 10 implies that \(\mathcal{B}(U_N) = \mathcal{B}(U'_N)\), contradicting \(R' \in \mathcal{B}(U'_N)\setminus\mathcal{B}(U_N)\). It follows that the \(k\)-blocking sets \(B\) and \(B'\) corresponding to \(U_N\) and \(U'_N\), resp., intersect in 2 \((\text{mod } p)\) points.

Using this, we exclude in Theorem 7 all small non-trivial linear \(k\)-blocking sets as codewords.

Theorem 7. Assume \(k \geq n/2\). If \(v\) is the incidence vector of a small non-trivial linear \(k\)-blocking set in \(\text{PG}(n, q)\), then \(v \notin C_k(n, q)\).
Proof. Let \( q = p^h, p \) prime, \( h \geq 1 \). We know that \( |\text{supp}(v)| \equiv 1 \pmod{p} \), since \( \text{supp}(v) \) corresponds to \( B(U) \) for some subspace \( U \) in \( \text{PG}(n+1)h - 1, p \), and \( |B(U)| = 1 \pmod{p} \) (see Lemma 7). We know from Theorem 8 that there exists a small linear \( k \)-blocking set \( w \) such that \( |\text{supp}(v) \cap \text{supp}(w)| \equiv 2 \pmod{p} \). Since \( |\text{supp}(w) \cap K| \equiv 1 \pmod{p} \) for every \( k \)-space \( K \) (Lemma 4), it follows that \( w \in (C_2 \cap C_k^\perp) \) (Lemma 5). Similarly, \( |\text{supp}(v) \cap K| \equiv 1 \pmod{p} \), for every \( k \)-space \( K \). Suppose that \( v \in C_k \). Lemma 6 implies that \( |\text{supp}(v) \cap \text{supp}(w)| \equiv |\text{supp}(v)| \pmod{p} \equiv 1 \pmod{p} \), a contradiction.

Corollary 2. For \( k \geq n/2 \), the only possible codewords \( c \) of \( C_k(n, q) \) of weight in \( \theta_k, 2q^k \], such that \( (c, S) \neq 0 \) for an \((n-k)\)-space \( S \), are scalar multiples of non-linear minimal \( k \)-blocking sets of \( \text{PG}(n, q) \).

Remark 7. In view of Corollary 8 it is important to mention the conjectures made in [13]. If these conjectures are true (i.e. all small minimal blocking sets are linear), then Corollary 8 eliminates all codewords of \( C_k(n, q) \backslash C_k(n, q)^\perp \) of weight in the interval \( \theta_k, 2q^k \].

For \( q = p \) prime and for \( q = p^2, p > 11 \) prime, we can exclude all such possible codewords. We rely on the following results.

Theorem 8. The only minimal \( k \)-blocking sets \( B \) in \( \text{PG}(n, p) \), with \( p \) prime and \( |B| < 2p^k \), such that every \((n-k)\)-space intersects \( B \) in \( 1 \pmod{p} \) points, are \( k \)-spaces of \( \text{PG}(n, p) \).

Proof. By induction on the dimension, it is possible to prove that if a line contains at least two points of \( B \), then this line is contained in \( B \). It now follows, by induction on the dimension, that \( B \) is a \( k \)-space.

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

Theorem 9. [13] A non-trivial minimal \((n-k)\)-blocking set of \( \text{PG}(n, p^2) \), \( p > 11, p \) prime, 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 \( \max{-1, n-2k-1} \leq t < n-k-1 \).

Theorems 8 and 9 together with Corollary 2 yield the following corollary.

Corollary 3. There are no codewords \( c \), with \( wt(c) \in \theta_k, 2q^k \], in \( C_k(n, q) \backslash C_k(n, q)^\perp \), with \( k \geq n/2 \), \( q \) prime or \( q = p^2, p > 11, p \) prime.

4 The dual code of \( C_k(n, q) \)

In this section, we consider codewords \( c \) in the dual code \( C_k(n, q)^\perp \) of \( C_k(n, q) \). The goal of this section is to find a lower bound on the minimum weight of the code \( C_k(n, q)^\perp \). Denote the minimum weight of a code \( C \) by \( d(C) \).

In the following lemmas, the problem of finding the minimum weight of \( C_k(n, q)^\perp \) is reduced to finding the minimum weight of \( C_1(n-k+1, q)^\perp \). Note that \( d(C_k(n, q)^\perp) \leq 2q^n-k \) since the difference of the incidence vectors of two \((n-k)\)-spaces of \( \text{PG}(n, q) \), intersecting in an \((n-k-1)\)-space, is a codeword of \( C_k(n, q)^\perp \).
Lemma 11. For each \( n \geq 2, \ 0 < k \leq n - 1 \), the following inequalities hold:
\[
d(C_k(n,q)^+) \geq d(C_{k-1}(n-1,q)^+) \geq \cdots \geq d(C_1(n-k+1,q)^+).
\]

Proof. Let \( c \) be a codeword of \( C_k(n,q)^+ \) of minimum weight, let \( R \) be a point of \( PG(n,q) \setminus \text{supp}(c) \), lying in a tangent line to \( \text{supp}(c) \), and let \( H \) be a hyperplane of \( PG(n,q) \) not containing \( R \). For each point \( P \in H \), define \( c'_P = \sum c_{P} \), with \( P \), the points of \( \text{supp}(c) \) on the line \( (R, P) \), and let \( c' \) denote the vector with coordinates \( c'_P, P \in H \). It easily follows that \( c' \in C_{k-1}(n-1,q)^+ \), and \( \text{supp}(c') \) is contained in the projection of \( \text{supp}(c) \) from the point \( R \) onto the hyperplane \( H \). Clearly, \( |\text{supp}(c')| \leq |\text{supp}(c)| \). Using this relation on a codeword \( c \) of minimum weight yields that \( d(C_{k-1}(n-1,q)^+) \leq d(C_k(n,q)^+) \). Continuing this process proves the statement.

Theorem 10. For each \( n \geq 2, \ 0 < k \leq n - 1 \), \( d(C_k(n,q)^+) = d(C_1(n-k+1,q)^+) \).

Proof. Embed \( \pi = PG(n-k+1,q) \) in \( PG(n,q) \), \( n > 2 \), and extend each codeword \( c \) of \( C_1(\pi)^+ \) to a vector \( c^{(n)} \) of \( V(\theta_n, p) \) by putting a zero at each point \( P \in PG(n,q) \setminus \pi \). Since the all one vector of \( V(\theta_n-k+1, p) \) is a codeword of \( C_1(n-k+1,q)^+ \), it follows that \( \sum_{P \in \pi} c_{P}^{(n)} = 0 \) for each \( c^{(n)} \). This implies that \( (c^{(n)}, K) = 0 \), for each \( k \)-space \( K \) of \( PG(n,q) \) which contains \( \pi \). If a \( k \)-space \( K \) of \( PG(n,q) \) does not contain \( \pi \), then \( (c^{(n)}, K \cap \pi) = 0 \), since \( K \cap \pi \) is a line or can be described as a pencil of lines through a given point, and \( (c, l) = 0 \) for each line \( l \) of \( \pi \). It follows that \( c^{(n)} \) is a codeword of \( C_k(n,q)^+ \) of weight equal to the weight of \( c \), which implies that \( d(C_k(n,q)^+) \leq d(C_1(n-k+1,q)^+) \).

Regarding Lemma 11 this yields that \( d(C_k(n,q)^+) = d(C_1(n-k+1,q)^+) \).

Lemma 12. Let \( B \) be a set of points in \( PG(n,q) \), with the property that those points of \( PG(n,q) \setminus B \) that are incident with a secant line to \( B \) are incident with no tangent lines to \( B \). If \( \dim(B) \geq n-k+2 \), then \( |B| \geq \theta_{n-k+1} \).

Proof. We first prove the following result.

Let \( P \) be a point in \( B \) and let \( L \) be a line through \( P \), lying in a plane \( \pi \) through \( P, R, S \), with \( R, S \in B \) and \( P \notin RS \), then \( L \) is a secant line to \( B \). If \( L \) is a tangent line to \( B \), then the point \( RS \cap L \) lies on a secant line and on a tangent line, a contradiction.

By induction, we prove that for each point \( P \in B \), there exists an \( r \)-space \( \pi_r \), with \( r \leq n-k+2 \), such that all lines through \( P \) in \( \pi_r \) are secant lines. The case \( r = 2 \) is already settled, so suppose that the statement is true for \( r, \ r < n-k+2 \). There is a point \( T \in B \notin \pi_r \) since \( \dim(B) \geq n-k+2 \). If \( M \) is a line through \( P \) in \( \langle \pi_r, T \rangle \), then \( \langle M, T \rangle \) intersects \( \pi_r \) in a line \( N \) through \( P \), which is a secant line according to the induction hypothesis. Hence, we find three non-collinear points in \( B \) in the plane \( \langle N, T \rangle \), so \( M \) is a secant line, so there is an \( (r+1) \)-space for which any line through \( P \) is a secant line. Counting the points of \( B \) on lines through \( P \) yields that \( |B| \geq \theta_{n-k+1} \).

Theorem 11. If \( c \) is a codeword of \( C_k(n,q)^+ \), \( n \geq 3 \), of minimal weight, then \( \text{supp}(c) \) is contained in an \( (n-k+1) \)-space of \( PG(n,q) \).

Proof. As already observed, we may assume that \( wt(c) \leq 2q^{n-k} \). Assume that \( \dim(\text{supp}(c)) \geq n-k+2 \). Using Lemma 12 we find a point \( R \notin \text{supp}(c) \) lying
on a tangent line to $\text{supp}(c)$ and lying on at least one secant line to $\text{supp}(c)$. It follows from Theorem 10 that

$$\text{wt}(c) = d(C_2(n, q)^\perp) = d(C_{k-1}(n-1, q)^\perp) = d(C_1(n-k+1, q)^\perp).$$

Let $c'$ be defined as in the proof of Lemma 11. Since $R$ lies on at least one secant line to $\text{supp}(c)$, $0 < \text{wt}(c') < \text{wt}(c)$. But this implies that $c'$ is a codeword of $C_{k-1}(n-1, q)^\perp$ satisfying $0 < \text{wt}(c') \leq \text{wt}(c) - 1 < d(C_{k-1}(n-1, q)^\perp)$, a contradiction.

In Theorem 11, we proved that finding the minimum weight of the code $C_k(n, q)^\perp$ is equivalent to finding the minimum weight of the code $C_1(n-k+1, q)^\perp$ of points and lines in $PG(n-k+1, q)$. Hence, we can use the following result due to Bagchi and Inamdar.

**Result 7.** [2, Proposition 2] When $q$ is prime, the minimum weight of the dual code $C_1(n, q)^\perp$ is $2q^{n-1}$. Moreover, the codewords of minimum weight are precisely the scalar multiples of the difference of two hyperplanes.

Using Result 7 together with Theorem 11 yields the following theorem.

**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.

When $q$ is not a prime, this result is false; we will present some counterexamples.

**Theorem 13.** Let $B$ be a minimal $(n-k)$-blocking set in $PG(n, q)$ of size $q^{n-k} + x$, with $x < (q^{n-k} + 1)/2$, such that there exists an $(n-k)$-space $T$ intersecting $B$ in $x$ points. The difference of the incidence vectors of $B$ and $T$ is a codeword of $C_k(n, q)^\perp$ with weight $2q^{n-k} + \theta_{n-k-1} - x$.

**Proof.** If $x < (q^{n-k} + 1)/2$, then $B$ is a small minimal $(n-k)$-blocking set, hence every $k$-space intersects $B$ in $1 \pmod{p}$ points (see 13). Let $c_1$ be the incidence vector of $B$ and let $c_2$ be the incidence vector of an $(n-k)$-space intersecting $B$ in $x$ points. Then $(c_1 - c_2, K) = (c_1, K) - (c_2, K) = 0$ for all $k$-spaces $K$, hence $c_1 - c_2$ is a codeword of $C_k(n, q)^\perp$, with weight $|B| + |T| - 2|B \cap T| = 2q^{n-k} + \theta_{n-k-1} - x$.

We can use this theorem to lower the upper bound on the possible minimum weight of codewords of $C_k(n, q)^\perp$. Put $V(n+1, q) = V(1, q) \times V(n-k, q) \times V(k, q) = F_q \times F_q^{n-k} \times F_q^k$ and put

$$B = \{(1, x, Tr(x))||x| \in F_q^{n-k}\} \cup \{(0, x, Tr(x))||x| \in F_q^{n-k}, x \neq 0\},$$

where $Tr$ is the trace function of $F_q^{n-k}$ to $F_p$, $p$ prime. The set $B$ is a subset of $F_q \times F_q^{n-k} \times F_q$ since $Tr(x) \in F_p \subset F_q, \forall x$. Moreover, $B$ is a linear subspace, inducing a blocking set of size $q^{n-k} + (q^{n-k} - 1)/(p-1)$, say $q^{n-k} + x$, w.r.t. the lines in $PG(F_q \times F_q^{n-k} \times F_q) \cong PG(n-k+1, q)$. Furthermore, there is an $(n-k)$-space $\pi$ such that $|B \cap \pi| = x$. Embedding $B$ in $PG(n, q)$ yields that $B$ is a minimal blocking set w.r.t. $k$-spaces, hence $B$ is a minimal $(n-k)$-blocking set such that there exists an $(n-k)$-space that intersects $B$ in $x$ points.

Using this, together with Theorem 13 yields the following corollary.
Corollary 4. For $q = p^h$, $p$ prime, $h \geq 1$,
\[
d(C_k(n,q)^\perp) \leq 2q^{n-k} + \theta_{n-k-1} - \frac{q^{n-k} - 1}{p-1}.
\]

In the case where $q$ is even, [2] gives an upper bound on the minimum weight.

Result 8. [6] Proposition 4] For $q$ even, the minimum weight of the code $C_1(n,q)^\perp$ is at most $q^{n-2}(q+2)$.

Result [8] together with Theorem [11] has the following corollary.

Corollary 5. For $q$ even, the minimum weight of $C_k(n,q)^\perp$ is at most $q^{n-k-1}(q+2)$.

Remark 8. It is easy to see that the minimum weight of $C_1(n-k+1,q)^\perp$, hence of $C_k(n,q)^\perp$, is at least $\theta_{n-k}$, every line through a point of supp($c$), with $c \in C_k(n-k+1,q)^\perp$, has to contain at least one other point of supp($c$). If $q$ is odd, Theorems [14] and [15] improve this lower bound. If $q$ is even, then $d(C_k(n,q)^\perp) > \theta_{n-k+1}$, for $n > 3$, since otherwise, supp($c$) would be a set $B$ of points in $PG(n-k+1,q)$, no three collinear, and [7, Theorem 27.4.6] states that $|B| \leq q^{n-k} - q^{n-k-1}/2 + 4q^{n-7/2}$, a contradiction. For $n = 3$ and $k = 1$, [6] Lemma 16.1.4] yields that $|B| \leq q^2 + 1$, a contradiction. For $n = 3$ and $k = 2$, it is easy to see that the minimum weight is $q+2$.

We will now prove a lower bound on the minimum weight of $C_k(n,q)^\perp$, $q$ not a prime, $q$ odd, by extending the bound of Sachar [12] on the minimum weight of $C_1(2,q)^\perp$.

Lemma 13. Suppose that there are $2m$ different non-zero symbols used in the codeword $c \in C_k(n,q)^\perp$, $q$ odd. Then
\[
wt(c) \geq \frac{4m}{2m+1} \theta_{n-k} + \frac{2m}{2m+1}.
\]

Proof. We use the same techniques as in the proof of Proposition 2.2 in [12]. Let $c$ be a codeword in $C_k^\perp$. Assume that $wt(c) \leq 2q^{n-k}$, and write $wt(c)$ as $\theta_{n-k} + x$.

Through every point $P$ of supp($c$), we can construct by induction on $s$, an $s$-space that only intersects supp($c$) in $P$, through a fixed $(s-1)$-space only intersecting supp($c$) in $P$, if $s \leq k - 1$, since the number of $s$-spaces through an $(s-1)$-space is $(q^{n-s+1} - 1)/(q-1) > 2q^{n-k}$ if $n-s > n-k$. So through every point $P$ of supp($c$), there is a $(k-1)$-space $K'$ which intersects supp($c$) only in the point $P$. For simplicity of notations, we use the terminology 2-secant for a $k$-space having two points of supp($c$). Let $K$ be a $(k-1)$-space intersecting supp($c$) in one point, for which the number of 2-secants through $K$ is minimal. We denote this number by $X$, or by $X_R$ in case $K$ intersects supp($c$) in the point $R$ of supp($c$).

Since $c$ is orthogonal to every $k$-space, if $K$ is a 2-secant through $R$ and $R'$, $R, R' \in supp(c)$, then $c_R + c_{R'} = 0$, so the symbol $c_{R'}$ occurs at least $X$ times in $c$. In fact, the number of occurrences of a certain non-zero symbol is always at least $X$.

The number of 2-secants through a given $(k-1)$-space intersecting supp($c$) in exactly one point, is at least $\theta_{n-k} + x + 1$. So it is easy to see that the number
of non-zero symbols used in $c$ must be even; let this number of non-zero symbols be $2m$.

This implies that

$$2m(\theta_{n-k} - x + 1) \leq \theta_{n-k} + x.$$  

Hence,

$$x \geq \frac{2m - 1}{2m + 1} \theta_{n-k} + \frac{2m}{2m + 1},$$

and

$$\text{wt}(c) \geq \frac{4m}{2m + 1} \theta_{n-k} + \frac{2m}{2m + 1}.$$  

\[ \square \]

**Theorem 14.** If $p \neq 2$, then $d(C_k(n, q^\perp)) \geq (4\theta_{n-k} + 2)/3$, $q = p^h$, $p$ prime, $h \geq 1$.

**Proof.** Let $c$ be a codeword of $C_k(n, q^\perp)$ with $\text{wt}(c) < (4\theta_{n-k} + 2)/3$. According to Lemma \ref{thm:lemma13} there is only one non-zero symbol used in $c$. Construct a $(k-1)$-space $\pi$ through a point $R$ of $\text{supp}(c)$ intersecting $\text{supp}(c)$ only in $R$. Then every $k$-space $K$ through $\pi$ has to contain at least $p - 1$ extra points of $\text{supp}(c)$ in order to get $(c, K) = 0$. But then $\text{wt}(c) \geq (p - 1)\theta_{n-k} + 1$, a contradiction.  

**Theorem 15.** The minimum weight of $C_k(n, q^\perp)$ is at least $(12\theta_{n-k} + 2)/7$ if $p = 7$, and at least $(12\theta_{n-k} + 6)/7$ if $p > 7$.

**Proof.** We use the same techniques as in the proof of Proposition 2.4 in \cite{12}. Let $c$ be a codeword of minimum weight of $C_k(n, q^\perp)$ and suppose that $\text{wt}(c) < (12\theta_{n-k} + 6)/7$. It follows from Lemma \ref{thm:lemma13} that there are at most four different non-zero symbols used in the codeword $c$. 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. Construct a $(k-1)$-space $\pi$ through a point $R$ of $\text{supp}(c)$, where $c_R = 1$ and $\pi \cap \text{supp}(c) = \{R\}$. Every $k$-space $\pi$ through $\pi$ contains at least a second point of $\text{supp}(c)$. At most $y$ of those $k$-spaces contain a point $R'$ of $\text{supp}(c)$ with $c_{R'} = -1$, so at least $\theta_{n-k} - y$ of those $k$-spaces only contain points $R'$ of $\text{supp}(c)$ with $c_{R'} = 1$. Since $(c, \pi) = 0$, such $k$-spaces contain 0 (mod $p$) points of $\text{supp}(c)$. This yields

$$\text{wt}(c) \geq (\theta_{n-k} - y)(p - 1) + y + 1.$$  

Using that $\text{wt}(c) < (12\theta_{n-k} + 2)/7$ implies that

$$p\theta_{n-k} - 7\theta_{n-k} - p + 7 < 0,$$

a contradiction if $p = 7$. Using that $\text{wt}(c) < (12\theta_{n-k} + 6)/7$ implies that

$$(p - 7)\theta_{n-k} + 7 - 3p < 0,$$

a contradiction if $p > 7$.

So we may assume that there are four non-zero symbols used in $c$, say 1, $-1$, $a$, $-a$. Using the same notations as in the proof of Lemma \ref{thm:lemma13} we see that

$$\text{wt}(c) \geq 4X_R.$$  

(1)
We call a $k$-space through one of the $(k - 1)$-spaces $K$, with $K \cap \text{supp}(c) = \{ R \}$, that has exactly two extra points of $\text{supp}(c)$, a 3-secant. Let $X_3$ denote the number of 3-secants through $K$, and let $X_w$ denote the number of $k$-spaces through $K$ that intersect $\text{supp}(c)$ in more than 3 points. We have the following equations:

\[ wt(c) \geq 1 + X_R + 2X_3 + 3X_w, \quad (2) \]
\[ \theta_{n-k} = X_R + X_3 + X_w. \quad (3) \]

Suppose first that there are no 3-secants, then substituting (3) in (1) and (2) gives

\[ wt(c) \geq 4\theta_{n-k} - 4X_w, \quad (4) \]
\[ wt(c) \geq 1 + \theta_{n-k} + 2X_w. \quad (5) \]

Eliminating $X_w$ using (4) and (5) gives

\[ 3wt(c) \geq 6\theta_{n-k} + 2, \]

a contradiction. This implies that $X_3 \neq 0$. Let $T$ be a 3-secant through $K$. The sum of the symbols used in $T$ has to be zero, hence

\[ (\ast) \quad 0 = 1 + 1 + a \text{ and } a = -2, \text{ or } 0 = 1 + a + a \text{ and } a = -1/2. \]

For each point $P$ with $c_P = -a$, the $k$-space through $K$ containing $P$ has to intersect $\text{supp}(c)$ in more than three points, since otherwise

\begin{align*}
1 - a - a &= 0 \text{ and } a = 1/2 \text{ or } \\
1 + 1 - a &= 0 \text{ and } a = 2.
\end{align*}

This contradicts ($\ast$) since $p > 5$ implies that $\{ 2, -2 \}$ cannot be the same as $\{ 1/2, -1/2 \}$. There are at least $X_R$ points with coefficient $-a$ and we see that they all must be on $k$-spaces contributing to $X_w$. Thus counting points again, we have

\[ wt(c) \geq 1 + X_R + 2X_3 + X_R = 1 + 2(\theta_{n-k} - X_3 - X_w) + 2X_3 = 1 + 2\theta_{n-k} - 2X_w. \quad (6) \]

Substituting (3) in (1) and (2) gives

\[ wt(c) \geq 4(\theta_{n-k} - X_3 - X_w) \quad (7) \]
\[ wt(c) \geq 1 + \theta_{n-k} + X_3 + 2X_w. \quad (8) \]

Eliminating $X_3$ and $X_w$ using (6), (7) and (8) yields

\[ 7wt(c) \geq 12\theta_{n-k} + 6 \]

and the proof is complete. \hfill \square

The second part of the following theorem is Corollary 5.7.5 of [1]. Here we give an alternative proof, similar to [2, Proposition 1].
Theorem 16. (1) The only possible codewords of weight in $[\theta_k, (12\theta_k + 6)/7]$ in $C_k(n, q)$, $k \geq n/2$, $q = p^h$, $p > 7$ prime, $h \geq 1$, are scalar multiples of incidence vectors of non-linear blocking sets.

(2) The minimum weight of $C_k(n, q)$ is $\theta_k$, and a codeword of weight $\theta_k$ is a scalar multiple of the incidence vector of a $k$-space.

Proof. (1) According to Lemma 2 there are two possibilities for a codeword $c \in C_k$ with $wt(c) < 2q^k$. Either $(c, S) \neq 0$ for every $(n-k)$-dimensional space $S$, and Corollary 2 yields that $c$ is a scalar multiple of the incidence vector of a non-linear blocking set, or $(c, S) = 0$ for all $(n-k)$-spaces $S$. But this implies that $c \in C_{n-k}$, which has weight at least $(12\theta_k + 6)/7$ (see Theorem 15).

(2) For the second statement, it is sufficient to use a result of Bose and Burton [4] that shows that the minimum weight of a $k$-blocking set in $PG(n, q)$ is equal to $\theta_k$, and that this minimum is reached if and only if the blocking set is a $k$-space. \qed

Remark 9. In view of Theorem 16 it is important to mention the conjectures made in [5]. If these conjectures are true (i.e. all small minimal blocking sets are linear), then Theorem 16 eliminates all codewords of $C_k(n, q)$ of weight in the interval $[\theta_k, (12\theta_k + 6)/7]$.

In the cases $q = p$ and $q = p^2$, with $p$ a prime, we can deduce more. Theorem 12, theorem 16, Theorem 8 and Theorem 9 yield the following theorems.

Theorem 17. There are no codewords with weight in $[\theta_k, 2q^k]$ in $C_k(n, q)$, $k \geq n/2$, where $q = p$ is prime.

Theorem 18. There are no codewords with weight in $[\theta_k, (12\theta_k + 6)/7]$ in $C_k(n, q)$, $k \geq n/2$, where $q = p^2$, $p > 11$ prime.

We now turn our attention to codewords in $C_k(n, q)$, $k \geq n/2$, $q = p^h$, $p$ prime, $h \geq 3$, with weight in $[\theta_k, (12\theta_k + 6)/7]$. We know from Theorem 15 that such codewords belong to $C_k(n, q) \setminus C_k(n, q)_\perp$, so they define minimal $k$-blocking sets $B$ intersecting every $(n-k)$-dimensional space in $1 \pmod{p}$ points (see Theorem 14, Lemma 3). Let $e$ be the maximal integer for which $B$ intersects every $(n-k)$-space in $1 \pmod{p^e}$ points. In [5] Corollary 5.2, it is proven that

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

We now derive an upper bound on $|B|$, based on [5] Theorem 5.3.

Theorem 19. Let $B$ be a minimal $k$-blocking set in $PG(n, q)$, $n \geq 2$, $q = p^h$, $p$ prime, $h \geq 1$, intersecting every $(n-k)$-dimensional space in $1 \pmod{p^e}$ points, with $e$ the maximal integer for which this is true. If $|B| \in [\theta_k, (12\theta_k + 6)/7]$ and that $p^e > 2$, then

$$|B| \leq q^k + \frac{2q^k}{p^e}.$$  

Proof. Put $E = p^e$ and let $\tau_{1+iE}$ be the number of $(n-k)$-dimensional spaces intersecting $B$ in $1+iE$ points. We count the number of $(n-k)$-dimensional spaces, the number of incident pairs $(R, \pi)$, with $R \in B$ and with $\pi$ an $(n-k)$-dimensional space through $R$, and the number of triples $(R, R', \pi)$, with $R$ and
$R'$ distinct points of $B$ and $\pi$ an $(n-k)$-dimensional space passing through $R$ and $R'$. This gives us the following formulas.

\[
\sum_{i \geq 0} \tau_{1+iE} = \frac{(q^{n+1} - 1)(q^n - 1)}{(q^{n-k+1} - 1)(q^{n-k} - 1)} \cdot X, \quad (9)
\]

\[
\sum_{i \geq 0} (1 + iE)\tau_{1+iE} = |B| \left( \frac{q^n - 1}{q^{n-k} - 1} \right) \cdot X, \quad (10)
\]

\[
\sum_{i \geq 0} (1 + iE)(1 + iE - 1)\tau_{1+iE} = |B|(|B| - 1) \cdot X, \quad (11)
\]

where

\[
X = \frac{(q^{n-1} - 1) \cdots (q^{k+1} - 1)}{(q^{n-k} - 1) \cdots (q - 1)}
\]

is the number of $(n-k)$-dimensional spaces through a line of $PG(n, q)$. Since \(\sum_{i \geq 0} i(i-1)E^2\tau_{1+iE} \geq 0\), we obtain

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

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

\[
|B| \leq q^k + \frac{2q^k}{E}.
\]

**Remark 10.** If $p^e > 4$, then $|B| < 3/2q^k$ in which case results of Sziklai prove that $e$ is a divisor of $h$ [13, Corollary 5.2].

We summarize the results on the minimum weight of $C_k(n, q)^{\perp}$, $k \geq n/2$, in the following table (with $\theta_n = (q^{n+1} - 1)/(q - 1)$).

| $p$   | $h$       | $d$                                      |
|-------|-----------|------------------------------------------|
| 2     | $(k, n) \neq (n-1, n)$ | $\theta_{n-k} + 1 < d \leq q^{n-k-1}(q + 2)$ |
| $p$   | 1         | $2p^{n-k}$                               |
| 2 < $p$ < 7 | $h > 1$    | $(4\theta_{n-k} + 2)/3 \leq d \leq 2q^{n-k} + \theta_{n-k-1} - \frac{q^{n-k-1}}{p^{p-1}}$ |
| 7     | $h > 1$   | $(12\theta_{n-k} + 2)/7 \leq d \leq 2q^{n-k} + \theta_{n-k-1} - \frac{q^{n-k-1}}{p^{p-1}}$ |
| $p$ > 7 | $h > 1$   | $(12\theta_{n-k} + 6)/7 \leq d \leq 2q^{n-k} + \theta_{n-k-1} - \frac{q^{n-k-1}}{p^{p-1}}$ |

**Table 1**: The minimum weight $d$ of $C_k(n, q)^{\perp}$, $k \geq n/2$, $q = p^h$, $p$ 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] A. Beutelspacher. Blocking sets and partial spreads in finite projective
spaces. Geom. Dedicata 9 (1980), 130–157.

[4] 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.

[5] S. Ferret, L. Storme, P. Sziklai, and Zs. Weiner. A $t$ (mod $p$) result on mul-
tiple $(n-k)$-blocking sets in $PG(n,q)$. Innov. Incidence Geom., to appear.

[6] J.W.P. Hirschfeld. Finite Projective Spaces of Three Dimensions. Oxford
University Press, Oxford (1985).

[7] J.W.P. Hirschfeld and J.A. Thas. General Galois Geometries. Oxford Uni-
versity Press, Oxford (1991).

[8] U. Heim. Proper blocking sets in projective spaces. Combinatorics (Rome
and Montesilvano, 1994). Discrete Math. 174 (1997), no. 1-3, 167–176.

[9] 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.

[10] M. Lavrauw, L. Storme, and 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., to appear.

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

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

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

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

[15] T. Szónyi and Zs. Weiner. Small blocking sets in higher dimensions. J.
Combin. Theory, Ser. A 95 (2001), 88–101.

[16] 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 [http://cage.ugent.be/~gvdvoorde]