Large weight code words in projective space codes

J. Limbupasiriporn L. Storme P. Vandendriessche[*]

February 29, 2012

Abstract

Recently, a large number of results have appeared on the small weights of the (dual) linear codes arising from finite projective spaces. We now focus on the large weights of these linear codes. For q even, this study for the code $C_k(n,q)^\perp$ reduces to the theory of minimal blocking sets with respect to the k-spaces of $\mathrm{PG}(n,q)$, odd-blocking the k-spaces. For q odd, in a lot of cases, the maximum weight of the code $C_k(n,q)^\perp$ is equal to $q^n+\cdots+q+1$, but some unexpected exceptions arise to this result. In particular, the maximum weight of the code $C_1(n,3)^\perp$ turns out to be 3^n+3^{n-1}. In general, the problem of whether the maximum weight of the code $C_k(n,q)^\perp$, with $q=3^h$ $(h\geq 1)$, is equal to $q^n+\cdots+q+1$, reduces to the problem of the existence of sets of points in $\mathrm{PG}(n,q)$ intersecting every k-space in $2 \pmod 3$ points.

Keywords: $2 \pmod 3$ sets, weights of code words, blocking sets, projective geometry codes

1 Introduction

Originally introduced by Gallager [7], low density parity check (LDPC) codes are used frequently these days due to their excellent empirical performance under belief-propagation/sum-product decoding. In some cases, their performance is even near to the Shannon limit [17]. In general, an LDPC code C is a linear block code defined by a sparse parity check matrix H; this is a matrix that contains a lot more 0s than nonzero symbols.

Codes from finite geometries have been shown to have excellent decoding performance for relatively short block lengths [11, 16, 18]. This led to a rediscovery and thorough study of finite geometry codes. Together with the bonus one gets from structural properties of the geometry (allowing a theoretical study of the code), finite geometry codes are generally considered to be the most interesting class of LDPC codes. Originally, only projective and affine spaces were studied, but lately several other constructions have been investigated, such as generalized quadrangles [10, 16], linear representations [19, 23, 24] and partial and semipartial geometries [9, 15].

[*]The third author is supported by a PhD fellowship of the Research Foundation - Flanders (FWO).

In particular, codes derived from projective spaces have been used in several high-end modern data transmission systems [3, 4]. In this paper, we will continue the study of the code words in the linear codes and the dual linear codes arising from finite projective spaces. A large number of results have already appeared on the small weights of the linear codes and dual linear codes arising from finite projective spaces [5, 6, 12, 13, 14].

We will focus on the large weights of the linear codes and dual linear codes arising from finite projective spaces. First of all, major differences between the results for q even and for q odd arise.

- For q even, the study of large weight code words in $C_k(n,q)^\perp$ reduces to the theory of minimal blocking sets with respect to the k-spaces of $\mathrm{PG}(n,q)$, odd-blocking the k-spaces. This shows that the maximum weight is equal to $q^n + \cdots + q^{n-k+1}$.
- For q odd, in a lot of cases, the maximum weight of the code $C_k(n,q)^\perp$ is equal to $q^n + \cdots + q + 1$, but some exceptions arise to this result. In particular, the maximum weight of the code $C_1(n,3)^\perp$ is equal to $3^n + 3^{n-1}$. In general, the problem of whether the maximum weight of the code $C_k(n,3)^\perp$ is equal to $3^n + \cdots + 3 + 1$ reduces to the problem of the existence of sets in $\mathrm{PG}(n,3)$ intersecting every k-space in 2 (mod 3) points. For $k > n/2$, such sets intersecting every k-space in 2 (mod 3) points trivially exist as the union of two disjoint $(n-k)$-spaces intersects every k-space in 2 (mod 3) points. For $k = 1$, such sets do not exist and for $2 \le k \le n/2$, the existence of such sets is an open problem.

2 Preliminaries

Notation 2.1. *We denote by* $\mathrm{PG}(n,q)$ *the* n*-dimensional projective space over the finite field* $\mathbb{F}_q$*. For* $n = 2$*, we call this a* projective plane *and write* $\mathrm{PG}(2,q)$*. The point set of* $\mathrm{PG}(n,q)$ *is denoted by* $\mathcal{P}$*.*

Definition 2.2. *A set* $S \subseteq \mathcal{P}$ *in* $\mathrm{PG}(n,q)$ *is called a* blocking set with respect to the k-spaces *if every* k*-space contains at least one point of* S*. If it is clear from the context what* k *is, we will simply call* S *a* blocking set*. If there is no* $s \in S$ *such that* $S \setminus \{s\}$ *is also a blocking set, then* S *is called* minimal*. If every* k*-space contains an odd number of points of* S*, then we say that* S *is* odd-blocking *the* k*-spaces.*

Definition 2.3. *An element of the vector space* $\mathbb{F}_p^{\mathcal{P}}$*, which consists of the mappings* $\mathcal{P} \to \mathbb{F}_p$*, can be seen as a vector of length* $|\mathcal{P}|$ *consisting of elements of* $\mathbb{F}_p$*. For a given subset* $\pi \subseteq \mathcal{P}$*, let* v^π *be its* characteristic function*; this is a* $\{0,1\}$ *mapping which is* 1 *for points in* π *and* 0 *for points outside of* π*. This vector* v^π *is called the* incidence vector *of* π*. Often, we will identify* π *with its incidence vector and write* π *instead of* v^π*. The support* $\mathrm{supp}(c)$ *of an element* $c \in \mathbb{F}_p^{\mathcal{P}}$ *is the set of points which is mapped to a nonzero element of* $\mathbb{F}_p$*.*

Notation 2.4. *The code* $C_k(n,q)$*,* $q = p^h$ *with* p *prime and* $h \ge 1$*, is the linear code over* $\mathbb{F}_p$ *generated by the incidence vectors of the* k*-dimensional subspaces of* $\mathrm{PG}(n,q)$*. Its dual, the code* $C_k(n,q)^\perp$*, is then the set of vectors* $c \in \mathbb{F}_p^{\mathcal{P}}$ *with* $c \cdot v^\pi = 0$ *(over* $\mathbb{F}_p$*) for each* k*-space* π*,* *where $\cdot$ denotes the standard inner product. In other words, a vector $c \in \mathbb{F}_p^{\mathcal{P}}$ is in $C_k(n,q)^\perp$ if and only if $\sum_{r\in\pi} c_r = 0$ for every k-space π of $\mathrm{PG}(n,q)$.*

Definition 2.5. *A $t \pmod p$ set with respect to the k-spaces of $\mathrm{PG}(n,q)$, with $q = p^h$ and p prime, is a set S which intersects every k-space of $\mathrm{PG}(n,q)$ in $t \pmod p$ points. By convention, we let $0 \le t \le p-1$.*

3 The case q even

In this section, we will study the code words of large weight in $C_k(n,q)^\perp$, when q is even. We are studying a binary code, hence a code word is uniquely identified by its support. In particular, the support $\mathrm{supp}(c)$ of a code word $c \in C_k(n,q)^\perp$ of large weight corresponds to a large set of points, intersecting every k-space in an even number of points. Since every k-space contains an odd number of points, the complement S of this set is a small set which intersects every k-space in an odd number of points. In particular, S contains at least one point of every k-space, hence it is a blocking set with respect to the k-spaces.

Theorem 3.1. *The maximum weight of $C_k(n,q)^\perp$, q even, is $q^n + \dots + q^{n-k+1}$, and all the code words of this weight are the incidence vector of the complement of an $(n-k)$-space of $\mathrm{PG}(n,q)$.*

Proof. The incidence vector of the complement of any $(n-k)$-space π is a code word of weight $q^n + \dots + q^{n-k+1}$ of $C_k(n,q)^\perp$: since each projective k-space intersects this $(n-k)$-space in a nonempty projective subspace, this intersection contains $1 \pmod q$ points, and hence its complement in π contains $0 \pmod q$ points. Therefore, the maximum weight of $C_k(n,q)^\perp$ is at least $q^n + \dots + q^{n-k+1}$.

Since the complement S of the support of a code word of $C_k(n,q)^\perp$ is a blocking set with respect to the k-spaces, we have $|S| \ge q^{n-k} + \dots + q + 1$ by the Bose-Burton theorem [2], and if equality occurs, then S is an $(n-k)$-space. This shows that the bound is sharp, and it characterizes the code words of weight $q^n + \dots + q^{n-k+1}$. □

The Bose-Burton result on blocking sets is crucial in the proof of Theorem 3.1, and this is not the only place where we will run into a connection with blocking sets. The following theorem improves [22, Theorem 3.1] for $p = 2$, for the special case of odd-blocking sets.

Theorem 3.2. *Let S be a set of projective points, odd-blocking the k-spaces of $\mathrm{PG}(n,q)$, q even. If $|S| \le 2(q^{n-k} + q^{n-k-1} + \dots + q + 1)$, then S is a minimal blocking set.*

Proof. Assume by contraposition that S is not minimal, i.e. there is a point $p \in S$ such that $S \setminus \{p\}$ still blocks the k-spaces. Hence, every k-space through p is blocked by S in at least 2 points. But it is also blocked by an odd number of points of S, so every k-space through p contains at least 3 points of S.

Now, there are two cases:

- either there exists a $(k-1)$-space π through p which contains no other points of S. Every k-space through π contains by assumption at least two other points of S, hence each of the $q^{n-k}+q^{n-k-1}+\cdots+q^2+q+1$ different k-spaces through π contains at least 2 points of S outside of π. Since two such k-spaces only intersect in π, this means that $|S| \geq 1+2(q^{n-k}+q^{n-k-1}+\cdots+q^2+q+1)$, a contradiction.

- either every $(k-1)$-space through p contains at least one other point of S. Let now i be the largest integer (with necessarily $i < k-1$) for which there exists an i-space through p which contains no other points of S. Such an integer i must exist, since $i=0$ clearly has this property and $i=k-1$ does not. Let now π be such an i-space through p, containing no other points of S. Because of the maximality of i, each of the $q^{n-i-1}+q^{n-i-2}+\cdots+q^2+q+1$ different $(i+1)$-spaces through π must again contain at least one other point of S. Since two such $(i+1)$-spaces only intersect in π, this means that $|S| \geq 1+(q^{n-i-1}+q^{n-i-2}+\cdots+q^2+q+1)$. Since $i \leq k-2$ and $q \geq 2$, this implies that

$$\begin{array}{rcl} |S| & \geq & 1+(q^{n-i-1}+q^{n-i-2}+\cdots+q^2+q+1) \\ & \geq & 1+(q^{n-k+1}+q^{n-k}+\cdots+q^2+q+1) \\ & \geq & 1+(2q^{n-k}+2q^{n-k-1}+\cdots+2q+2+1) \\ & > & 2(q^{n-k}+q^{n-k-1}+\cdots+q+1), \end{array}$$

  a contradiction.

Both cases lead to a contradiction and hence S must be minimal. □

The preceding theorem implies that the study of the code words in $C_k(n,q)^\perp$, q even, of weight larger than or equal to $q^n+\cdots+q^{n-k+1}-q^{n-k}-\cdots-q-1$ is reduced to the study of the minimal blocking sets with respect to the k-spaces of $\mathrm{PG}(n,q)$, odd-blocking the k-spaces. Some important results on minimal blocking sets with respect to the k-spaces of $\mathrm{PG}(n,q)$ were obtained by Szőnyi [21], Szőnyi and Weiner [22], and Sziklai [20].

Let $S(q)$ be the set of possible sizes of minimal blocking sets in $\mathrm{PG}(2,q)$ with cardinality smaller than $\frac{3}{2}(q+1)$, then [20, Corollary 5.1 and 5.2] yield the following summarizing theorem for q even.

Theorem 3.3. *Let c be a code word of the code $C_k(n,q)^\perp$, q even, of weight larger than $q^n+\cdots+q+1-\sqrt{2}q^{n-k}$. Then the weight of c equals $q^n+\cdots+q+1-x$, with $x \in S(q^{n-k})$. Moreover, c is the incidence vector of the complement of a small minimal blocking set, odd-blocking the k-spaces.*

Regarding larger minimal blocking sets with respect to the k-spaces of $\mathrm{PG}(n,q)$, not many results are known. Here, there are still many open problems, including results on the cardinalities of these minimal blocking sets.

4 Large weight constructions

From now on, we will assume that q is odd. We consider the p-ary linear code of points and k-spaces of $\mathrm{PG}(n,q)$, with $q = p^h$ and with $p > 2$ prime. A code word of the code $C_k(n,q)^\perp$ corresponds to a map φ from the set of projective points to $\mathbb{F}_p$, such that for each k-space Π we have $\sum_{p\in\Pi}\varphi(p) = 0$ as an element of $\mathbb{F}_p$. The image of a point under φ is called the coefficient of that point.

In this section, we try to determine when the maximum possible Hamming weight of this code is attained, i.e. when there exist code words of weight $q^n + \cdots + q + 1$. In case this does not work, we provide constructions to attain sharp lower bounds on the maximum weight of these codes. Surprisingly, we will again find several strong links with small minimal blocking sets. We begin with a useful lemma.

Lemma 4.1. *Let $\{B_i\}_{i\in I}$ be a family of $1 \pmod p$ sets with respect to the k-spaces of $\mathrm{PG}(n,q)$, such that no point is contained in more than $p-1$ of these sets. Then the maximum weight of $C_k(n,q)^\perp$ is at least*

$$q^n + q^{n-1} + \cdots + q + 1 - \left|\bigcap_{i\in I} B_i\right|.$$

Proof. For each $i \in I$, define $c^{(i)}$ to be the incidence vector of the complement of B_i. Since B_i intersects every k-space in $1 \pmod p$ points, and every k-space has $1 \pmod p$ points itself, the complement of B_i intersects every k-space in $0 \pmod p$ points and hence $c^{(i)}$ is a code word of $C_k(n,q)^\perp$.

Now, $c := \sum_{i=0}^{p-2} c^{(i)}$ is a code word of $C_k(n,q)^\perp$, of which we will now determine its weight. The coefficient in c of each point consists of a sum of $p-1$ elements, and each element is either 0 or 1. Hence, a zero coefficient in the sum c cannot be obtained by summing up ones. Therefore, if a point has zero coefficient in the sum c, it has to be zero in each $c^{(i)}$, which means that it should lie in each of the B_i. Therefore, the weight of c is exactly $q^n + q^{n-1} + \cdots + q + 1 - \left|\bigcap_{i\in I} B_i\right|$, as claimed. □

The easiest example of a small minimal blocking set with respect to the k-spaces, is an m-space with $m \geq n-k$. This yields us the following lower bounds on the maximum weight.

Theorem 4.2. *The maximum weight of $C_k(n,q)^\perp$, $q = p^h$, p prime, $h \geq 1$, is*

- *exactly $q^n + q^{n-1} + \cdots + q + 1$ if $(n+1)/k \leq p-1$,*
- *at least $q^n + q^{n-1} + \cdots + q^{n-k(p-1)+1}$ if $(n+1)/k > p-1$.*

Proof. Let $m := \left\lceil \frac{n+1}{k} \right\rceil$. Define as follows subspaces $H_0, \ldots, H_{m-1}$ of $\mathrm{PG}(n,q)$. For $i = 0, 1, \ldots, m-2$, let H_i be the $(n-k)$-space with equations $X_{ik} = X_{ik+1} = \cdots = X_{(i+1)k-1} = 0$. Let H_{m-1} be the $k(m-1)$-space with equations $X_{k(m-1)} = X_{k(m-1)+1} = \cdots = X_n = 0$.

If $(n+1)/k \leq p-1$, then $S := \{H_0, \ldots, H_{m-1}\}$ is a set of $1 \pmod{p}$ sets with respect to the k-spaces. The intersection of all sets in S is trivial, because the coordinates $(X_0, \ldots, X_n)$ of any point in $\bigcap_{i=0}^{m-1} H_i$ must have $X_0 = \cdots = X_{k-1} = 0$, $X_k = \cdots = X_{2k-1} = 0$, …, $X_{k(m-1)} = X_{k(m-1)+1} = \cdots = X_n = 0$ and hence it is the zero vector, which is not a point of $\mathrm{PG}(n,q)$. Since there are only $\lceil (n+1)/k \rceil \leq p-1$ sets in S, each point is indeed contained in at most $p-1$ sets of S. Lemma 4.1 yields the desired result.

If $(n+1)/k > p-1$, then $S := \{H_0, \ldots, H_{p-2}\}$ is a set of $1 \pmod{p}$ sets with respect to the k-spaces. Since S only contains $p-1$ sets, each point is contained in at most $p-1$ sets of S. The intersection of all sets in S consists of all points $(X_0, \ldots, X_n)$ for which $X_0 = \cdots = X_{k-1} = 0$, $X_k = \cdots = X_{2k-1} = 0$, …, $X_{k(p-2)} = \cdots = X_{k(p-1)-1} = 0$. This is a projective subspace of dimension $n - k(p-1)$ in $\mathrm{PG}(n,q)$, which has $q^{n-k(p-1)} + q^{n-k(p-1)-1} + \cdots + q + 1$ points. Lemma 4.1 yields the desired result. □

If $(n+1)/k \leq p-1$, then a maximum weight of $q^n + q^{n-1} + \cdots + q + 1$ is reached. If $(n+1)/k > p-1$, the contrary is not necessarily true. For example, we have the following sufficient condition for the maximum weight $q^n + q^{n-1} + \cdots + q + 1$ to appear, based on $t \pmod{p}$ sets.

Theorem 4.3. *If a $t \pmod{p}$ set exists with respect to the k-spaces of $\mathrm{PG}(n,q)$, with $t \not\equiv 0, 1 \pmod{p}$, then the maximum weight of $C_k(n,q)^\perp$ is $q^n + q^{n-1} + \cdots + q + 1$.*

Proof. Let S be such a set and let T be its complement. Assign coefficient 1 to all points in T and assign coefficient $1 - t^{-1}$ to all points in S, where the inversion of t is done over $\mathbb{F}_p$. We will show that this defines a code word of $C_k(n,q)^\perp$. Since we are given that every k-space intersects S in $t \pmod{p}$ points and T in $p+1-t \pmod{p}$ points, the sum of all coefficients in every k-space is $t \cdot (1 - t^{-1}) + (p+1-t) \cdot 1 \equiv 0 \pmod{p}$, so c is a code word of $C_k(n,q)^\perp$. Since 1 and $1 - t^{-1}$ are nonzero elements of $\mathbb{F}_p$, c has full weight, as claimed. □

Sometimes the existence of $t \pmod{p}$ sets is trivial, for example when $k \geq \frac{n+1}{2}$.

Corollary 4.4. *If $k \geq \frac{n+1}{2}$, two skew $(n-k)$-spaces exist in $\mathrm{PG}(n,q)$ and hence both Theorem 4.2 and and Theorem 4.3 show that a maximum weight of $q^n + q^{n-1} + \cdots + q + 1$ is attained for $C_k(n,q)^\perp$.*

In other cases it is however not at all obvious. Even in the planar case (where $n = 2$ and $k = 1$), this is not trivial. Since $\frac{n+1}{k} = 3$, the maximum weight is attained for $p \geq 5$ by Theorem 4.2, but for $p = 3$, no such easy construction is known.

Lemma 4.5. *If $q = 3^h$, where $h > 1$, then there exists a non-square element in $\mathbb{F}_q \setminus \{x^2 - x | x \in \mathbb{F}_q\}$.*

Proof. Let f be the mapping of $\mathbb{F}_q$ into itself defined by $f(x) = x^2 - x$ for all $x \in \mathbb{F}_q$. Then $f(1-x) = (1-x)^2 - (1-x) = x^2 - x$ for all $x \in \mathbb{F}_q$, so we have $f(x) = f(1-x)$ for all $x \in \mathbb{F}_q$. Observe that for any $x \in \mathbb{F}_q$, $1 - x = x$ if and only if $2x = 1$, i.e. if and only if $x = 2$. Thus the cardinality of $Im(f)$ is $\frac{q-1}{2} + 1 = \frac{q+1}{2}$.

We will show that there exists an element in $\mathbb{F}_q \setminus Im(f)$ which is non-square. Suppose, to the contrary, that every non-square element of $\mathbb{F}_q$ is in $Im(f)$. Then $Im(f)$ is the set of zero and all non-square elements of $\mathbb{F}_q$. Let $x \in \mathbb{F}_q \setminus \mathbb{F}_3$ and $y = 2 - x$. Then

$$\begin{aligned} f(x)f(y) &= (x^2-x)(y^2-y) = (xy)^2 - xy(y+x) + xy \\ &= (xy)^2 - 2xy + xy = (xy)^2 - xy \\ &= f(xy). \end{aligned}$$

Since both $f(x)$ and $f(y)$ are non-square, it follows that $f(x) = \omega^i$ and $f(y) = \omega^j$ for some odd integers i and j, where ω is a primitive element for $\mathbb{F}_q$. Hence, $i + j$ is even and $f(xy) = f(x)f(y) = \omega^{i+j}$ is square, contradiction. □

Lemma 4.6 ([8, Lemma 13.8]). *In* $\mathrm{PG}(2,q)$, *where* $q = 3^h$, *the set* $\{(1,x,x^3) \mid x \in \mathbb{F}_q\} \cup \{(0,x,x^3) \mid x \in \mathbb{F}_q \setminus \{0\}\}$ *is a minimal blocking set which intersects every line in* $1 \pmod 3$ *points.*

Theorem 4.7. *If* $q = 3^h$, *where* $h > 1$, *then* $\mathrm{PG}(2,q)$ *contains a* $2 \pmod 3$ *set of size* $3q-1$.

Proof. By Lemma 4.5, there exists a non-square element b in $\mathbb{F}_q \setminus \{x^2 - x \mid x \in \mathbb{F}_q\}$. Consider the mapping $\varphi : (x,y,z) \mapsto (z, y+bx, x)$ from $\mathrm{PG}(2,q)$ into itself. This is a collineation of $\mathrm{PG}(2,q)$.

Now let

$$S = \{(1,x,x^3) \mid x \in \mathbb{F}_q\} \cup \{(0,x,x^3) \mid x \in \mathbb{F}_q \setminus \{0\}\}.$$

Clearly, all points in the first set are distinct and disjoint from the second set, hence this part contains q points of S. For the second part, points may coincide since projective points are only defined up to a nonzero scalar multiple. In particular, one has $(0,x,x^3) = (0,y,y^3)$ if and only if $\frac{x^3}{x} = \frac{y^3}{y}$, hence if and only if $\left(\frac{x}{y}\right)^2 = 1$. Therefore, each point appears twice in this second set, making the total cardinality of S equal to $q + \frac{q-1}{2}$.

By Theorem 4.6, S is a blocking set intersecting every line in $1 \pmod 3$ points, and hence, so is $T = \varphi(S)$. Note that

$$T = \{(x^3, x+b, 1) \mid x \in \mathbb{F}_q\} \cup \{(x^3, x, 0) \mid x \in \mathbb{F}_q \setminus \{0\}\}.$$

Now we look at the union of S and T. If S and T are disjoint, then the union of these sets gives a $2 \pmod 3$ set of cardinality $2\left(q + \frac{q-1}{2}\right) = 3q-1$. We will show that S and T are disjoint. Suppose by contradiction that there exists a point P in the intersection of S and T. Clearly, this is impossible in all but the following cases.

- If P belongs to the first sets of S and T, i.e. $P = (1,x,x^3) = (y^3, y+b, 1)$ for some $x, y \in \mathbb{F}_q \setminus \{0\}$, then since $(1,x,x^3) = (y^3, xy^3, (xy)^3)$, we obtain the equation $xy^3 = y+b$ and $(xy)^3 = 1$, and the latter implies that $xy = 1$, which gives $y^2 = y + b$ or $b = y^2 - y$, a contradiction.
- If P belongs to the second set of S and to the first set of T with zero element in $\mathbb{F}_q$, i.e. $P = (0,x,x^3) = (0,b,1)$ for some $x \in \mathbb{F}_q \setminus \{0\}$, then since $(0,x,x^3) = (0,x^{-2},1)$, it follows that $b = x^{-2}$ which contradicts the fact that b is non-square.

Hence, S and T are disjoint, and the result follows. □

So, the plane code $C_1(2,q)^\perp$, with $q > 3$ odd, indeed has maximum weight q^2+q+1.

5 Upper bounds on the maximum weight

In this section, we will provide some upper bounds on the maximum weight. From the preceding section, one might get the feeling that the study for q odd is not really interesting, as one always attains the maximum weight, or gets at least very close to the maximum weight. However, this is not correct, as we will now reveal upper bounds which show quite a gap relative to $q^n+q^{n-1}+\cdots+q+1$.

First we show that if the characteristic of the field is 3, then the converse of Theorem 4.3 holds as well.

Theorem 5.1. *If $p=3$, the maximum weight $q^n+q^{n-1}+\cdots+q+1$ is attained in $C_k(n,q)^\perp$ if and only if there exists a $2 \pmod 3$ set with respect to the k-spaces of $\mathrm{PG}(n,q)$.*

Proof. The 'if' part follows from Theorem 4.3. For the 'only if' part, let c be a code word of weight $q^n+q^{n-1}+\cdots+q+1$ in $C_k(n,q)^\perp$. Let S be the set of points with coefficient 1 in c and let T be its complement, i.e. the set of points with coefficient 2 in c. Now fix an arbitrary k-space π. Let s and t be respectively the number of points of S and T in π. Clearly, $s+t \equiv 1 \pmod p$. Moreover, since c is a code word, $s+2t \equiv 0 \pmod p$. Solving this, we get $s \equiv t \equiv 2 \pmod p$, i.e., S and T are $2 \pmod 3$ sets with respect to the k-spaces of $\mathrm{PG}(n,q)$. □

For $q=3$, this yields a negative result.

Lemma 5.2. *The projective plane $\mathrm{PG}(2,3)$ does not have a $2 \pmod 3$ set with respect to the lines.*

Proof. Let $q=3$. Clearly, a $2 \pmod 3$ set S has two points on every line. In particular, let $r \notin S$, then each of the 4 lines through r contains two points of S, i.e. $|S|=8$. However, the complement T of S is also a $2 \pmod 3$ set, i.e. $|T|=8$. But there are only 13 points in this plane, a contradiction. □

Corollary 5.3. *The linear code $C_1(2,3)^\perp$ does not have code words of weight $q^2+q+1=13$. Hence, the maximum weight of $C_1(2,3)^\perp$ is q^2+q. In other words, the second bound from Theorem 4.2 is sharp for $q=3, n=2, k=1$.*

Now we prove a reduction lemma. Again, it reveals a link with blocking sets and makes use of the Bose-Burton Theorem [2]. It will greatly extend the gap between the actual maximum weight and $q^n+q^{n-1}+\cdots+q+1$ in some cases.

Lemma 5.4. *If there exists an integer m with $k \leq m \leq n$, for which $C_k(m,q)^\perp$ does not attain full weight, then $C_k(n,q)^\perp$ has maximum weight at most $q^n + \cdots + q^{n-m+1}$.*

Proof. Let c be a code word of maximum weight in $C_k(n,q)^\perp$. Let S be the set of points on which c is zero, i.e. S is the complement of supp(c). If there exists an m-space Π disjoint from S, then all points in Π correspond to nonzero positions in the code word. Since $\sum_{r\in\pi} c_r = 0$ for every k-space π of $\mathrm{PG}(n,q)$, this also holds for all k-spaces $\pi \subseteq \Pi$. Since the positions corresponding to points outside of Π are not relevant for these equations, they still hold when replacing them by 0, hence the restriction of c to the positions in Π is a code word of $C_k(m,q)^\perp$. But $C_k(m,q)^\perp$ does not attain full weight; this contradicts our assumption.

Hence, each m-space contains at least one point of S, which means that S is a blocking set with respect to the m-spaces of $\mathrm{PG}(n,q)$, and so, by the Bose-Burton Theorem [2], $|S|$ has at least the size of an $(n-m)$-space, i.e. $|S| \geq q^{n-m} + \cdots + q + 1$. Hence, the maximum weight of $C_k(n,q)^\perp$ is at most $q^n + \cdots + q^{n-m+1}$. □

Combining Corollary 5.3 and Lemma 5.4, with $q = 3$, $m = 2$ and $k = 1$, we get the following result.

Theorem 5.5. *The maximum weight in $C_1(n,3)^\perp$ is $3^n + 3^{n-1}$.*

This is far below the expected value $3^n + 3^{n-1} + \cdots + 3 + 1$. The maximum weight of $C_k(n,3)^\perp$ is still an open problem for $1 < k < \frac{n+1}{2}$.

Remark 5.6. *The preceding results show that the study of $2 \pmod 3$ sets in $\mathrm{PG}(n,q)$, $q = 3^h$, plays a crucial role for the investigation of the large weight code words of the code $C_k(n,q)^\perp$. We therefore propose to investigate the existence problem of these $2 \pmod 3$ sets in the cases not discussed in this article.*

An other interesting problem is to determine the exact maximum weight of the codes $C_k(n,q)^\perp$, q odd, not yet discussed in Theorem 4.2 and in the remaining theorems of this article. A way to prove that the maximum weight of $C_k(n,q)^\perp$, q odd, is equal to $q^n + \cdots + q + 1$ is to prove the existence of $t \pmod p$ sets with respect to the k-spaces of $\mathrm{PG}(n,q)$, with $t \not\equiv 0, 1 \pmod p$, as indicated in Theorem 4.3. It is unknown whether one can ever obtain a larger weight than with the construction in Lemma 4.1.

Acknowledgment. The first author thanks the Department of Mathematics at Ghent University for their hospitality. The authors also wish to thank Dr. G. Van de Voorde for her suggestions which improved a first version of this article.

References

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

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

[3] I.B. Djordjevic and B.V. Vasic, Projective geometry LDPC codes for ultralong-haul WDM high-speed transmission. *IEEE Photonics Technology Letters* **15** (2003), 784–786.

[4] I.B. Djordjevic, S. Sankaranarayanan and B.V. Vasic, Projective-Plane Iteratively Decodable Block Codes for WDM High-Speed Long-Haul Transmission Systems. *J. Lightwave Technol.* **22** (2004), 695–702.

[5] V. Fack, Sz. L. Fancsali, L. Storme, G. Van de Voorde and J. Winne, Small weight codewords in the codes arising from Desarguesian projective planes. *Des. Codes Cryptogr.* **46** (2008), 25–43.

[6] A. Gács, T. Szőnyi and Zs. Weiner, Private communication (2009).

[7] R.G. Gallager, Low density parity check codes. *IRE Trans. Inform. Theory* **8** (1962), 21–28.

[8] J.W.P. Hirschfeld, Projective Geometries over Finite Fields, Second Edition. *Oxford University Press*, 1998.

[9] S.J. Johnson and S.R. Weller, Codes for Iterative Decoding From Partial Geometries. *IEEE Trans. Commun.* **52** (2004), 236–243.

[10] J.-L. Kim, K.E. Mellinger and L. Storme, Small weight codewords in LDPC codes defined by (dual) classical generalized quadrangles. *Des. Codes Cryptogr.* **42** (2007), 73–92.

[11] Y. Kou, S. Lin and M.P.C. Fossorier, Low-density parity-check codes based on finite geometries: a rediscovery and new results. *IEEE Trans. Inform. Theory* **47** (2001), 2711–2736.

[12] M. Lavrauw, L. Storme and G. Van de Voorde, On the code generated by the incidence matrix of points and hyperplanes in $\mathrm{PG}(n,q)$ and its dual. *Des. Codes Cryptogr.* **48** (2008), 231–245.

[13] M. Lavrauw, L. Storme and G. Van de Voorde, On the code generated by the incidence matrix of points and k-spaces in $\mathrm{PG}(n,q)$ and its dual. *Finite Fields Appl.* **14** (2008), 1020–1038.

[14] M. Lavrauw, L. Storme, P. Sziklai and G. Van de Voorde, An empty interval in the spectrum of small weight codewords in the code from points and k-spaces of $PG(n,q)$. *J. Combin. Theory, Ser. A* **116** (2009), 996–1001.

[15] X. Li, C. Zhang and J. Shen, Regular LDPC codes from semipartial geometries. *Acta Appl. Math.* **102** (2008), 25–35.

[16] Z. Liu and D.A. Pados, LDPC codes from generalized polygons. *IEEE Trans. Inform. Theory* **51** (2005), 3890–3898.

[17] D.J.C. MacKay and R.M. Neal, Near Shannon limit performance of low density parity check codes. *Electron. Lett.* **32** (1996), 1645–1646.

[18] T.M.N. Ngatched, F. Takawira and M. Bossert, An improved decoding algorithm for finite-geometry LDPC codes. *IEEE Trans. Commun.* **57** (2009), 302–306.

[19] V. Pepe, L. Storme and G. Van de Voorde, Small weight codewords in the LDPC codes arising from linear representations of geometries. *J. Combin. Des.* **17** (2009), 1–24.

[20] P. Sziklai, On small blocking sets and their linearity. *J. Combin. Theory, Ser. A* **115** (2008), 1167–1182.

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

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

[23] P. Vandendriessche, Some low-density parity-check codes derived from finite geometries. *Des. Codes Cryptogr.* **54** (2010), 287–297.

[24] P. Vandendriessche, LDPC codes associated with linear representations of geometries. *Adv. Math. Commun.* **4** (2010), 405–417.

Address of the authors:

Jirapha Limbupasiriporn: Department of Mathematics, Faculty of Science, Silpakorn University, Nakorn Pathom 73000, Thailand (email: jlimbup@su.ac.th)

Leo Storme: Ghent University, Department of Mathematics, Krijgslaan 281 - Building S22, 9000 Ghent, Belgium (email: ls@cage.ugent.be, `http://cage.ugent.be/~ls`)

Peter Vandendriessche: Ghent University, Department of Mathematics, Krijgslaan 281 - Building S22, 9000 Ghent, Belgium (email: pv@cage.ugent.be)