Projective Geometric Codes

Bhaskar Bagchi and S. P. Inamdar

Statistics and Mathematics Unit, Indian Statistical Institute, Bangalore Centre, 8th Mile, Mysore Road, Bangalore 560059, India
E-mail: inamdar@isibang.ac.in

Received September 20, 2001

In this article, we determine the words of minimum weight in the code of the incidence system of s- versus t-flats in a finite projective space. Our proof depends on a few combinatorial results on the geometry of flats which may be of independent interest. We also give bounds for the minimum weight of the dual of this code and show that they are attained in many cases. The lower bound is a consequence of a general result on the dual code of an incidence system.

1. INTRODUCTION

A triplet $(X, \mathscr{B}, I)$ of sets is called an *incidence system* if $I \subseteq X \times \mathscr{B}$. Elements of X are called the points and those of $\mathscr{B}$ are called the blocks of this incidence system. We say that the point x is incident with a block B, denoted by xIB, if $(x, B) \in I$. If k is a field, k^X denotes the k-vector space of all functions from X to k. The k-ary code C of the incidence system is the linear subspace of k^X spanned by the 'characteristic functions' χ_B, $B \in \mathscr{B}$. Here, χ_B is defined by $\chi_B(x) = 1$ if xIB and $= 0$ otherwise. (In case $k = \mathbb{F}_p$, the finite field of prime order p, this code is called the p-ary code of the incidence system.) The vectors in this code are called the words. The support of a word w is the set $S = \{x \in X \mid w(x) \neq 0\}$. The cardinality of S is called the Hamming weight (or simply, the weight) of w. By the minimum weight of a code, one means the minimum non-zero weight of the words in that code. When X is a finite set, the vector space k^X has a natural 'inner product' (i.e. a non-degenerate symmetric bilinear form) given by $\langle v, v' \rangle = \sum_{x \in X} v(x)v'(x)$. The dual $C^\perp$ of the code C is the orthogonal complement of C in k^X with respect to this inner product. A comprehensive reference for codes obtained from incidence systems is [1].

Let $\mathbb{P}^n$ denote the projective space of dimension n over the finite field $\mathbb{F}_q$ of characteristic p. A subset of $\mathbb{P}^n$ is called *a flat* if it contains the line joining any two of its points. An s-flat of $\mathbb{P}^n$ is a flat of projective dimension s. By

convention, the empty set is a flat of dimension -1. By a hyperplane in $\mathbb{P}^n$, we mean an $(n-1)$-flat. Let $G(s,n)$ denote the (Grassmannian) set of all s-flats in $\mathbb{P}^n$. For $0 \leqslant s < t < n$, let $\Delta_{s,t}(n,q)$ denote the incidence system whose points and blocks are the s- and t-flats in $\mathbb{P}^n$, respectively, and the incidence is set inclusion. Let $C_{s,t}(n,q) \subset \mathbb{F}_p^{G(s,n)}$ denote the p-ary code of $\Delta_{s,t}(n,q)$. The codes $C_{0,t}(n,q)$ are just the p-ary codes classically associated with the design of t-flats in $\mathbb{P}^n$.

For $-1 \leqslant r \leqslant m$, let $\binom{m+1}{r+1}_q$ denote the number of r-flats in $\mathbb{P}^m$. Thus,

$$\binom{m+1}{r+1}_q = \frac{(q^{m+1}-1)(q^m-1)\cdots(q^{m+1-r}-1)}{(q^{r+1}-1)(q^r-1)\cdots(q-1)}.$$

The main result of this paper is Theorem 1, where we prove that the minimum weight words of $C_{s,t}(n,q)$ are precisely the scalar multiples of the blocks of $\Delta_{s,t}(n,q)$. The paper is organised as follows.

Section 2 contains a couple of combinatorial lemmas. The first lemma characterises s-flats as the subsets of $\mathbb{P}^n$ intersecting every $(n-s)$-flat and having minimum possible cardinality. This lemma occurs as Theorem 2 in [4]. However, our proof is considerably shorter. As a companion and corollary of this lemma, we prove—in particular—that any (non-empty) point set containing no more elements than an $(n-t)$-flat must meet some t-flat in exactly one point. The second lemma determines the minimum number of points covered by a given number of flats. Its corollary may be viewed as another characterisation of a flat of $\mathbb{P}^n$.

Section 3 presents the proof of Theorem 1. The proof is by induction on s. The case $s = 0$ is well known, see for example [1, Corollary 5.7.5, p. 186]. It was proved independently by Smith [10] and Delsarte *et al.* [5]. Their proof involves indentifying $C_{0,t}(n,q)$ as a subfield subcode of a generalised Reed–Muller code and giving an explicit description of the polynomial functions that represent the code words. However, in Proposition 1, we give another proof of this result which is simple and geometric in nature. For even q, Bagchi and Sastry gave a similar proof of this proposition in [3].

In Section 4, we prove a general lower bound (in terms of the minimum number of blocks through a point and the maximum number of blocks through a pair of points) on the minimum weight of $C^\perp$ where C is the p-ary code of an arbitrary incidence system (Theorem 2). This theorem is a generalisation of the main theorem of [7] which studied the case of partial linear spaces.

Section 5 discusses the minimum weight of the codes $C_{s,t}^\perp(n,q)$. Theorem 2 implies the lower bound of Theorem 3 which significantly improves known bounds even in the case $s = 0$. The results of this paper lead us to:

Conjecture. If q is prime, the minimum weight of $C_{s,t}^{\perp}(n,q)$ is $2q^{n-t}$, and the only words of minimum weight are the scalar multiples of the 'standard words'.

(See Section 5 for the definition of standard words in $C_{s,t}^{\perp}(n,q)$.) When $s=0$, this conjecture can be verified using the theory developed in [5]. Section 5 contains some partial results in support of this conjecture. Namely, in Propositions 2 and 3 we prove this conjecture when $t=s+1$ or $q=2$. Proposition 4 shows that, in general, the statement of the conjecture is false for q even, $q>2$. However, we have no such example when q is odd.

Hamada found a formula for the dimension of $C_{0,t}(n,q)$ in [6]. Recently, a streamlined version of this formula was independently given in [2, Formula (58); 8, Theorem 2.13]. The referee has informed us that a computationally efficient generating function formulation of the Hamada's formula has been obtained by Moorhouse (see [9]). It would be nice to have a dimension formula for the codes $C_{s,t}(n,q)$ in general.

2. COMBINATORICS OF FLATS

DEFINITION. Let F be an s-flat in $\mathbb{P}^n$ and let G be an $(n-s-1)$-flat disjoint from F. The projection from F is the map $\pi:\mathbb{P}^n\backslash F \to G$ sending $y\notin F$ to the unique point in $G\cap\langle F,y\rangle$. Here $\langle F,y\rangle$ denotes the $(s+1)$-flat containing F and y.

Note that the image of an r-flat H under π is an $(r-r'-1)$-flat where r' is the dimension of $H\cap F$. The cardinality of a (finite) set S is denoted by $|S|$.

LEMMA 1. *If a set $S\subseteq\mathbb{P}^n$ intersects every s-flat, then $|S|\geqslant \binom{n-s+1}{1}_q$. Equality holds if and only if S is an $(n-s)$-flat.*

Proof. We proceed by induction on s. The lemma is trivial for $s=0$ and n arbitrary. For any point $x\notin S$, consider the projection of S from x into a hyperplane not containing x. If the image of S missed an $(s-1)$-flat L in this hyperplane, then S would not intersect the s-flat $\langle L,x\rangle$. Thus, the image of S intersects every $(s-1)$-flat of this hyperplane. Therefore, by the induction hypothesis, the image of S contains $\geqslant \binom{n-s+1}{1}_q$ points. Since S contains at least as many points as this image, the inequality holds. Moreover, in case of equality, the projection map is one-to-one when restricted to S. Hence, any line through $x\notin S$ can intersect S in at most one point. Therefore, S is a flat since any line containing two points of S is contained in S. ∎

COROLLARY 1. *Let $0 \leqslant s \leqslant t \leqslant n$. Let $\mathscr{S}$ be a collection of s-flats of $\mathbb{P}^n$ with $|\mathscr{S}| \leqslant \begin{bmatrix} n-t+1 \\ 1 \end{bmatrix}_q$. For any $F \in \mathscr{S}$, there exists a t-flat T in $\mathbb{P}^n$ such that F is the only element of $\mathscr{S}$ contained in T.*

Proof. Fix an $(n-s-1)$-flat G disjoint from F. Let $\pi: \mathbb{P}^n \backslash F \to G$ be the projection from F. For every $H \neq F$ in $\mathscr{S}$, choose a point $h \in H \backslash F$. Let S denote the set of points thus chosen. By Lemma 1, there must exist a $(t-s-1)$-flat L in G that misses the image of S under π. Therefore, F is the only element of $\mathscr{S}$ contained in the t-flat $\langle L, F \rangle$ spanned by L and F. ∎

LEMMA 2. *Let $1 \leqslant s \leqslant t$.*

(a) *Let $\mathscr{S}$ be a collection of s-flats. If $\cap \mathscr{S} \neq \emptyset$ and $|\mathscr{S}| \geqslant \begin{bmatrix} t \\ s \end{bmatrix}_q$, then $|\cup \mathscr{S}| \geqslant \begin{bmatrix} t+1 \\ 1 \end{bmatrix}_q$.*

(b) *Let $\mathscr{S}$ be a collection of $(s-1)$-flats. If $|\mathscr{S}| \geqslant \begin{bmatrix} t \\ s \end{bmatrix}_q$, then $|\cup \mathscr{S}| \geqslant \begin{bmatrix} t \\ 1 \end{bmatrix}_q$.*

Proof. First note that parts (a) and (b) are equivalent for each fixed s. To see this, suppose (b) holds. Let $\mathscr{S}$ be as in (a) and let $v \in \cap \mathscr{S}$. Fix a hyperplane H not passing through v. Let $\mathscr{S}'$ be the collection of $(s-1)$-flats $F \cap H$ for all $F \in \mathscr{S}$. By construction, $|\mathscr{S}'| = |\mathscr{S}|$. Now, applying part (b) to $\mathscr{S}'$, one sees that the number of lines through v contained in $\cup \mathscr{S}$ is at least $\begin{bmatrix} t \\ 1 \end{bmatrix}_q$. Hence, the cardinality of $\cup \mathscr{S}$ is at least $1 + q\begin{bmatrix} t \\ 1 \end{bmatrix}_q = \begin{bmatrix} t+1 \\ 1 \end{bmatrix}_q$. Thus (b) $\Rightarrow$ (a). Clearly, one can reverse this argument to show that (a) $\Rightarrow$ (b). We now apply induction on s to prove (b).

The statement is obviously true when $s = 1$. Let $s > 1$. Let $\mathscr{S}$ be as in (b). For a point v in $\cup \mathscr{S}$, let $\mathscr{S}_v$ denote the subset $\{P \in \mathscr{S} \mid v \in P\}$ of $\mathscr{S}$. If for some v the cardinality of $\mathscr{S}_v$ is at least $\begin{bmatrix} t-1 \\ s-1 \end{bmatrix}_q$, then by part (a) with s, t replaced by $s-1$, $t-1$, respectively (the induction hypothesis), $\cup \mathscr{S}_v$ itself contains the required number of points. Thus, we assume that each $v \in \cup \mathscr{S}$ is contained in at most $\begin{bmatrix} t-1 \\ s-1 \end{bmatrix}_q$ elements of $\mathscr{S}$. Let us now count in two ways the ordered pairs (v, P) such that $v \in P \in \mathscr{S}$. On the one hand, the number of such pairs is at least $\begin{bmatrix} t \\ s \end{bmatrix}_q \begin{bmatrix} s \\ 1 \end{bmatrix}_q$. On the other hand, this number is at most $|\cup \mathscr{S}| \cdot \begin{bmatrix} t-1 \\ s-1 \end{bmatrix}_q$. Since, we have

$$\begin{bmatrix} t \\ s \end{bmatrix}_q \begin{bmatrix} s \\ 1 \end{bmatrix}_q = \begin{bmatrix} t \\ 1 \end{bmatrix}_q \begin{bmatrix} t-1 \\ s-1 \end{bmatrix}_q, \tag{1}$$

the result follows. (To prove the above identity, fix a $(t-1)$-flat T and count in two ways the ordered pairs (v, Q) such that $v \in Q$ and Q is an $(s-1)$-flat in T.) ∎

COROLLARY 2. *Let $1 \leqslant s \leqslant t$. Let $\mathscr{S}$ be a non-empty collection of s-flats such that every point $v \in \cup\mathscr{S}$ is contained in at least $\begin{bmatrix} t \\ s \end{bmatrix}_q$ elements of $\mathscr{S}$. Then, $|\mathscr{S}| \geqslant \begin{bmatrix} t+1 \\ s+1 \end{bmatrix}_q$ and equality holds if and only if $\mathscr{S}$ is the collection of all s-flats in a t-flat.*

Proof. For a point $v \in \cup\mathscr{S}$, let $\mathscr{S}_v = \{P \in \mathscr{S} \mid v \in P\}$. We count the ordered pairs (v,P) where $v \in \cup\mathscr{S}$ and $P \in \mathscr{S}_v$. For any $v \in \cup\mathscr{S}$, Lemma 2 implies that $|\cup\mathscr{S}| \geqslant |\cup\mathscr{S}_v| \geqslant \begin{bmatrix} t+1 \\ 1 \end{bmatrix}_q$. Hence, the number of such pairs is at least $\begin{bmatrix} t+1 \\ 1 \end{bmatrix}_q \cdot \begin{bmatrix} t \\ s \end{bmatrix}_q$. On the other hand, the number of such pairs is equal to $\begin{bmatrix} s+1 \\ 1 \end{bmatrix}_q \cdot |\mathscr{S}|$. Now identity (1) (with s, t replaced by $s+1$, $t+1$) proves that $|\mathscr{S}| \geqslant \begin{bmatrix} t+1 \\ s+1 \end{bmatrix}_q$.

Moreover, $|\mathscr{S}| = \begin{bmatrix} t+1 \\ s+1 \end{bmatrix}_q$ if and only if for every $v \in \cup\mathscr{S}$, we have $|\cup\mathscr{S}| = \begin{bmatrix} t+1 \\ 1 \end{bmatrix}_q = |\cup\mathscr{S}_v|$ and hence $\cup\mathscr{S} = \cup\mathscr{S}_v$. In this case, for any two distinct points v and w in $\cup\mathscr{S}$, $w \in \cup\mathscr{S}_v$. Hence, the line in $\mathbb{P}^n$ which joins v and w is contained in $\cup\mathscr{S}$. Thus, $\cup\mathscr{S}$ is a t-flat and every element of $\mathscr{S}$ is contained in it. This proves the result. ∎

3. THE CODE $C_{s,t}(n,q)$

LEMMA 3. *Let S be the support of a word $w \in C_{0,t}(n,q)$. If S intersects an $(n-t)$-flat in exactly one point, then S intersects every $(n-t)$-flat.*

Proof. We assume on the contrary that there exists an $(n-t)$-flat M disjoint from S. Therefore, χ_M is orthogonal to w. For any $(n-t)$-flat N, the word $\chi_M - \chi_N$ is in the dual of $C_{0,t}(n,q)$. Hence, w is also orthogonal to all the $(n-t)$-flats N. But by assumption, there exists an $(n-t)$-flat meeting S in exactly one point to which w cannot be orthogonal. This contradiction proves the lemma. ∎

PROPOSITION 1. *The minimum weight of $C_{0,t}(n,q)$ is $\begin{bmatrix} t+1 \\ 1 \end{bmatrix}_q$. Further, the only words of minimum weight in this code are the scalar multiples of the t-flats in $\mathbb{P}^n$.*

Proof. If $w \in C_{0,t}(n,q)$ is a non-zero word of weight $\leqslant \begin{bmatrix} t+1 \\ 1 \end{bmatrix}_q$ then, by the $s=0$ case of Corollary 1, there exists an $(n-t)$-flat which intersects its support in exactly one point. Thus, by Lemma 3 the support of w meets every $(n-t)$-flat. Hence by Lemma 1, the weight of w is $\begin{bmatrix} t+1 \\ 1 \end{bmatrix}_q$ and its support is a t-flat. Since two words of minimum weight having the same support must be scalar multiples of each other (otherwise a linear combination of them will have strictly less weight), this completes the proof. ∎

THEOREM 1. *The minimum weight of $C_{s,t}(n,q)$ is $\binom{t+1}{s+1}_q$. Moreover, the only words of minimum weight in this code are the scalar multiples of the blocks of $\Delta_{s,t}(n,q)$.*

Proof. The proof is by induction on s. Proposition 1 is the case $s=0$. So let $s>0$ and $w \in C_{s,t}(n,q)$ be a non-zero word. Let $\mathscr{S}$ be the support of w and let $v \in \cup\mathscr{S}$. View $\mathbb{P}^{n-1}$ as the quotient of $\mathbb{P}^n$ by the point v. For any $F \in G(s,n)$, let $\bar{F}$ denote its image in $\mathbb{P}^{n-1}$. If $v \in F$, then $\bar{F}$ is an $(s-1)$-flat of $\mathbb{P}^{n-1}$. Let $\pi_v : \mathbb{F}_p^{G(s,n)} \to \mathbb{F}_p^{G(s-1,n-1)}$ be the unique linear map satisfying

$$\pi_v(F) = \begin{cases} \bar{F} & \text{if } v \in F, \\ 0 & \text{otherwise} \end{cases}$$

for $F \in G(s,n)$. Looking at the images of the generators of $C_{s,t}(n,q)$, we see that $\pi_v(C_{s,t}(n,q)) = C_{s-1,t-1}(n-1,q)$. Moreover, because of our choice of v, $\pi_v(w)$ is a non-zero word in $C_{s-1,t-1}(n-1,q)$. Hence, by the induction hypothesis, the cardinality of the support of $\pi_v(w)$ is at least $\binom{t}{s}_q$. This proves that every point $v \in \cup\mathscr{S}$ is contained in at least $\binom{t}{s}_q$ elements of $\mathscr{S}$. Now, by Corollary 2, $|\mathscr{S}| \geqslant \binom{t+1}{s+1}_q$ and in case of equality, w has the same support as the generating word corresponding to the t-flat $\cup\mathscr{S}$. Since two words of minimum weight having the same support are scalar multiples of each other, the theorem stands proved. ∎

4. GENERAL INCIDENCE SYSTEMS

Recall that a 2-design with parameters (v,k,λ) (a $2-(v,k,\lambda)$ design) is an incidence system on v points such that (i) each block is incident with k points, and (ii) any two distinct points are together incident with λ blocks. It follows that (iii) each point is incident with $n+\lambda$ blocks, where the number n (the so-called order of the design) is given by $n(k-1) = \lambda(v-k)$. If D_1 and D_2 are two $2-(v,k,\lambda)$ designs on disjoint point sets X_1 and X_2, their λ-join $D_1 *_\lambda D_2$ is defined to be the incidence system with point set $X_1 \cup X_2$ whose blocks are (i) blocks of D_1 and D_2 and (ii) blocks of type $\{x_1, x_2\}$ for every $x_1 \in X_1$, $x_2 \in X_2$, each of these new blocks occurring λ times.

Let $D = (X, \mathscr{B}, I)$ be an incidence system and Y be a subset of X. By the incidence system induced on Y by D we mean the incidence system $(Y, \mathscr{B}, I \cap (Y \times \mathscr{B}))$. We now have the following generalisation of the main theorem of [7] (which is the case $\lambda = 1$).

THEOREM 2. *Let n and λ be positive integers. Let D be an incidence system with at least $n+\lambda$ blocks incident with every point and at most λ blocks incident with any pair of distinct points. Then, for any prime p, the minimum*

weight of the p-ary code $C^{\perp}$ (the dual of the code of D) is at least $2(\frac{n}{\lambda}+1-\frac{n}{\lambda p})$. Moreover, in case of equality, the incidence system induced by D on the support of any word of minimum weight is of the form $D_1 *_{\lambda} D_2$, where D_1 and D_2 are $2-(\frac{n}{\lambda}+1-\frac{n}{\lambda p}, p, \lambda)$ designs.

Proof. We prove the theorem by way of contradiction. Let D be a counter-example satisfying (a) D has the smallest number v of points among all counter-examples, and (b) D has the largest possible number of blocks among all counter-examples satisfying (a). Since the minimum weight of a code is by definition the minimum of the weights of the non-zero words in it, the theorem is vacuously true in case $C^{\perp}=\{0\}$. Therefore, $C^{\perp}\neq\{0\}$. The induced subsystem of D on the support of any non-zero word w of $C^{\perp}$ is also a counter-example. Thus (a) implies that the full point set $\mathscr{X}$ of D is the support of any non-zero w and hence $C^{\perp}$ is one dimensional. Since D is a counter-example, it follows that

$$v\leqslant 2\left(\frac{n}{\lambda}+1-\frac{n}{\lambda p}\right). \tag{2}$$

Let M be a non-empty proper subset of a block L such that $\chi_M\in C$. Then the incidence system obtained from D by deleting the block L and adding the pair of blocks M, $L\backslash M$ is a counter-example with larger number of blocks. Since this contradicts property (b) of D, we see that $\chi_M\notin C$ for any such M. Fix a basis $\{w\}$ of $C^{\perp}$. The above observation implies that for any proper non-empty subset M of a block of D,

$$\sum_{A\in M} w(A)\neq 0. \tag{3}$$

For any $A\in\mathscr{X}$, let x_A, y_A, z_A denote the number of blocks through A of cardinality 2, 3, 4, respectively. We now count the pairs (B, L) such that $B\neq A$ and L is a block containing A and B. Since pairs of points occur in at most λ blocks, we get: $x_A+2y_A+3(n+\lambda-x_A-y_A)\leqslant\lambda(v-1)$ and $x_A+2y_A+3z_A+4(n+\lambda-x_A-y_A-z_A)\leqslant\lambda(v-1)$. Therefore, by (2), we have

$$3x_A+2y_A+z_A\geqslant 2n+3\lambda+\frac{2n}{p} \tag{4}$$

and

$$2x_A+y_A\geqslant n+2\lambda+\frac{2n}{p}. \tag{5}$$

Similarly, we have $\lambda(v-1)\geqslant x_A+2y_A+\sum_{i=1}^{m}(|L_i|-1)$, where L_i's are the blocks through A of size >3. Since $y_A\geqslant n+\lambda-x_A-m$, by (2),

we get

$$x_A \geqslant \lambda + \frac{2n}{p} + \sum_{i=1}^{m} (|L_i| - 3). \tag{6}$$

The theorem is trivial for $p = 2$ (namely, one argues as in [1, Lemma 2.4.2, p. 54]). Thus, we assume that $p \geqslant 3$. Fix a point $Q \in \mathscr{X}$ such that $x_Q \leqslant x_A$ for all $A \in \mathscr{X}$. We normalise the generator w of $C^{\perp}$ by assuming $w(Q) = -1$. We now colour $\mathscr{X}$ by elements of $\mathbb{F}_p$ using this w, wherein a point P gets the colour $w(P)$. As the characteristic function of a block is in the dual of $\langle w \rangle$, the sum of the colours occurring on any block is $0 \pmod p$. Let $\mathscr{S} = \{\alpha \in \mathbb{F}_p \mid w(P) = \alpha \text{ for some point } P\}$ denote the set of colours and let $X_\alpha \subseteq \mathscr{X}$ denote the set of points with colour α. The number of blocks of size 2 through any point is at least x_Q. Hence, for every $\alpha \in \mathscr{S}$, at least $\frac{x_Q}{\lambda}$ points of $\mathscr{X}$ are coloured $-\alpha$. As $x_Q > 0$, we have $\alpha \in \mathscr{S}$ if and only if $-\alpha \in \mathscr{S}$. Hence

$$|X_\alpha| \geqslant \frac{x_Q}{\lambda} \quad \text{for all } \alpha \in \mathscr{S}.$$

Also, $|\mathscr{S}|$ is even as $0 \notin \mathscr{S}$ ($\mathscr{X}$ is the support of w). Thus, $|\mathscr{S}| = 2r$ for some r with $1 \leqslant r \leqslant \frac{p-1}{2}$. Since $\mathscr{X}$ is partitioned by X_α's, by (2),

$$r x_Q \leqslant n + \lambda - \frac{n}{p}. \tag{7}$$

First consider the case $r = 1$. In this case $\mathscr{S} = \{1, -1\}$. By (3), the blocks containing a point each of colour 1 and -1 have size 2. Also, any block all of whose points have the same colour must be of size p. Thus, all blocks have size either 2 or p. Also, by (7), the number α of blocks of size p through Q is at least $\frac{n}{p}$. Let $\beta = x_Q$ so that $\alpha + \beta \geqslant n + \lambda$. We also have $\alpha(p-1) + \beta \leqslant \lambda(v-1)$. Hence

$$2n + \lambda - \frac{2n}{p} = \operatorname{Min}\{\alpha(p-1) + \beta\} \leqslant \lambda(v-1) \leqslant 2n + \lambda - \frac{2n}{p}. \tag{8}$$

Here, the minimum is taken over all real numbers α and β such that $\alpha \geqslant \frac{n}{p}$ and $\alpha + \beta \geqslant n + \lambda$. This minimum is attained only when $\beta = n + \lambda - \frac{n}{p}$ and $\alpha = \frac{n}{p}$. Thus, $x_Q = n + \lambda - \frac{n}{p}$. As $x_Q \leqslant \lambda |X_1|$, we must have $|X_1| \geqslant \frac{n}{\lambda} + 1 - \frac{n}{\lambda p}$. Similarly, $|X_{-1}| \geqslant \frac{n}{\lambda} + 1 - \frac{n}{\lambda p}$. Therefore, by (2), $|X_1| = |X_{-1}| = \frac{n}{\lambda} + 1 - \frac{n}{\lambda p}$ and $x_A = x_Q$ for all $A \in \mathscr{X}$. Also, the inequality in (8) must be an equality. Therefore, for any point $P \neq Q$, the pair $\{P, Q\}$ occurs in exactly λ blocks. Since $x_A = x_Q$, the above argument holds for any $A \in \mathscr{X}$ in place of Q. It follows that D is the λ-join of two 2-design with parameters as in the

statement of the theorem. This is a contradiction since D is supposed to be a counter-example.

Thus, we may assume that $r > 1$. As $1 < r \leqslant \frac{p-1}{2}$, we have $p > 3$. Hence (6) and (7) implies that $r \neq \frac{p-1}{2}$. We thus have $1 < r < \frac{p-1}{2}$.

Let G denote the graph whose vertex set is $\mathscr{S}$ and whose edges are given by the following rule:

$$\alpha \text{ and } \beta \text{ are adjacent if and only if } \alpha + \beta = 0 \text{ or } 1 \text{ in } \mathbb{F}_p.$$

Since $0 \notin \mathscr{S}$, the degree of 1 is one in G. The only possible loop of G is at the vertex $\frac{p+1}{2}$ and this loop occurs if and only if $\frac{p+1}{2}$ belongs to $\mathscr{S}$. If $\alpha_1 \cdots \alpha_m \alpha_1$ is a non-trivial cycle in G, then m must be even, as the edges of types $\{\alpha, -\alpha\}$ and $\{\alpha, 1-\alpha\}$ must alternate in the cycle. Also,

$$(\alpha_1 + \alpha_2) + \cdots + (\alpha_{m-1} + \alpha_m) = (\alpha_2 + \alpha_3) + \cdots + (\alpha_m + \alpha_1).$$

As one of these sums is zero and the other is $\frac{m}{2}$, m must be a multiple of $2p$. Since $m \leqslant |\mathscr{S}| < p - 1$, G cannot contain any cycles. Therefore, each connected component of G is a path. In case $\frac{p+1}{2} \in \mathscr{S}$, one of these paths has a loop at one end.

Case 1. *The graph G is connected*: In this case, G must be the path $1(-1)2(-2)\cdots r(-r)$. Since $r < \frac{p-1}{2}$, G does not have a loop at either end.

Let l denote the number of blocks L of size > 2 through Q such that at most one point in $L \setminus \{Q\}$ has colour different from $-r$. Since $r > 1$, $Q \notin X_{-r}$. Hence, $|\{Q\} \cup X_{-r}| \geqslant 1 + \frac{x_Q}{\lambda}$. Counting pairs (R, M) where R is a point outside $\{Q\} \cup X_{-r}$ and $M \supseteq \{Q, R\}$ is a block, we get

$$2(n + \lambda - x_Q - l) + x_Q \leqslant \lambda\left(v - \left(1 + \frac{x_Q}{\lambda}\right)\right) \leqslant 2n + \lambda - \frac{2n}{p} - x_Q.$$

Therefore, $l \geqslant \frac{n}{p} + \frac{\lambda}{2} > \frac{n}{p}$. We now estimate the cardinality of such a block L. Since the colours on L add up to $0 \pmod p$, it follows that the colour of the remaining point is $m \pmod p$ where $m = 1 + (|L| - 2)r$. Since, $|L| > 2$, $m > r$; also $m \pmod p$ is in the set of colours $\mathscr{S} = \{1, \ldots, r, p-r, \ldots, p-1\}$. Therefore, $m \geqslant p - r$. That is, $|L| \geqslant \frac{p-1}{r} + 1$ for any such block L. Since, each of these l blocks through Q have size $\geqslant \frac{p-1}{r} + 1 > 3$, by (6), we get

$$x_Q > \lambda + \frac{2n}{p} + \frac{n}{p}\left(\frac{p-1}{r} - 2\right) = \lambda + \frac{n}{r} - \frac{n}{pr}.$$

However, this bound contradicts (7).

Case 2. *G is disconnected*: Let $\mathscr{S}' \subseteq \mathscr{S}$ denote the set of colours which have degree one in G. Since G contains at most one loop and is disconnected, we must have $|\mathscr{S}'| \geqslant 3$.

Let M be a block of size 3 through Q. As the colours on M add to 0 (mod p), the colours of the two points of $M \setminus \{Q\}$ add up to 1 (mod p) and hence they cannot be from $\mathscr{S}'$. Thus, for all $\alpha \in \mathscr{S}'$, $M \cap X_\alpha \subseteq \{Q\}$. We now count the pairs (P, L) such that $Q \neq P \in \mathscr{X} \setminus (\bigcup_{\alpha \in \mathscr{S}'} X_\alpha)$ and L is a block containing $\{P, Q\}$. Since for every block of size 3 through Q we have two choices for P, it follows that $2y_Q \leqslant \lambda(v - |\mathscr{S}'|\frac{x_Q}{\lambda})$. Hence, by (2) and (5), $|\mathscr{S}'| < 4$.

Thus, $|\mathscr{S}'| = 3$ and $2y_Q + 3x_Q \leqslant \lambda v \leqslant 2n + 2\lambda - \frac{2n}{p}$. By (5), we also have $2y_Q + 4x_Q \geqslant 2n + 4\lambda + \frac{4n}{p}$. Hence, $x_Q \geqslant 2\lambda + \frac{6n}{p}$. This, together with (7), forces $1 < r < \frac{p}{6}$.

Also, G must contain a loop as the number of vertices in G of degree 1 is odd. Thus, the graph G consists of two components. One is

$$1(-1)2(-2)\cdots t(-t) \quad \text{for some } t \text{ such that } 1 \leqslant t < r$$

and the other is

$$\left(\frac{p+1}{2}\right)\left(\frac{p+1}{2}\right)\left(\frac{p-1}{2}\right)\left(\frac{3-p}{2}\right)\left(\frac{p-3}{2}\right)\cdots\left(\frac{p+1-(2r-2t)}{2}\right).$$

Thus $1, -t$ and $\alpha = \frac{p+1-(2r-2t)}{2} = \frac{p+1}{2} - r + t$ are the three vertices of degree one in G. If every block of size 4 through Q contains one point from $\mathscr{X} \setminus (\bigcup_{\alpha \in \mathscr{S}'} X_\alpha)$ which is different from Q, then there are at least $2y_Q + z_Q$ pairs (P, L) as before. This implies that $2y_Q + z_Q \leqslant \lambda(v - 3\frac{x_Q}{\lambda})$. This contradicts (4). Hence, there exists a block L of size 4 through Q contained in $\{Q\} \cup X_{-t} \cup X_\alpha$ (by (3), no point of X_1 is contained in a block of size 4 through Q).

Let L contain i points from X_α so that the sum of the colours occurring on L is $i(\frac{p+1}{2} - r + t) - (3 - i)t - 1$ with $0 \leqslant i \leqslant 3$. Since this sum is 0 (mod p), varying i between 0 and 3, we infer that one of the integers $3t + 1$, $2(r + t) + 1$, $2r - t$, $6(r - t) - 1$ is a multiple of p. However, this cannot happen as $1 \leqslant t < r < \frac{p}{6}$. This completes the proof of the theorem. ∎

5. THE DUAL CODE $C_{s,t}^{\perp}(n, q)$

For any two flats L and M, let $[L, M]$ denote the collection of all s-flats F such that $L \subseteq F \subseteq M$. Let $\chi_{[L,M]} \in \mathbb{F}_p^{G(s,n)}$ denote its characteristic function. Take any $(s-1)$-flat A and two $(n-t+s)$-flats B and C such that $B \cap C$ is an $(n-t+s-1)$-flat and $A \subset B \cap C$. Then, $\chi_{[A,B]} - \chi_{[A,C]}$ is a word of weight $2q^{n-t}$ of $C_{s,t}^{\perp}(n, q)$.

DEFINITION. For any triplet (A, B, C) as above, $\chi_{[A,B]} - \chi_{[A,C]}$ is called a *standard word* in $C^{\perp}_{s,t}(n, q)$.

THEOREM 3. *The minimum weight d of $C^{\perp}_{s,t}(n, q)$ satisfies*

$$2\left(\frac{q^{n-s}-1}{q^{t-s}-1}\left(1-\frac{1}{p}\right)+\frac{1}{p}\right) \leqslant d \leqslant 2q^{n-t}.$$

If the lower bound is attained, then we must have $t = s + 1$.

Proof. The upper bound follows from the existence of the standard words. In the incidence system $\Delta_{s,t}(n, q)$, each 'point' is in $\binom{n-s}{t-s}_q$ blocks and any two distinct 'points' are together in at most $\binom{n-s-1}{t-s-1}_q$ blocks. Therefore, the lower bound follows from Theorem 2.

If this lower bound is attained, let w be a minimum weight word. Let $\mathscr{S}$ denote the support of w. Because of equality in Theorem 2, any two s-flats in $\mathscr{S}$ are contained in the maximum possible number of t-flats. This means that any two of them must intersect in an $(s-1)$-flat. Hence, any three of them are contained in an $(s+2)$-flat. Therefore, for $t \geqslant s+2$, any three of these s-flats are contained in a common t-flat. However, Theorem 2 guarantees the existence of three s-flats which are not contained in a single block in the induced structure on $\mathscr{S}$. Thus, it follows that $t = s + 1$. ∎

LEMMA 4. *The p-ary code $C^{\perp}_{t-1,t}(n, q)$ attains the lower bound given by Theorem 3 if and only if $C^{\perp}_{0,1}(n-t+1, q)$ does so. In this case, any word of minimum weight of $C^{\perp}_{t-1,t}(n, q)$ is a pull-back of a minimum weight word in $C^{\perp}_{0,1}(n-t+1, q)$.*

Proof. In the incidence system $\Delta_{t-1,t}(n, q)$, any two distinct 'points' are contained in at most one block. We therefore call a set of 'points' collinear if there exists a t-flat containing all of its elements. Thus, two 'points' are collinear if and only if they have a $(t-2)$-flat in common.

Let $\mathscr{S}$ be the support of a word w in $C^{\perp}_{t-1,t}(n, q)$ attaining the lower bound of Theorem 3. Because of equality in Theorem 2, any two 'points' of $\mathscr{S}$ are collinear. We now claim that there exists a $(t-2)$-flat M which is contained in every element of $\mathscr{S}$.

Given three $(t-1)$-flats in $\mathbb{P}^n$ any two of which intersect in a $(t-2)$-flat, either all of them contain a common $(t-2)$-flat or they are contained in a t-flat. This shows that any three 'non-collinear' elements of $\mathscr{S}$ have a $(t-2)$-flat in common. Now, Theorem 2 says that $\mathscr{S}$ can be partitioned into two equal parts such that any three collinear 'points' of $\mathscr{S}$ are contained in the same part. This fact implies that all the $(t-1)$-flats in $\mathscr{S}$ have a $(t-2)$-flat M in common.

View $\mathbb{P}^{n-t+1}$ as a quotient of $\mathbb{P}^n$ by M and let π be the quotient map. The word $\bar{w}$ defined by $\bar{w}(v) = w(\pi^{-1}(v))$ is an element of $C_{0,1}^{\perp}(n-t+1, q)$ attaining the lower bound given in Theorem 3. Clearly, this formula can be used (for any choice of a $(t-2)$-flat M, with the understanding that value of w is zero for any $(t-1)$-flat not containing M) to construct a word w from a given $\bar{w}$. ∎

PROPOSITION 2. *When q is prime, the minimum weight of $C_{t-1,t}^{\perp}(n,q)$ is $2q^{n-t}$. Moreover, the words of minimum weight are precisely the scalar multiples of the standard words in $C_{t-1,t}^{\perp}(n,q)$.*

Proof. When $q = 2$, this proposition is a special case of Proposition 3 below. Thus, we assume that $q > 2$. In the case $q = p$ and $t = s+1$, the upper and lower bounds in Theorem 3 coincide. Therefore, the scalar multiples of standard words in $C_{t-1,t}^{\perp}(n,p)$ are words of minimum weight. Under the pull-back construction of Lemma 4, a standard word goes to a standard word. Thus, it is enough to prove that the minimum weight words of $C_{0,1}^{\perp}(n,p)$ are the scalar multiples of the standard words for any prime $p > 2$.

Let S be the support of a word w of weight $2p^{n-1}$ in $C_{0,1}^{\perp}(n,p)$. Let $S = S_1 \cup S_2$ be the partition of S given by Theorem 2. Fix a point v in S_1 and a hyperplane G not containing v. Let π denote the projection from v to G. Let $H = \pi(S_1 \setminus \{v\})$ and $K = \pi(S_2)$.

Let L be any line through v. Because of Theorem 2, we have: (i) L does not meet both $S_1 \setminus \{v\}$ and S_2, (ii) L meets $S_1 \setminus \{v\}$ in 0 or $p-1$ points and (iii) L meets S_2 in at most one point. Therefore, we get: (a) $H \cap K = \emptyset$, (b) the restriction of π to $S_1 \setminus \{v\}$ is $(p-1)$ to one, and (c) the restriction of π to S_2 is one-to-one. Thus, $|H| = \binom{n-1}{1}_p$ and $|K| = p^{n-1}$ so that $|G| = |H| + |K|$. Therefore, by (a), G is the disjoint union of H and K.

We claim that H is an $(n-2)$-flat in G. If it is not, then by Lemma 1 there exists a line L in G disjoint from H. Then $L \subset K$. Because of (c), the 2-flat $\langle L, v\rangle$ meets S_2 in $|L| = p+1$ points. Thus, $\Delta_{0,1}(n,p)$ induces a $2-(p+1, p, 1)$ design on $S_2 \cap \langle L, v\rangle$. Since $p > 2$, there is no 2-design with these parameters. This proves our claim.

Thus, S_1 is contained in the $(n-1)$-flat $H_1 = \langle H, v\rangle$. Since no line is contained in S_1, every line in H_1 intersects $M = H_1 \setminus S_1$. Thus, by Lemma 1, M is an $(n-2)$-flat in H_1. Let $H_2 = M \cup S_2$. Any line joining two points of S_2 contains p points from S_2 and meets H_1 in a point of M. Thus, a line joining two points of S_2 or two points of M is contained in H_2. Moreover, a line joining a point of M and a point of S_2 cannot contain any point S_1. This means that it is a line containing p points of S_2. Therefore, by the previous argument, such a line is also contained in H_2. Thus H_2 is an $(n-1)$-flat. Thus, S is the symmetric difference of the hyperplanes H_1 and H_2 which meet

in M. Therefore, S is also the support of the standard word corresponding to the triplet $(\emptyset, H_1, H_2)$. Since, two words of minimum weight having the same support are scalar multiples of each other, this proves the proposition. ∎

The following results completely settle the case $q = 2$.

LEMMA 5. *The minimum weight of $C^{\perp}_{s,t}(n,2)$ is 2^{n-t+1}. Further, any word of minimum weight in $C^{\perp}_{s,t}(n,2)$ is a pull-back of a word of minimum weight in $C^{\perp}_{0,t-s}(n-s,2)$.*

Proof. Let w be a word of minimum weight in $C^{\perp}_{s,t}(n,2)$. Let $\mathscr{S}$ be its support. If $|\mathscr{S}| \leqslant \begin{bmatrix} n-t+1 \\ 1 \end{bmatrix}_2$, Corollary 1 tells us that there exists a t-flat T containing exactly one element of $\mathscr{S}$. Then, w cannot be orthogonal to χ_T. This forces that $|\mathscr{S}| \geqslant \begin{bmatrix} n-t+1 \\ 1 \end{bmatrix}_2 + 1 = 2^{n-t+1}$. Existence of the standard words shows that $|\mathscr{S}| = 2^{n-t+1}$.

Fix an s-flat $F \in \mathscr{S}$ and an $(n-s-1)$-flat G disjoint from F. Let $\pi : \mathbb{P}^n \backslash F \to G$ be the projection from F. For every $H \neq F$ in $\mathscr{S}$, choose a point $h \in \pi(H \backslash F)$. Let T denote the set of points thus chosen. We claim that T is an $(n-t)$-flat of G. Since $|T| \leqslant \begin{bmatrix} n-t+1 \\ 1 \end{bmatrix}_2$, by Lemma 1, it is enough to prove that every $(t-s-1)$-flat of G intersects T. Let L be a $(t-s-1)$-flat of G such that $L \cap T = \emptyset$. In this case, F is the only element of $\mathscr{S}$ contained in the t-flat $\langle L, F \rangle$. Therefore, w is not orthogonal to the characteristic function of this t-flat. Since this cannot happen, our claim is proved. Hence, $|T| = \begin{bmatrix} n-t+1 \\ 1 \end{bmatrix}_2 = |\mathscr{S}| - 1$. Since this happens independent of all the choices involved, we see that $\pi(H \backslash F)$ is a singleton set for every $H \neq F$ in $\mathscr{S}$. Thus, $H \cap F$ is an $(s-1)$-flat for all $H \neq F$. Since F was an arbitrary element of $\mathscr{S}$, it follows that any two distinct s-flats in $\mathscr{S}$ must intersect in an $(s-1)$-flat.

Fix an element $H_0 \in \mathscr{S} \backslash \{F\}$ and let $M = H_0 \cap F$. We now claim that the $(s-1)$-flat M is contained in every element of $\mathscr{S}$. Let $H_1 \in \mathscr{S} \backslash \{F, H_0\}$. If H_1 does not contain M, then the $(s-1)$-flat $H_0 \cap H_1$ must contain a point v outside F. In this case, $\pi(H_0 \backslash F) = \pi(v) = \pi(H_1 \backslash F)$ so that $|T| \leqslant |\mathscr{S}| - 2$ which cannot happen. Thus, M is contained in every element of $\mathscr{S}$. Therefore, by viewing $\mathbb{P}^{n-s}$ as the quotient of $\mathbb{P}^n$ by the $(s-1)$-flat M, one sees that w is a pull-back of its image $\bar{w}$ in $C^{\perp}_{0,t-s}(n-s,2)$. This proves the lemma since the weight of w is equal to that of $\bar{w}$. ∎

PROPOSITION 3. *The minimum weight of $C^{\perp}_{s,t}(n,2)$ is 2^{n-t+1} and the words of minimum weight are precisely the standard words.*

Proof. After Lemma 5, it suffices to prove that the standard words are the only words of minimum weight in $C^{\perp}_{0,t}(n,2)$. Since this is a Reed–Muller code, this actually follows from the existing theory of such codes. However, we present an elementary and self-contained proof.

Let S be the support of a word w of weight 2^{n-t+1} in $C_{0,t}^{\perp}(n,2)$. Fix a point v in S and a hyperplane H not containing v. Let π be the projection from v to H. Arguing as in the proof of Lemma 5, we see that $T = \pi(S\backslash\{v\})$ is an $(n-t)$-flat in H. Hence, S is contained in the $(n-t+1)$-flat $Y = \langle T, v\rangle$. Let $Z = Y\backslash S$.

We claim that Z is an $(n-t)$-flat. Let p_1 and p_2 be two distinct points in Z and let p_3 be the third point on the line L joining p_1 and p_2. To prove our claim, we wish to show that $L \subset Z$. There exists a t-flat W such that $W \cap Y = L$. If $p_3 \notin Z$, then $W \cap S = \{p_3\}$. This means that w is not orthogonal to χ_W, contradiction. Thus, $S = Y\backslash Z$ where Y is an $(n-t+1)$-flat and Z is an $(n-t)$-flat in Y. Let Z_1, Z_2 be two $(n-t)$-flats of Y such that $Y = Z \cup Z_1 \cup Z_2$. Then S is also the support of the standard word corresponding to $(\emptyset, Z_1, Z_2)$. Since two distinct words in a binary code cannot have the same support, this completes the proof. ∎

LEMMA 6. *The minimum weight of $C_{s,t}^{\perp}(n+1,q)$ is at most q^{s+1} times the minimum weight of $C_{s,t}^{\perp}(n,q)$.*

Proof. For any word $w \in C_{s,t}^{\perp}(n,q)$, we can construct a word $\hat{w} \in C_{s,t}^{\perp}(n+1,q)$ in the following way: Fix a point $v \in \mathbb{P}^{n+1}$ and view $\mathbb{P}^n$ as hyperplane H in $\mathbb{P}^{n+1}$ not passing through v. Let $\pi : \mathbb{P}^{n+1}\backslash\{v\} \to H$ denote the projection from v. Define $\hat{w} \in \mathbb{F}_p^{G(s,n+1)}$ by

$$\hat{w}(F) = \begin{cases} w(\pi(F)) & \text{if } v \notin F, \\ 0 & \text{if } v \in F. \end{cases}$$

For an $(s+1)$-flat F of $\mathbb{P}^{n+1}$ containing v, the number of s-flats in F not containing v is q^{s+1}. This implies that the number of s-flats of $\mathbb{P}^{n+1}$ which are mapped under π to a given s-flat in $\mathbb{P}^n$ is q^{s+1}. Hence, the weight of $\hat{w}$ is q^{s+1} times the weight of w. Let M be a t-flat in $\mathbb{P}^{n+1}$. If M does not contain v, then $\pi(M)$ is a t-flat of H. Further, $\langle \hat{w}, M\rangle = \langle w, \pi(M)\rangle = 0$. If M contains v, then $\langle \hat{w}, M\rangle = q^{s+1}\langle w, \pi(M)\rangle = 0$. Therefore, $\hat{w}$ defines a word of $C_{s,t}^{\perp}(n+1,q)$. ∎

PROPOSITION 4. *For q even, the minimum weight of the code $C_{t-1,t}^{\perp}(n,q)$ is at most $q^{n-t-1}(q+2)$. Further, the equality holds in case $n = t+1$.*

Proof. Since hyperovals in $\mathbb{P}^2$ are words of weight $q+2$ in $C_{0,1}^{\perp}(2,q)$, the inequality holds for $t = 1$, $n = 2$. Now repeated application of Lemma 6 implies the inequality for $t = 1, n$ arbitrary. The construction of the word $\bar{w}$ from w as outlined in the proof of Lemma 4 now implies the inequality in general. When $n = t+1$, Theorem 3 implies that $q+2$ is the minimum weight. ∎

It seems plausible that the above upper bound is actually attained even when $n > t + 1$. In the end, we observe that Corollary 1 can be applied to the support of a non-zero word of the code $C_{s,t}^{\perp}(n.q) \oplus \langle \mathbf{1} \rangle$ (where $\mathbf{1}$ is the all one vector) to show that its minimum weight is at least $\binom{n-t+1}{1}_q$. In case $s = 0$, this bound is attained and, by Lemma 1, the words of minimum weight are the scalar multiples of the $(n - t)$-flats.

REFERENCES

1. E. F. Assmus and J. D. Key, Designs and their codes, Cambridge Tracts in Math., Vol. **103,** Cambridge Univ. Press, Cambridge, UK, 1992.
2. M. Bardoe and P. Sin, The permutation modules for $GL(n + 1, \mathbb{F}_q)$ acting on $\mathbb{P}^n(\mathbb{F}_q)$ and $\mathbb{F}_q^{n+1}$, *J. London Math. Soc.* (2) **61** (2000), 58–80.
3. Bhaskar Bagchi and N. S. Narasimha Sastry, Minimum weight words of binary codes associated with finite protective geometries, *Discrete Math.* **57** (1985), 307–310.
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 code, *J. Combin. Theory* **1** (1966), 96–104.
5. P. Delsarte, J. M. Goethals, and F. J. MacWilliams, On generalised Reed–Muller codes and their relatives, *Inform. and Control* **16** (1970), 403–442.
6. N. Hamada, The rank of the incidence matrix of points and d-flats in finite geometries, *J. Sci. Hiroshima Univ. Ser. A-I* **32** (1968), 381–396.
7. S. P. Inamdar, Rigidity theorems for partial linear spaces, *J. Combin. Theory Ser. A* **96** (2001), 388–395.
8. S. P. Inamdar and N. S. Narasimha Sastry, Codes from Veronese and Segre embeddings and Hamada's formula, *J. Combin. Theory Ser. A* **96** (2001), 20–30.
9. P. Sin, The p-rank of the incidence matrices of intersecting linear subspaces, preprint.
10. K. J. C. Smith, Majority decodable codes derived from finite geometries, *Inst. Statist. Mimeo Ser.* **561** (1967).