Determining sets

Lynn Margaret Batten*

University of Manitoba
Winnipeg R3T 2N2 CANADA

Abstract

We give several constructions of determining sets in various settings. We also demonstrate the connections between determining sets, skew k-arcs and linear codes of minimum distance 5.

1. ***Motivation.***

Let P be a non-empty set of elements which we shall call *points*. Let $\mathcal{B}$ be a non-empty set of subsets of $\mathcal{P}$ which we shall call *blocks*. We consider the use of a point/block system $\mathcal{S} = (\mathcal{P}, \mathcal{B})$ in a message sending scenario in the sense that elements of $\mathcal{B}$ will be thought of as *messages* (on the point set $\mathcal{P}$) relayed from one person or station to another. The set $\mathcal{P}$ need not necessarily be finite, but finiteness will be assumed in some of what follows.

For example let $\mathcal{P} = \{1,2,3,4,5,6,\}$, $\mathcal{B} = \{\{1,2,3,5,\},\{2,4\},\{1,3,6\}\}$. If A decides to send $\{1,2,3,5\}$ to B as a message, A may instead send the subset $\{5\}$ or the subset $\{2,3\}$ for instance, and B can easily establish that $\{1,2,3,5\}$ was intended. (This is because $\{1,2,3,5\}$ is the *unique block* in the message set containing the sets $\{5\}$ and $\{2,3\}$.)

Notice that if a set of blocks contains two blocks one of which is a subset of the other, then no subset of the smaller block uniquely determines that block. However, if no block in $\mathcal{B}$ is a subset of any other, each block has at least one subset which uniquely determines it – simply take the full block.

The above motivates the following definitions.

The triple $(\mathcal{P}, \mathcal{B}, \mathcal{C})$ is called a *critical system* if $\mathcal{P}$ is a non-empty set of elements called *points*, $\mathcal{B}$ a non-empty set of subsets of $\mathcal{P}$ called *blocks* and $\mathcal{C}$ a non-empty set of subsets of $\mathcal{P}$ called *critical sets* such that each block contains at least one critical set and each critical set is contained in a unique block.

Returning to the message sending scenario, one could ask, why not just use the full block as a message. There are two principal reasons. First of all, in a very large (finite) system, a great deal of space can be saved by transmitting only a small portion of each block. Secondly, as was shown in [4], in a cryptologic setting it is useful to have several choices of critical sets for each block.

* Research supported in part by NSERC grant OGP045831

In section 2, we consider critical systems from the point of view of antichains. Section 3 gives recursive constructions for critical systems. The connection between critical systems and blocking sets is facilitated in section 4 by the introduction of *determining sets*. We show how determining sets can be constructed in Desarguesian projective planes and prove that a planar determining set can be extended to a determining set in higher dimensions. In the final section, we introduce a concept complementary to that of determining set: skew n-arc, and prove that skew n-arcs in $PG(m,q)$ are equivalent to linear codes of minimum distance 5. An improvement to known parameters of such codes is also presented.

2. *Antichains.*

An *antichain* in a poset $(\mathcal{L},\sim)$ with relation $\sim$ is a subset of the elements of $\mathcal{L}$, no two of which are related [1]. When $\mathcal{L}$ is the set of all subsets of a fixed point set $\mathcal{P}$, ordered by inclusion, for any antichain $\mathcal{B}$ the triple $(\mathcal{P},\mathcal{B},\mathcal{B})$ is a critical system. Conversely, given a critical system $(\mathcal{P},\mathcal{B},\mathcal{C})$, choose a subset of $\mathcal{C}'$ of $\mathcal{C}$ such that each block has a unique critical set in $\mathcal{C}'$. Then $\mathcal{C}'$ is clearly an antichain.

The following well-known result of E. Sperner gives an upper bound on the number of blocks forming an antichain on a fixed point set.

Sperner (1928) [22] Let $\mathcal{A}$ be an antichain of subsets of a v-set $\mathcal{P}$. Then $|\mathcal{A}| \leq \binom{v}{[\frac{v}{2}]}$. Moreover, the case of equality occurs precisely when each block has size $[\frac{v}{2}]$. (Here $[\frac{v}{2}]$ for v odd is without loss of generality either $\frac{v-1}{2}$ or $\frac{v+1}{2}$.)

The construction of maximal antichains having vectors with different numbers of 1's has been of interest to a number of people. In particular, it may be required that a certain given set of vectors (blocks) appears in the maximal antichain. Many of the algorithms used in the constructions of antichains are based on the following theorem due to Dilworth.

Dilworth (1950) [12]. In any poset P, the maximum size of an antichain is equal to the minimum number of chains in a chain decomposition of P.

Dantzig and Hoffman [11] then use a linear programming approach to find chain decompositions in finite posets. Anderson [1] gives further information on, and references to, antichains.

Note that any t-design with $\lambda = 1$ forms a critical system where the points and blocks are the same in each system and the critical sets are the t-subsets. Thus each block of size k contains $\binom{k}{t}$ *minimal* critical sets.

3. *Recursive Constructions*

We first of all give the obvious *direct product* construction of critical systems on finite point sets.

We shall consider a block of a critical system as the corresponding row in a fixed incidence matrix for the system.

For $\mathcal{S}_i = (\mathcal{P}_i,\mathcal{B}_i,\mathcal{C}_i)$, $1 \leq i \leq n$, a critical system on v_i points, define $\prod_{i=1}^{n} \mathcal{B}_i$

(respectively $\prod_{i=1}^{n} \mathcal{C}_i$) as

$$\{(a_1^1, a_2^1, \cdots a_{v_1}^1, a_1^2, a_2^2, \cdots a_{v_2}^2, \cdots a_1^n, a_2^n, \cdots a_{v_n}^n) \mid (a_1^i, a_2^i, \cdots a_{v_i}^i) \in \mathcal{B}_i\}$$

(respectively $\mathcal{C}_i$). The following lemma is then easy.

LEMMA 1. *If $\mathcal{S}_i = (\mathcal{P}_i, \mathcal{B}_i, \mathcal{C}_i)$, $1 \leq i \leq n$, is a critical system on v_i points and b_i blocks, where the point sets are considered to be disjoint, then*

$$\prod_{i=1}^{n} S_i = (\bigcup_{i=1}^{n} \mathcal{P}_i, \prod \mathcal{B}_i, \prod \mathcal{C}_i)$$

is a critical system on $\prod_{i=1}^{n} v_i$ points and $\prod_{i=1}^{n} b_i$ blocks.

An advantage of this direct product construction is that it increases the number of (minimal) critical sets per block. A second advantage is that the size of maximal antichains remains relatively large (see the gluing construction below for a comparison), with a maximum possible size of $\prod_{i=1}^{n} \binom{v_i}{\lfloor \frac{v_i}{2} \rfloor}$.

A second construction, common in coding theory (see [21] for instance) is the idea of 'gluing'. We again identify each block of a finite critical system with the corresponding row in a fixed incidence matrix for the system. Let A and B be two $v \times b$ such incidence matrices. Define

$$G_0 = \begin{pmatrix} A & 0 \\ 0 & B \end{pmatrix} \text{ and } G_1 = \begin{pmatrix} A & I \\ I & B \end{pmatrix}.$$

The next lemma is immediate.

LEMMA 2. *G_0 and G_1 are the incidence matrices of distinct critical systems on $2v$ points and $2b$ blocks.*

Note that the '0' and '1' operations can be repeatedly applied, resulting in matrices such as

$$((G_0)_1)_1 = \left(\begin{array}{cc|cc|cc} AO & I & & & & I \\ OB & & & & & \\ I & AO & & & & \\ & OB & & & & \\ \hline & & & AO & & \\ & & & OB & I & \\ I & & & & AO & \\ & & & I & OB & \end{array}\right)$$

In comparison with the direct product construction, we note that a block in G_0 or G_1 has the same number of critical sets as the corresponding block in A or B. Moreover, the maximal possible antichain size in G_0 or G_1 is $2\binom{v}{\lfloor \frac{v}{2} \rfloor}$.

4. ***Determining Sets.***

Let $S = (\mathcal{P}, \mathcal{B}, \mathcal{C})$ be a critical system. Take one critical set C_i for each block. If no C_i is the empty set, then $D = \cup C_i$ forms a 1-*blocking set* in the sense of Ball and Blokhuis [2], that is, each block meets D in at least one point. If, in addition, no block is contained in D, then D is a *blocking set* in the sense of Bruen [7].

We note that a 1-*blocking set* need not necessarily give rise to a family of critical sets in a natural way. This is exhibited by the following example.

Let $\mathcal{B} = \{\{1,2,3\}, \{2,3,6,8\}, \{4,5,6\}, \{4,7,8\}\}$ be the blocks of a system on the eight points $1, 2, \ldots 8$. Then $X = \{2,3,4\}$ is a blocking set. Each point, $2, 3, 4$, is on two blocks. The pair $\{2,3\}$ is in two blocks. No other non-empty subset of X occurs in any block. Thus X cannot determine critical sets for the blocks in $\mathcal{B}$.

This leads us to the following definition and lemma.

Definition. Let $\mathcal{P}$ be a non-empty set of elements and $\mathcal{B}$ a non-empty set of subsets of $\mathcal{P}$. Let D be a subset of $\mathcal{P}$ with the property that $D \cap \mathcal{B}_i \neq D \cap \mathcal{B}_j$ for all distinct elements B_i,B_j of $\mathcal{B}$, and no $D \cap \mathcal{B}_i = \varnothing$. Then D is called a *determining set* for the pair $(\mathcal{P}, \mathcal{B})$.

LEMMA 3. *Let $(\mathcal{P}, \mathcal{B}, \mathcal{C})$ be a critical system and for each $B_i \in \mathcal{B}$ choose $C_i \in \mathcal{C}$ with $C_i \subseteq B_i$. Then $(\mathcal{P}, \mathcal{B})$ has determining set $\cup C_i$.*

Proof. Let $D = \cup C_i$. Suppose that for some $B_i \neq B_j$ we have $D \cap B_i = D \cap B_j$. Since $C_i \subseteq D \cap B_i = D \cap B_j$, it follows that $C_i \subseteq B_i \cap B_j$ which contradicts the fact that each critical set is contained in a unique block. Therefore $D \cap B_i \neq D \cap B_j$ for $B_i \neq B_j$ and so D is a determining set. □

That the converse is false can be seen by examining the example of section 1. The set $D = \{2,3\}$ is easily checked to be a determining set. The block intersections with D are $\{2,3\}$ $\{2\}$ and $\{3\}$. These clearly cannot constitute a set of critical sets.

In the Fano plane [3], any set of four points including a line forms a determining set. In any projective plane of order $q > 2$, the points of a triangle of lines, without the points of intersection, form a determining set.

We are particularly interested in connections between determining sets and linear codes and so will concentrate, for the remainder of the section, on determining sets in projective geometries. However, we first present a result in the general situation which classifies determining sets in terms of *blocking sets* which have been well studied in projective spaces.

Definition. A *minimal blocking set* is a blocking set such that each of its points is on at least one tangent. (The notion of *t-blocking* has been considered by many people. See for instance [2].)

LEMMA 4. *Let $S = (\mathcal{P}, \mathcal{B})$ be a point/block system in which each block is uniquely determined by any pair of its points. Then a subset X of $\mathcal{P}$ is a determining set for S if and only if X is a 1-blocking set and each point of X is on at most one tangent block to X.*

Proof. Suppose X is a determining set. Then each block meets X. Suppose some point of X is on two tangent blocks B_1 and B_2. Then $X \cap B_1 = X \cap B_2$ gives a contradiction. Conversely, if X is a determining set, suppose $X \cap B_1 = X \cap B_2$ for distinct blocks B_1 and B_2. Then $|B_1 \cap B_2| \leq 1$ implies that $X \cap B_1$ and $X \cap B_2$ are singleton sets and so we have two tangents to X at a point, a contradiction. □

If D is a minimal blocking set in projective plane of order q, it is well known [8] that $q + \sqrt{q} + 1 \leq |D| \leq q\sqrt{q} + 1$. Minimal blocking sets will, in general, have too many tangents to be determining sets; but the extremal case $|D| = q\sqrt{q} + 1$, provides an example of a blocking set for which each point is on a unique tangent, known as a *unital.*

Definition. A *semioval* in a system $S = (\mathcal{P}, \mathcal{B})$ is a subset X of the point set such that each point of X is on a unique tangent block to X. Hubaut [16] proved that if S is a semioval in a projective plane of order q, then $q + 1 \leq |S| \leq q\sqrt{q} + 1$. Classic examples of semiovals in projective planes are ovals (on $q + 1$ points) and unitals. However, ovals are not 1-blocking sets, and so not determining sets. An example of a blocking semioval that can be constructed in every projective plane is a triangle of lines with the intersections of the lines deleted. This set of $3(q - 1)$ lines has line intersection sizes 1, 3 and $q - 1$.

Given a determining set X in a projective plane, if X has no lines of size two, then removing a single point results in a new determining set. In fact, the removal of an arbitrary subset of points Y of X will still produce a determining set as long as no line of X is reduced to a single point.

A determining set D in a projective plane is said to be *regular* if, for each positive integer i, all points of D are on the same number of lines of size i in D. Hence, unitals and the triangle example are regular determining sets.

In $PG(2, q)$ many examples of regular determining sets can be found using the
following

CONSTRUCTION. *Let G be a Singer group [17] for $PG(2, q)$, and d a divisor of q^2+q+1. Let H be a subgroup of G of order d. Let $\{H_i \mid i \in \{1, \cdots, (q^2+q+1)/d\}$ be the point orbits under H. Then*

(a) if any line meets each H_i, then each H_i is a 1-blocking set (and is blocking if $d < q^2 + q + 1$), $1 \leq i \leq (q^2 + q + 1)/d$.

(b) if any line meets each H_i, but meets at most one H_i in a unique point, then each H_i is a regular determining set, $1 \leq i \leq (q^2 + q + 1)/d$.

(c) if any line meets each H_i, but meets precisely one H_i in a unique point, then each H_i is a regular blocking semioval, $1 \leq i \leq (q^2 + q + 1)/d$.

Using this method, J. Dover used Magma [10] to compute determining sets in $PG(2, q)$ for $q < 900$. We report the results in the table below for $q < 200$. Since $q^2 + q + 1$ prime will give no results, we delete all of these cases. In addition, any determining set obtained by this construction will be a blocking set, i.e. will not contain a line, and so $q + \sqrt{q} + 1 \leq d \leq q\sqrt{q} + 1$ may be assumed. In fact d cannot equal $q + \sqrt{q} + 1$ as this gives a Baer subplane [6] which can never be a

determining set. Thus, we also delete from the table below all values for q for which a factorization of q^2+q+1 includes no d in the range $q+\sqrt{q}+1 < d \leq q\sqrt{q}+1$.

q	determining sets: no of points/intersection sizes
7	19 pts $\{1,3,4\}$. This is a semioval [18].
9	none
11	none
13	none
16	91 pts $\{3,7\}$.
23	none
25	93 pts $\{3,8\}$; 217 pts $\{7,12\}$.
29	none
32	none
37	201 pts $\{3,7,8\}$.
47	none
49	817 pts $\{13,16,21\}$.
61	291 pts $\{3,4,6,11\}$.
64	219 pts $\{3,11\}$; 1387 pts $\{19,27\}$.
67	none
79	none
81	949 pts $\{4,13\}$.
83	none
107	889 pts $\{4,8,9,12\}$.
109	none
113	991 pts $\{6,7,8,12,15\}$.
121	399 pts $\{3,14\}$; 703 pts $\{3,5,6,7,11\}$; 777 pts $\{2,4,6,7,9,10\}$; 2109 pts $\{13,20,21\}$; 4921 pts $\{37,48\}$.
125	829 pts $\{4,9\}$.
128	2359 pts $\{14,21,24\}$.
137	none
139	1497 pts $\{7,10,11,16\}$.
149	721 pts $\{3,4,5,7,15\}$.
151	1093 pts $\{4,5,7,9,13,15\}$.
163	1273 pts $\{5,7,9,11,16\}$; 1407 pts $\{5,6,7,9,12,13\}$.
169	9577 pts $\{49,57,64\}$.
181	none
191	1183 pts $\{3,4,5,6,7,9,10\}$.
193	1783 pts $\{3,4,6,9,10,13,14\}$.
197	2053 pts $\{7,8,9,10,11,17\}$.

Only one additional blocking semioval was found, for $q = 211$ (the next case in the table). Results on blocking semiovals will appear in [5]

So far, our constructions are only of determining sets in projective planes. For the coding theory context, we would like to extend the planar situation to higher dimensions. The following theorem allows us to make this extension.

THEOREM 1. *Any set of points X in $PG(m-1,q)$ with at most one tangent line to X at each point of X extends to a set, with the same property, of $PG(m,q)$, $m \geq 3$.*

Proof. Let X be a set with the property described in the statement of the theorem in $S_{m-1} = PG(m-1,q)$. Let α be a generator of the Singer group G of $S_m = PG(m,q)$. Then α is regular on hyperplanes of S_m and so there is a 1-1 correspondence between α^i and hyperplanes of $S_m, 1 \leq i \leq |G|$. Let X_i be the copy of X in each hyperplane H_i under α^i, and let $X^\alpha = \bigcup_{i=1}^{|G|} X_i$. We claim that X^α has the tangent property: let $x \in X^\alpha$ be on two tangent lines ℓ_1 and ℓ_2. The plane $\langle \ell_1, \ell_2 \rangle$ sits in a hyperplane H_i of S_m for which $x \in X_i$ and x is on two tangents to X_i in H_i. This is a contradiction. □

COROLLARY. *Any determining set in $PG(m-1,q)$ extends to a determining set in $PG(m,q), m \geq 3$.*

Proof. It is easy to see that if each line of $PG(m-1,q)$ meets X in the above proof, then each line of $PG(m,q)$ meets X^α. □

5. ***Codes and skew n-arcs.***

In this section we use standard terminology and results for linear codes as found for instance in [15] or [21]. A *linear* $[n,k,d]$ *code* is a k-dimensional subspace of $V(n,q)$, the n-dimensional vector space over $GF(q)$, which has *minimum weight* at least d. A *generator matrix* G for such a code is a $k \times n$ matrix whose rows generate the subspace. A *parity check matrix* for such a code is an $(n-k) \times n$ matrix H such that $GH^t = 0$. The code has minimum weight $\geq d$ if and only if every set of $\leq d-1$ columns of H is linearly independent. The value $r = n-k$ is also called the *redundancy.*

The following result gives the fundamental connection between determining sets and codes in case $q = 2$. It is not difficult to see that the statement is false for $q > 2$.

THEOREM 2 (L. M. Batten and A. Khodkar). *Let K be a subset of $PG(m,2)$ with $|K| = n$ and $\dim\langle K \rangle = r-1$. Let H be an $(m+1) \times n$ matrix whose columns are the vectors of K in $V(m+1,2)$ in any fixed order. Let $C = \{x \in GF(2)^n \mid Hx^t = 0\}$. Then $PG(m,2) \backslash K$ is a determining set if and only if C is an $[n, n-r, 5]$ code.*

Proof. Suppose C is an $[n, n-r, 5]$ code. Then no set of < 5 columns of H is dependent. Thus K contains no line of $PG(m,2)$, whence $PG(m,2) \backslash K$ is blocking. Moreover, a point of $PG(m,2) \backslash K$ on two tangents corresponds to four dependent vectors of K (coplanar points of $PG(m,2)$). Thus $PG(m,2) \backslash K$ is a determining set.

In the other direction, C is clearly an $[n, n-r, d]$ code for some d. If $PG(m,2) \backslash K$ is a determining set, it follows that K contains no set of 2, 3, or 4 dependent points, and so $d \geq 5$. □

The set of vectors K in the above proof has, for $d \geq 5$, a property which we wish to isolate. It motivates the next definition.

Definition. A *skew n-arc*, $n \geq 1$, in a point/block system $(\mathcal{P}, \mathcal{B})$ is a subset K of the point set such that no three points of K are collinear, and no four points of K lie on two blocks which meet in $\mathcal{P}$.

In $PG(m, 2), m \geq 2$, the complement of a determining set is a skew n-arc for some n. In general, this is false for $PG(m, q), q > 2$. So an analogue for Theorem 2 in the general case is properly given in terms of skew n-arcs:

THEOREM 2'. *Let K be a subset of $PG(m, q)$ with $|K| = n$ and $\dim\langle K\rangle = r-1$. Let H be an $(m+1) \times n$ matrix whose columns are the vectors of K in $V(m+1, q)$ in any fixed order. Let $C = \{x \in GF(q)^n \mid Hx^t = 0\}$. Then K is a skew n-arc in $PG(m, q)$ if and only if C is an $[n, n-r, 5]$ code.*

In $PG(m, 2)$ a skew $(m+2)$-arc can be obtained by taking the standard basis of $m+1$ unit vectors and adding the all 1's vector. In general, this is far from the best possible obtainable in terms of size.

In $PG(m, q)$ with determining set D, the set $\{\ell \cap D \mid \ell \text{ a line of } PG(m, q)\}$ forms a critical set for the geometry. Hence lemmas 1 and 2 can be used to obtain critical systems for recursively defined structures.

Finding (maximal) skew n-arcs in projective geometries is therefore of considerable interest since it relates to the determination of (maximal) linear codes of minimum distance 5. For minimum distance $d = 4$, linear codes correspond to *n-caps*, sets of points in $PG(m, q)$ no three of which are collinear. These have been much studied by many people; see for instance [9] and its references. Brouwer and Verhoeff [6] gives tables of values for n, k and d which are of considerable value when constructing codes. See also Dumer [13] for an examination of bounds on code parameters relative to fixed minimum distance.

Recent work of Karpovsky, Chakrabarty and Levitin [19] examine properties similar to those of determining sets and relations with coding theory. They investigate the problem of covering the vertices of a graph G such that each vertex of G is uniquely identified by the vertices that cover it. Formally, the question is posed as follows: Given an undirected graph G and an integer $t \geq 1$, find a (minimal) set of vertices $\mathcal{C}$ such that every vertex of G belongs to a unique set of balls of radius t centered at the vertices in $\mathcal{C}$. Then $\mathcal{C}$ is viewed as an identifying code such that all vertices in it are codewords.

Let A be a set of non-negative integers and for a fixed integer n, let $s(A, n)$ denote the number of solutions of $a + a' = n$ with $a, a' \in A$, $a \leq a'$. If $s(A, n) \leq 1$ for all n, then A is called a *Sidon set* [14]. Thus n is determined by at most one pair (a, a') of integers of A, $a \leq a'$. Connections between Sidon sets and coloured hypergraphs were given in [20].

The author wishes to thank the referee for pointing out some of the references above.

REFERENCES

1. Anderson, I., *Combinatorics of Finite Sets*, Oxford University Press, Oxford, New York, 1987.
2. Ball, S. and Blokhuis, A., 'On the size of a double blocking set in $PG(2, q)$', submitted.
3. Batten, L. M., *Combinatorics of finite geometries*, Cambridge University Press, 2nd edition, Cambridge, New York, 1997.
4. Batten, L. M. 'Protocol for a private key cryptosystem with signature capability based on blocking sets in t-design', submitted.
5. Batten, L. M. and Dover, J. 'Blocking semiovals with three intersection sizes', preprint.
6. Brouwer, A. E. and Verhoeff, T., 'An updated table of minimum-distance bounds for binary linear codes', *IEEE Trans. on Inf. Theory 39* No. 2 (1993), 662–677.
7. Bruen, A. A., 'Baer subplanes and blocking sets', *Bull. Amer. Math. Soc. 76* (1970), 342–344.
8. Bruen, A. A. and Thas, J. A. 'Blocking sets', *Geom. Ded. 6* (1977), 193–203.
9. Bruen, A. A., Thas, J. A. and Blokhuis, A., 'On M. D. S. codes, arcs in $PG(n, q)$ with q even, and a solution of three fundamental problems of B. Segre.' *Invent. Math. 92* (1988), 451–459.
10. Cannon, J. and Playoust, C. An introduction to Magma, University of Sydney, Sydney, 1993.
11. Dantzig, G. B. and Hoffman, A. J., 'Dilworth's theorem on partially ordered sets' in *Linear Inequalities and Related Systems, Annals of Math Studies* no. *38*, (Ed. Kuhn and Tucker) (1956), 207–214.
12. Dilworth, R. P., 'A decomposition theorem for partially ordered sets'. *Ann. Math. 51* (1950), 161–165.
13. Dumer, I., 'Nonbinary double error-correcting codes designed by means of algebraic varieties'. IEEE *Trans. Inf. Theory 41* (1995), 1657–1666.
14. Graham,R. L., Grötschel, M. and Lovász, L. *Handbook of Combinatorics*, MIT Press, Oxford, Cambridge, Tokyo, 1995.
15. Hill, R., *A First Course in Coding Theory*, Oxford University Press, Oxford, New York, 1988.
16. Hubaut, X. 'Limitation du nombre de points d'un (k, n) arc régulier d'un plan projectif fini', *Accad. Naz. Lincei Ser. 8 48*, No. 5 (1970), 490–493.
17. Hughes, D. R. and Piper, F. C., *Design Theory*, Cambridge University Press, Cambridge, New York, 1985.
18. Innamorati, S. and Maturo, A., 'The spectrum of minimal blocking sets', submitted.
19. Karpovsky, M. G., Chakrabarty, K. and Levitin, L. B., 'On a new class of codes for identifying vertices in graphs'. *IEEE Trans. Inf. Theory 44* (1998), 599–611.
20. Lefmann, H., Rödl, V. and Wysocka, B., 'Multicolored subsets in colored hypergraphs'. *J. Comb. Theory (A) 74* (1996), 209–248.

21. Pless V., *Introduction to the theory of error-correcting codes*, John Wiley and Sons, New York, Toronto, 1982.
22. Sperner, E., 'Ein Satz über Untermengen einer endlichen Menge.' *Math. Z.* *27* (1928), 544–548.

(Received 21/10/99; revised 14/1/2000)