Recursive constructions for large caps

Yves Edel
Mathematisches Institut der Universität
Im Neuenheimer Feld 288
69120 Heidelberg (Germany)
Jürgen Bierbrauer
Department of Mathematical Sciences
Michigan Technological University
Houghton, Michigan 49931 (USA)

July 22, 1997

Abstract

We introduce several recursive constructions for caps in projective spaces. These generalize the known constructions in an essential way and lead to new large caps in many cases. Among our results we mention the construction of $\{(q+1)(q^2+3)\}-$caps in $PG(5,q)$ and of $\{q^4+2q^2\}$-caps in $PG(6,q)$.

1 Introduction

A **cap** in $PG(k-1,q)$ is a set of points no three of which are collinear. If we write the n points as columns of a matrix we obtain a (k,n)-matrix such that every set of three columns is linearly independent, hence the generator matrix of a linear orthogonal array of strength 3. This is a check matrix of a linear code with minimum distance ≥ 4. We arrive at the following:

Theorem 1 *The following are equivalent:*

- *A set of n points in $PG(k-1,q)$, which form a cap.*
- *A q-ary linear orthogonal array of length n, dimension k and strength 3.*
- *A q-ary linear code $[n, n-k, 4]_q$.*

Denote by $m_2(k-1,q)$ the maximum cardinality of a cap in $PG(k-1,q)$. In the binary case this is a trivial problem. In fact, choosing all nonzero $(k-1)$-tuples as columns we obtain a binary $(k-1, 2^{k-1}-1)$-matrix of strength 2, where the number of rows is clearly maximal. The dual is a binary code $[2^{k-1}-1, 2^{k-1}-k, 3]_2$. Addition of a parity-check bit yields $[2^{k-1}, 2^{k-1}-k, 4]_2$. We conclude

$$m_2(k-1,2) = 2^{k-1}.$$

We can assume $q > 2$ in the sequel. For small dimensions there is no problem. Trivially $m_2(1,q) = 2$. It is an easy exercise to show that the solution of the homogeneous equation $Z^2 = XY$ form a set of $q+1$ points in $PG(2,q)$ no three of which are collinear. This is maximal if q is odd. If q is a power of 2, then each such **oval** on $q+1$ points may be embedded in a **hyperoval** of $q+2$ points. In other words

$$m_2(2,q) = \begin{cases} q+1 & \text{if } q \text{ is odd} \\ q+2 & \text{if } q \text{ is even.} \end{cases}$$

In projective dimension 3 the situation is just as clear:

$$m_2(3,q) = q^2 + 1 \text{ if } q > 2.$$

(q^2+1)-caps in $PG(3,q)$ are known as **ovoids.** Just as in dimension 2 they may be constructed as elliptic quadrics.

2 The known recursive constructions

Only two general recursive constructions for large caps appear to be known. First of all there is Segre's construction from [6], which is based on ovoids and yields the following:

Theorem 2 (Segre) $m_2(l+3,q) \geq q^2 m_2(l,q)+1$,

By induction the following explicit bound is obtained:

$$m_2(3l,q) \geq (q^{2l+2}-1/(q^2-1),$$

as well as analogous bounds on $m_2(3l+1,q)$ and $m_2(3l+2,q)$.

The second general recursive construction is due to Mukhopadhyay [4]:

Theorem 3 (Mukhopadhyay) *Assume the following exist:*

1. *An n-cap in $AG(k,q)$, and*
2. *an m-cap in $PG(l,q)$.*

Then there is an mn-cap in $PG(k+l,q)$.

Mukhopadhyay applies this Theorem in cases $n=1,2,3$. In case $k=1$ this yields in particular the following doubling process:

Theorem 4 (doubling) $m_2(l+1,q) \geq 2 \cdot m_2(l,q)$.

Case $k=2$ yields

$$m_2(l+2,q) \geq \begin{cases} (q+1)\cdot m_2(l,q) & \text{if } q \text{ is odd} \\ (q+2)\cdot m_2(l,q) & \text{if } q \text{ is even.} \end{cases}$$

In case $k=3$ a slight strengthening leads him to another proof of Segre's Theorem 2.

3 A coding-theoretic explanation of the recursive constructions

We start by giving coding-theoretic proofs for some of the recursive constructions mentioned in Section 2. The following is known as the $(u,u+v)$-**construction** in the coding-theoretic literature.

Lemma 1 (**$(u, u+v)$-construction**) *Let C_i be codes $[n, k_i, d_i]_q, i = 1, 2$. Define a code C of length $2n$ whose codewords are parametrized by pairs (u, v), where $u \in C_1, v \in C_2$. The codeword of C parametrized by (u, v) is $(u|u+v)$. Then C is a code*

$$[2n, k_1 + k_2, min(d_2, 2d_1)]$$

If C_2 has parameters $[n, n-k, 4]$ we can choose C_1 to be the all-even code $[n, n-1, 2]$ and obtain a code $[2n, 2n-(k+1), 4]$. In geometrical language this is the doubling theorem 4. In fact, it yields a little more: as $q > 2$ the all-even code $[n, n-1, 2]$ contains a vector of weight n. This shows that the code C constructed via Lemma 1 also has maximum weight $2n$. Geometrically this means that there is a hyperplane, which avoids our point set. We obtain a point set contained in the affine geometry $AG(k, q)$.

Theorem 5 *If there is an n-cap in $PG(l, q)$, then there is a $2n$-cap in $AG(l+1, q)$.*

As an example we obtain a 20-cap in $AG(4, 3)$. This is known as the affine **Pellegrino cap** (see [5]). We can use Theorem 5 together with Theorem 3 and obtain

Theorem 6 $m_2(k+l+1, q) \geq 2 \cdot m_2(k, q) \cdot m_2(l, q)$.

It is known that $m_2(5, 3) = 56$. Application of Theorem 6 to the 56-cap in $PG(5, 3)$ (the **Hill cap**, see [3]) yields $m_2(l+6, 3) \geq 112 \cdot m_2(l, 3)$, in particular $m_2(9, 3) \geq 1120$ and $m_2(11, 3) \geq 6272$.
Theorem 3 can be proved by the basic coding-theoretic method of concatenation, which we use in the following form (see [2]):

Definition 1 (**Blokh-Zyablov concatenation**) *Let $\mathcal{C}_i$ be a linear Q_i-ary code $[N, K_i, D_i], i = 1, 2, \ldots, s$ (the* **outer codes***), where $Q_i = q^{h_i}$. Let further $\mathcal{E}_1 \subset \ldots \subset \mathcal{E}_s$ be a chain of linear q-ary codes $[n, k_i, d_i]$ (the* **inner codes***) such that the codimensions satisfy $k_i - k_{i-1} = h_i$. Put $h_1 = k_1$. Choose $\mathbb{F}_q$-isomorphisms $\alpha_i : \mathbb{F}_{Q_i} \longrightarrow U_i \subseteq \mathbb{F}_q^n$, where U_i is a complement of $\mathcal{E}_{i-1}$ in $\mathcal{E}_i$. The words of the* **concatenated code**

$$Concat(\mathcal{C}_1, \ldots, \mathcal{C}_s; \mathcal{E}_1 \subset \ldots \subset \mathcal{E}_s)$$

are in bijection with the s-tuples $(u_1, \ldots, u_s)$*, where* $u_i \in \mathcal{C}_i$*. The word of the concatenated code corresponding to* $(u_1, u_2, \ldots, u_s)$ *is* $\alpha_1(u_1) + \ldots + \alpha_s(u_s)$*, where the* α_i *are defined coordinatewise.*

Lemma 2 *The concatenated code* $Concat(\mathcal{C}_1, \ldots, \mathcal{C}_s; \mathcal{E}_1 \subset \ldots \subset \mathcal{E}_s)$ *of Definition 1 is a linear q-ary code with parameters* $[nN, \sum_{i=1}^{s} h_i K_i, min_i\{d_i D_i\}]$*.*

Proof: The length is obvious. The mapping from the s-tuples of words of the outer codes to the words of the concatenated code is clearly $\mathbb{F}_q$-linear. By construction the kernel of the mapping is trivial. The statement concerning the dimension follows. Consider a nonzero tuple $(u_1, u_2, \ldots, u_s)$, where $u_i \in \mathcal{C}_i$. Choose i maximal such that $u_i \neq 0$. Then $\alpha_i(u_i)$ has weight $\geq d_i D_i$. The addition of vectors $\alpha_j(u_j), j < i$ does not destroy this property. Here we use the fact that the $\mathcal{E}_i$ form a chain, and the choice of the U_i. ∎

Consider a chain $\mathcal{E}_1 \subset \mathcal{E}_2 \subset \mathcal{E}_3 \subset$ of q-ary codes with parameters

$$[n, n-(k+1), 4] \subset [n, n-1, 2] \subset [n, n, 1].$$

This chain will exist if and only if a code $\mathcal{E}_1$ with the given parameters exists, which contains a word of weight n. Geometrically this is equivalent to an n-cap in the affine geometry $AG(k, q)$. We have then $h_1 = n - (k+1), h_2 = k, h_3 = 1$. We use codes $\mathcal{C}_1 = [m, m, 1]_{Q_1}, \mathcal{C}_2 = [m, m-1, 2]_{q^k}$ and $\mathcal{C}_3 = [m, m-(l+1), 4]_q$. Observe that $\mathcal{C}_1, \mathcal{C}_2$ always exist, independent of the choice of m and l. Code $\mathcal{C}_3$ is equivalent to an m-cap in $PG(l, q)$. Concatenation yields a q-ary code with length nm, dimension $m[n-(k+1)] + (m-1)k + m - (l+1) = mn - (k+l+1)$ and minimum weight 4. We have proved the following:

Theorem 7 *Assume there exists a q-ary code* $[n, n-(k+1), 4]$ *whose dual has maximum weight n, and a q-ary code* $[m, m-(l+1), 4]$*. Then there exists a code*

$$[nm, nm-(k+l+1), 4]_q.$$

This is precisely Theorem 3, stated in terms of coding theory. Case $k = 1, n = 2$ yields Theorem 4. The special case leading to a code $[102, 96, 4]_4$ has been given by L.Tolhuizen in his Ph.D. thesis [7].
As ovoids are not affine we cannot apply Theorem 3 to cover a gap of three

in the dimension. In particular we have not given a satisfactory explanation of Theorem 2 yet. It is clear that a more general construction must exist, which covers the case when none of the two caps is contained in the affine geometry. This will be done in the following section.

4 New recursive constructions

Theorem 8 *Assume the following exist:*

1. *An n-cap $K_1 \subset PG(k,q)$ and a hyperplane H of $PG(k,q)$ such that $|K_1 \setminus H| = w$, and*
2. *an m-cap in $PG(l,q)$.*

Then there is an $\{wm+(n-w)\}$-cap in $PG(k+l,q)$.

Proof: We use the language of linear orthogonal arrays. We say that a matrix has **strength** t if any set of t of its columns is linearly independent. The assumptions of the Theorem guarantee the existence of the following q-ary matrices:

- A $(k+1,n)$-matrix A of strength three, whose first row has w entries $=1$ in the first columns, whose remaining entries are 0, and
- an $(l+1,m)$-matrix B of strength 3.

We have to construct a $(k+l+1, wm+n-w)$-matrix of strength three. Let a vary over the first w columns of A, b over the columns of B and α over the last $n-w$ columns of A. Denote by a' the k-tuple arising by omitting the leading entry 1 in column a. The columns of our matrix are defined as follows:

$$s(a,b) = (b,a') \text{ and } s(\alpha) = (0,\alpha),$$

where a, b, α vary as described above. Observe that the coordinate segments have lengths $l+1$ and k, respectively. We have to show that any three of these columns are linearly independent. It is clear that there is no 0-column and that no two of our columns are scalar multiples of each other. Assume some three columns are linearly dependent. We know that the coefficients of the dependency are nonzero. As A has strength three, at least one of the columns must have type $s(a,b)$. The first segment of coordinates shows that at least two columns must have this type. Assume one of the columns does have type $s(\alpha)$. The linear dependency looks as follows:

$$\lambda_1(b_1,a_1')+\lambda_2(b_2,a_2')+\lambda_3(0,\alpha)=0.$$

As B has strength 3 we conclude $b_1=b_2, \lambda_1+\lambda_2=0$. It follows $0=\lambda_1 a_1'+\lambda_2 a_2'+\lambda_3\alpha=\lambda_1 a_1+\lambda_2 a_2+\lambda_3\alpha$, a contradiction. We conclude that all three columns must have type $s(a,b)$. The linear dependency looks as follows:$\sum_{i=1}^3 \lambda_i(b_i,a_i')=0$. The first coordinate segment shows $b_1=b_2=b_3$ and $\sum_{i=1}^3\lambda_i=0$. The second segment now shows $\sum_{i=1}^3\lambda_i a_i=0$, hence $a_1=a_2=a_3$, contradiction.$\blacksquare$

Theorem 8 is a common generalization of Theorems 2 and Theorem 3. In fact, Theorem 2 is obtained as an application of Theorem 8 to ovoids. Theorem 3 is obtained in the special case $n=w$. It is observed in [4] that Theorem 3, when applied to two affine caps (case $n=w, m=v$) yields an affine cap. Our construction displays this feature, too (the first row of the resulting matrix has nonzero entries). Moreover our construction has another interesting property in this direction. Assume i rows of A have all entries nonzero (equivalently: there are i hyperplanes in general position, which avoid cap K_1). Then the resulting matrix still has $i-1$ rows with all entries nonzero. We obtain the following:

Corollary 1 *Assume the following exist:*

1. *An n-cap in $AG(k,q)$, which is avoided by $i\geq 2$ hyperplanes in general position, and*
2. *an m-cap in $PG(l,q)$.*

Then there is an mn-cap in $AG(k+l,q)$, which is avoided by some $i-1$ hyperplanes in general position.

This applies in particular in case $k=2$. As ovals and hyperovals certainly possess triangles of exterior lines we have $i=3$ (equivalently: a generator matrix of the (hyper)oval can be found, all of whose entries are nonzero). Repeated application of Corollary 1 yields the following:

Theorem 9 *The following caps exist, for all dimensions l, k, m :*

- *an $\{m_2(2,q)\cdot m_2(l,q)\}-$cap in $AG(l+2,q)$,*
- *an $\{m_2(2,q)\cdot m_2(l,q)\cdot m_2(k,q)\}-$cap in $AG(l+k+2,q)$, and*
- *an $\{m_2(2,q)\cdot m_2(l,q)\cdot m_2(k,q)\cdot m_2(m,q)\}-$cap in $PG(l+k+m+2,q)$.*

Among the applications of Theorem 9 we mention a 102-cap in $AG(5,4)$ and a 156-cap in $AG(5,5)$, both of which are avoided by two hyperplanes. What is a little unsatisfactory about Theorem 8 is that it does not use its ingredients in a symmetrical fashion. We symmetrize the approach. Let the following be given:

- A $(k+1,n)$-matrix A of strength three, whose first row has w entries $=1$ in the first columns, whose remaining entries are 0, and
- an $(l+1,m)$-matrix B of strength 3, whose first row has v entries $=1$ in the first columns, whose remaining entries are 0.

Denote by a one of the w first columns of A, by α one of the $n-w$ last columns. Analogously denote by b one of the v first columns of B, by β one of the $m-v$ of its last columns. Further a', α', b', β' are obtained by omitting the first entry (0 or 1). With this terminology the columns used in the proof of Theorem 8 are $(1,b',a')^t, (0,\beta',a')^t$ and $(0,0,\alpha')^t$. This exhibits the asymmetrical nature of the construction. Let us consider instead the columns of the following types:

$$(1,b',a')^t \text{ (type I) }, (0,\beta',a')^t \text{ (type II) }, (0,b',\alpha')^t \text{ (type III) }.$$

Observe that the coordinate segments have lengths 1,l and k, respectively. Theorem 8 shows that the columns of types I and II yield a matrix of strength 3. By symmetry the same is true of the columns of types I and III. Let the matrix M consist of all the columns of types I,II and III.
Our first aim is a recursive construction making more efficient use of ovoids. More in general let us consider the case $w=n-1, v=m-1$ (equivalently: each of our caps, $K_1 \subset PG(k,q)$ and $K_2 \subset PG(l,q)$ possesses a tangent hyperplane). We claim that M has strength three. In order to simplify the proof we choose notation such that the first column of A is $(1,0,0,\ldots,0)$,

likewise for the first column of B. This can be achieved by adding suitable multiples of the first row to the remaining rows.
We claim that column α' is not a multiple of any column a'. This is certainly true when a' is the zero column. If $a' \neq 0$ is a multiple of α', then we obtain a multiple of the first column as a linear combination of a and α, contradicting the fact that A has strength three.
We check at first that M has strength ≥ 2. It suffices to prove that no column of type II is a scalar multiple of a column of type III. Assume $\lambda \cdot (0, \beta', a') = \mu \cdot (0, b', \alpha')$. The last coordinate segment shows that $\lambda \cdot a' = \mu \cdot \alpha'$, a contradiction. It is now just as easy to show that M has strength 3. Assume three columns are linearly dependent. We know that the coefficients of the linear relation must be nonzero. We also know that a column of type II and a column of type III must be involved. If the third column has type I, then the first coordinate yields a contradiction. Because of symmetry we can assume that two columns of type III and one of type II are involved. The linear dependency looks as follows:

$$\lambda_1(0, b_1', \alpha') + \lambda_2(0, b_2', \alpha') + \lambda_3(0, \beta', a') = 0.$$

The last segment shows $(\lambda_1 + \lambda_2)\alpha' = -\lambda_3 a'$. By what we have shown above this forces $\lambda_1 + \lambda_2 = 0$. This together with the middle segment shows $\lambda_1 b_1 + \lambda_2 b_2 + \lambda_3 \beta = 0$, a contradiction to the fact that B has strength 3. We have proved the following:

Theorem 10 *Assume the following exist:*

1. *An n-cap $K_1 \subset PG(k, q)$ possessing a tangent hyperplane, and*
2. *an m-cap $K_2 \subset PG(l, q)$ possessing a tangent hyperplane.*

Then there is an $\{nm - 1\}$-cap in $PG(k + l, q)$.

This Theorem certainly applies when K_1 and K_2 both are ovoids. We obtain the following:

Theorem 11 $m_2(6, q) \geq q^4 + 2q^2$.

In particular $m_2(6, 4) \geq 288, m_2(6, 5) \geq 675$.

5 A product construction

Next we describe a general and very formal product construction.

Definition 2 • *Let $F : \mathbb{F}_q^u \longrightarrow \mathbb{F}_q^v$ be a mapping. Denote by $M(F)$ the family of all vectors $(x, y) \in \mathbb{F}_q^{u+v}$, where $y \in F(x)$. As we want to interpret $M(F)$ as a set of points in $PG(u+v-1, q)$, we add the condition that $F(\lambda \cdot x) = \emptyset$ whenever $F(x) \neq \emptyset$ and $\lambda \neq 0, 1$ (equivalently: x varies over a family of representatives of $PG(u-1, q)$). We may also consider $M(F)$ as a matrix, where the order of the columns is immaterial.*

- *Let $F : \mathbb{F}_q^u \longrightarrow \mathbb{F}_q^v$ and $G : \mathbb{F}_q^u \longrightarrow \mathbb{F}_q^{v'}$ as above be given. Here we choose notation such that if $F(x) \neq \emptyset$ and $G(\lambda \cdot x) \neq \emptyset$ for some $0 \neq \lambda \in \mathbb{F}_q$, then $\lambda = 1$. Define $(F \otimes G) : \mathbb{F}_q^u \longrightarrow \mathbb{F}_q^{v+v'}$ by*

$$(F \otimes G)(x) = \{(y, y') \mid y \in F(x), y' \in G(x)\}.$$

Here is the promised general product construction:

Theorem 12 *Let $F : \mathbb{F}_q^u \longrightarrow \mathbb{F}_q^v$ and $G : \mathbb{F}_q^u \longrightarrow \mathbb{F}_q^{v'}$. If $M(F)$ and $M(G)$ both have strength 3 (equivalently: are caps in $PG(u+v-1, q)$ and $PG(u+v'-1, q)$, respectively), then $M(F \otimes G)$ has strength 3 and hence represents a cap in $PG(u+v+v'-1, q)$.*

The proof of Theorem 12 is trivial. We make use of the following description of conic sections in $PG(2, q)$ and elliptic quadrics in $PG(3, q)$, which has been given in [1]:

Proposition 1 *Let q be a prime power. Consider $\mathbb{F}_q$ and its quadratic extension $\mathbb{F}_{q^2}$. Fix an element $a \in \mathbb{F}_q^*$.*

1. *The set of columns $(1, b)^t$, where $b \in \mathbb{F}_{q^2}$ varies over the elements satisfying $b^{q+1} = a$, has strength 3 (equivalently: this describes an oval in the projective plane of order q).*
2. *The columns $e_2 = (0 : 1 : 0 : \mathbf{0})^t$ and $(1 : a \cdot u^{q+1} : u)^t$, where u varies over $\mathbb{F}_{q^2}$, form an ovoid in $PG(3, q)$.*

We see that the ovoid given in Proposition 1 may be described in the language of Definition 2 by a function $F : \mathbb{F}_q^2 \longrightarrow \mathbb{F}_q^2$, where $F(1,0) = F(0,1) = \{(0,0)\}$ and $|F(x)| = q+1$ for all $x = (1,\alpha), 0 \neq \alpha \in \mathbb{F}_q$. Direct application of Theorem 12 to two copies of this ovoid yields a cap in $PG(5,q)$ of size $1+1+(q-1)(q+1)^2$. We will refine this construction as follows:
Consider three types of points in $PG(5,q)$: type I consists of all (x,y,z), where $x = (1,\alpha)$ as above and $y^{q+1} = z^{q+1} = \alpha$. Type II consists of all 6-tuples $(x', 0, \zeta)$, where $x' = (1,0)$ or $= (0,1)$ and $\zeta^{q+1} = 1$. Type III consists of all columns $(x', \rho, 0)$, with x' as above and $\rho^{q+1} = \alpha_0$. Here $\alpha_0 \in \mathbb{F}_q \setminus \{0,1\}$ is fixed. This defines a set of $(q-1)(q+1)^2 + 4(q+1) = (q+1)(q^2+3)$ points in $PG(5,q)$. We claim that they form a cap.
It follows from Theorem 12 that the points of type I form a cap. Proposition 1 shows that the same if true of the points of type II and of those of type III. It is also clear that no two of our vectors are scalar multiples of each other. Assume there is a nontrivial linear combination involving three of our columns. The middle set of coordinates shows that at most one of them can have type II. Likewise at most one can have type III. It follows that at least one point of type I has to be involved. Assume two points of type I are involved. If the third point has type II, then the first two coordinate sets yield a contradiction. If the third point has type III, then the first and the last set of coordinates taken together yield a contradiction. We conclude that the only critical case is when one column of each type is involved. The linear combination looks as follows:

$$\lambda_1 \cdot (x_1, y_1, z_1) + \lambda_2 \cdot (a', 0, \zeta) + \lambda_3 \cdot (b', \rho, 0) = 0.$$

Here $x_1 = (1,\alpha) \in \mathbb{F}_q^2$ and $y_1^{q+1} = z_1^{q+1} = \alpha$. The last coordinate section shows $\lambda_1 z_1 = -\lambda_2 \zeta$, the middle section shows $\lambda_1 y_1 = -\lambda_3 \rho$. Consider the first section. It is impossible that $a' = b'$. We have to consider two cases:
Assume $a' = (1,0), b' = (0,1)$. Then $\lambda_2 = -\lambda_1, \lambda_3 = -\lambda_1 \alpha$. Together with the equations above we get $z_1 = \zeta, y_1 = \alpha\rho$. Raising to the $(q+1)^{th}$ power we obtain $\alpha = 1$ and $\alpha = \alpha^2 \alpha_0$, hence $\alpha_0 = 1$, contradiction.
The second case is $a' = (0,1), b' = (1,0)$. Then $\lambda_3 = -\lambda_1, \lambda_2 = -\lambda_1 \alpha$. We obtain $y_1 = \rho, z_1 = \alpha\zeta$. Raising to the $(q+1)^{th}$ power yields $\alpha = \alpha_0$ and $\alpha = \alpha^2$. We obtain the contradiction $\alpha_0 = \alpha = 1$. We have proved the following:

Theorem 13 *There is a $\{(q+1)(q^2+3)\}-$cap in $PG(5,q)$.*

Moreover we have given an effective description of such a cap. In particular we obtain $m_2(5,5) \geq 168$.

References

[1] Y.Edel and J.Bierbrauer: *A family of caps in projective 4-space in characteristic 2,* submitted to *Rendiconti di Matematica Pura ed Applicata.*

[2] E.L.Blokh, V.V.Zyablov:*Coding of generalized concatenated codes, Probl. Information Transmission* **10** (1974),218-222.

[3] R.Hill: *On the largest size of cap in* $S_{5,3}$, *Atti Accad. Naz. Lincei Rendiconti* **54**(1973),378-384.

[4] A.C. Mukhopadhyay: *Lower bounds on* $m_t(r,s)$, *Journal of Combinatorial Theory A* **25**(1978),1-13.

[5] G.Pellegrino: *Sul massimo ordine delle calotte in* $S_{4,3}$, *Matematiche (Catania)***25**(1970),1-9.

[6] B. Segre: *Le geometrie di Galois, Ann.Mat.Pura Appl.***48** (1959),1-97.

[7] L.M.G.M. Tolhuizen: *Cooperating error-correcting codes and their decoding,* Ph.D. dissertation, Eindhoven University of Technology, Eindhoven, The Netherlands, June 1996.