Large caps

Jürgen Bierbrauer
Department of Mathematical Sciences
Michigan Technological University
Houghton, Michigan 49931 (USA)

January 29, 2002

1 Introduction

A **cap** is a set of points no three of which are collinear. We study the following question:

Problem 1. *What is the maximum number of points of a cap in projective geometry $PG(N, q)$ and in affine geometry $AG(N, q)$?*

Denote by $m_2(N, q) = m_2(PG(N, q))$ the maximum size of a cap in $PG(N, q)$ and by $m_2(AG(N, q))$ the maximum size of a cap in $AG(N, q)$. The binary case is not very interesting as $AG(N, 2)$ is a cap. It follows $m_2(N, 2) = m_2(AG(N, 2)) = 2^N$. In the sequel we assume $q > 2$.

Let $\mathcal{K} \subset PG(k-1, q)$ be a cap, where $|\mathcal{K}| = n$. We can represent $\mathcal{K}$ by a (k, n)-matrix M with entries from $\mathbb{F}_q$, whose columns are representatives for the points in $\mathcal{K}$. The defining condition of a cap (n points from $PG(k-1, q)$, no three on a line) is equivalent to the statement that no three columns of M are linearly dependent. Let $\mathcal{C} = \mathcal{C}(M)$ be the vector space (code) generated by the rows of M, and $\mathcal{C}^\perp$ its dual with respect to the dot product. It should be noted that M and $\mathcal{C}(M)$ are not canonically determined by $\mathcal{K}$. This is due to the fact that we have to choose representatives for the points of $\mathcal{K}$ to determine the columns of M. Each column is determined only up to nonzero multiples by $\mathcal{K}$. While this choice has no influence on the basic parameters of the code and its dual (length, dimension, distance distribution, strength) it does have an influence on the parameters of subfield codes, for example.

We have $dim(\mathcal{C}^\perp) = n - k$ (it can be assumed that M has rank k as otherwise $\mathcal{K}$ would be a cap in a lower-dimensional projective space), and the minimum distance of $\mathcal{C}^\perp$ is ≥ 4. On the other hand, the columns of a check matrix of a code $[n, n-k, 4]_q$ form a cap in $PG(k-1, q)$. The minimum distance of $\mathcal{C}(M)$ is the minimal intersection size of $\mathcal{K}$ with the complement of a hyperplane. A different point of view is obtained by writing out the elements of $\mathcal{C}(M)$ as rows of a matrix and interpreting them as points of a sample space. Each of the n columns of the array defines a random variable on $\mathcal{C}(M)$ with values in $\mathbb{F}_q$. The defining property of a cap, equivalently the linear independence of any three columns of M, says that any three of the n random variables are statistically independent. In design-theoretic terms this is equivalent to stating that $\mathcal{C}(M)$ is a linear **orthogonal array** of strength 3.

Proposition 1. *The following are equivalent:*

- *An n-cap $\mathcal{K} \subset PG(k-1, q)$, which is not contained in a hyperplane,*
- *a (k, n)-matrix M of rank k with entries from $\mathbb{F}_q$ such that any three columns are linearly independent,*
- *a linear code $[n, k]_q$, which is an orthogonal array of strength* 3,
- *a linear code $[n, n-k]_q$ of minimum distance ≥ 4.*

Proposition 1 shows in particular that the theory of caps in projective spaces over finite fields is identical to the theory of linear codes of minimum distance 4. Each of the equivalent statements of Proposition 1 (geometric, linear algebraic, statistical, coding theoretic) indicates its own type of application. Each of these points of view motivates generalizations. In coding theory a natural generalization of linear codes with minimum distance 4 are high-dimensional codes with small minimum distance, for instance $d \leq 5$. Another natural coding-theoretic generalization is from the linear to the additive case. From a statistical point of view it is natural to relax the condition of statistical independence (of any three random variables) in some way. We will come back to these and other generalizations later in this text.

2 The canonical models

In projective dimensions 2 and 3 quadrics yield canonical models for caps. In this section we use vector space dimensions. Let V be a vector space over $\mathbb{F}_q$. If q is odd, then **symmetric bilinear forms** on V are equivalent to **quadratic forms** on V : the quadratic form determined by $(,)$ is $Q(x) = (x, x)$, the symmetric bilinear form defined by the quadratic form Q is

$$(x, y) = \frac{1}{2}(Q(x + y) - Q(x) - Q(y)).$$

The **radical** $Rad(V)$ is the subspace of vectors, which are orthogonal to the whole space V. A symmetric bilinear form is **non-degenerate** if $rad(V) = 0$ (equivalently: the Gram matrix has nonzero determinant).

Let $V = V(d, q)$ with non-degenerate symmetric bilinear form $(,)$ and corresponding quadratic form Q, where q is odd. The corresponding **quadric** $Var(Q)$ (Var stands for *variety*) consists of the points in $PG(d-1, q)$ on which Q vanishes (the **isotropic points**). Fix a non-square $c_0 \in \mathbb{F}_q$. Call V **anisotropic** if $Q(v) \neq 0$ for all $v \neq 0$. It is easy to see that necessarily $d \leq 2$ in this case, and a 2-dimensional anisotropic space has a basis v_1, v_2 such that $(v_1, v_1) = 1, (v_1, v_2) = 0, (v_2, v_2) = -c_0$. As the structure is uniquely determined it is clear that every nonzero field element is represented equally often, hence $q+1$ times, under Q. Anisotropic 2-dimensional spaces represent projective lines not containing a point of the quadric.

Let now $d = 3$. We can choose $v_1 \neq 0$ such that $(v_1, v_1) = 0$. As $v_1 \notin Rad(V)$ we can find v_2 such that $(v_1, v_2) = 1$. Replacing v_2 by $av_1 + v_2$ if necessary we can assume $(v_2, v_2) = 0$. Let $H = \langle v_1, v_2 \rangle$. Then H (a **hyperbolic plane**) is non-degenerate. It follows that we have an orthogonal decomposition $V = H \perp H^\perp$, where $H^\perp$ is non-degenerate. As we are in dimension $d = 3$ the process ends here: $V = H \perp \langle v_3 \rangle$, where $(v_3, v_3) \neq 0$. We can choose either $(v_3, v_3) = 1$ or $(v_3, v_3) = c_0$.

Let $h(1, c)$ be the number of vectors v in a hyperbolic plane such that $Q(v) = c$. Clearly $h(1, 0) = 2q - 1$ and $h(1, c) = q - 1$ for all $c \neq 0$. A hyperbolic plane represents a projective line containing 2 points of the quadric. Let $g(1, c)$ be the corresponding representation numbers in our $V(3, q)$. We have $g(1, 0) = (2q - 1) + \frac{q-1}{2}(q - 1)2 = q^2$. The number of isotropic points in $PG(2, q)$ is therefore $(q^2 - 1)/(q - 1) = q + 1$. These form the points of a $(q + 1)$-cap in $PG(2, q)$.

Consider $d = 4$. The inductive process shows that only two situations can occur: either $V = H_1 \perp H_2$ is orthogonal sum of two hyperbolic planes (this is the **hyperbolic** or $(+)$- or dihedral case) or $V = H \perp A$ is the orthogonal sum of a hyperbolic plane and a 2-dimensional anisotropic space (this is the **elliptic** or $(-)$- or quaternion case). Let $h(2,c)$ be the representation numbers of the quadratic form in the 4-dimensional hyperbolic case and $e(2,c)$ the corresponding numbers for the elliptic case. Using the numbers $h(1,c)$ we obtain $h(2,0) = (2q-1)^2 + (q-1)^3 = q^3 + q^2 - q$. The number of points on the hyperbolic quadric in $PG(3,q)$ is therefore $(q^3 + q^2 - q - 1)/(q-1) = (q+1)^2$. The representation numbers for the 2-dimensional anisotropic type are of course $e(1,0) = 1, e(1,c) = q+1$ for all $c \neq 0$. Let $e(2,c)$ be the representation numbers for the 4-dimensional elliptic type. We have $e(2,0) = (2q-1)+(q-1)(q-1)(q+1) = q^3-q^2+q$. The number of points of the elliptic quadric in $PG(3,q)$ is therefore $(q^3-q^2+q-1)/(q-1) = q^2+1$.

The elliptic quadric in $PG(3,q)$ is a (q^2+1)-cap. The inductive process shows that in each even dimension d there will be two types of non-degenerate quadrics. As for $d \geq 5$ we can split off two hyperbolic planes (yielding lines in $PG(d-1,q)$ all of whose points are isotropic), these quadrics cannot be caps in $PG(d-1,q)$. Let us denote by $Q^+_{2d-1}(q)$ the hyperbolic quadric in $PG(2d-1,q)$ (the vector space $V(2d,q)$ is orthogonal sum of d hyperbolic planes), by $Q^-_{2d-1}(q)$ the elliptic quadric in $PG(2d-1,q)$ (the vector space is orthogonal sum of $d-1$ hyperbolic planes and a 2-dimensional anisotropic space). The corresponding representation numbers are $h(d,c)$ and $e(d,c)$, respectively.

How can we tell the elliptic from the hyperbolic case? With respect to the bases that we have chosen the Gram matrix of the 4-dimensional hyperbolic bilinear form has determinant 1, whereas in the 4-dimensional elliptic case the determinant is c_0. Change of basis introduces a quadratic factor in the determinant. This shows the following:

Theorem 1. *Let q be odd. A non-degenerate symmetric bilinear form in $V(4,q)$ is elliptic if and only if the determinant of the Gram matrix is a non-square.*

The same method works in arbitrary dimension. We see that quadrics do give us very good caps in $PG(2,q)$ and in $PG(3,q)$ whereas no caps are obtained in higher projective dimensions.

In characteristic 2 the quadratic form carries more information than the underlying bilinear symmetric form. The procedure of classifying the quadratic forms is analogous to the odd characteristic case, and the representation numbers are the same. It is an elementary observation that a $(q+1)$-cap in $PG(2,q)$ can be embedded in a $(q+2)$-cap if and only if q is a power of 2. For a geometric proof that q^2+1 is the maximum size of a cap in $PG(3,q), q>2$ see [26].

Theorem 2. *Let $q>2$. We have*

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

$m_2(3,q) = q^2+1$ *and* $m_2(AG(3,q)) = q^2$.

It is a combinatorial fact that an ovoid ((q^2+1)-cap in $PG(3,q)$) intersects each plane in either 1 or $q+1$ points, and each point of the ovoid is on exactly one tangent plane. This implies the last statement of Theorem 2. The **Tits ovoids** [41] form a family of ovoids in characteristic 2, which are not equivalent to elliptic quadrics.

Let us sum up: in projective dimension up to 3 we have canonical models for large caps. These are quadrics. In larger projective dimensions quadrics cannot be caps. Quadratic forms are derived from homogeneous polynomials of degree 2. Consider the case

$$Q(x_1,x_2,x_3,x_4) = \sum_{i=1}^{4} a_i x_i^2$$

in odd characteristic. The corresponding symmetric bilinear form is

$$(x,y) = \sum_{i=1}^{4} a_i x_i y_i,$$

where $x=(x_1,x_2,x_3,x_4), y=(y_1,y_2,y_3,y_4)$. This shows that the Gram matrix is the diagonal matrix $diag(a_1,a_2,a_3,a_4)$. The quadratic form is nondegenerate if and only if $a_i \neq 0$ for all i. We conclude from Theorem 1 that Q is elliptic if and only if $a_1a_2a_3a_4$ is a non-square. Let us specialize to $q=3$. Choose $a_1=-1=2, a_2=a_3=a_4=1$. The ovoid in $PG(3,3)$ is therefore described by the equation $x_1^2 = x_2^2+x_3^2+x_4^2$. The points of the ovoid are

$(0:1:1:1)$	$(1:0:0:1)$
$(0:1:2:1)$	$(1:0:0:2)$
$(0:2:1:1)$	$(1:0:1:0)$
$(0:2:2:1)$	$(1:0:2:0)$
	$(1:1:0:0)$
	$(1:2:0:0)$

3 The case of dimension 4

The case of projective dimension 4 is in a way particularly difficult. No canonical models are available and the dimension is too small to admit useful recursive constructions. The best known constructions are based upon ovoids in hyperplanes. We concentrate upon the following asymptotic problem:

Definition 1. *The pair (α, c) of positive numbers is* **asymptotically reachable** *by 4-dimensional caps if there is an infinite family of caps of size s_q in $PG(4,q)$ such that $lim_{q\rightarrow\infty} s_q/q^\alpha \geq c$. Exponent α is asymptotically reachable if (α, c) is asymptotically reachable for some $c > 0$.*

Problem 2. *Is an exponent $\alpha > 2$ asymptotically reachable by 4-dimensional caps?*

Using two ovoids in two different hyperplanes we see that $(\alpha, c) = (2, 2)$ certainly is asymptotically reachable. In characteristic 2 nothing better is known.

Problem 3. *Is $(2, c)$ asymptotically reachable by 4-dimensional caps in characteristic 2 for some $c > 2$?*

The following is from [38, 5].

Theorem 3. *$(\alpha, c) = (2, 2.5)$ is asymptotically reachable by 4-dimensional caps in odd characteristic.*

We sketch the construction in case $q \equiv 3(\text{mod } 4)$. Use homogeneous coordinates $(x_1 : x_2 : x_3 : x_4 : x_5)$ in $PG(4,q)$. Consider the hyperplanes $H_1 = (x_3 = 0), H_2 = (x_4 = 0)$ and $H_3 = (x_5 = 0)$. The quadrics $Q_i, i = 1,2,3$ are given by the following:

$$\begin{array}{rcl} Q_1(x) & = & x_1^2 + x_2^2 - x_4^2 + x_5^2 \\ Q_2(x) & = & x_1^2 + x_2^2 + x_3^2 - x_5^2 \\ Q_3(x) & = & x_1^2 + x_2^2 + 2x_3^2 - 2x_4^2 \end{array}$$

As observed in Section 2 the symmetric bilinear form corresponding to Q_1 is

$$(x,y)_1 = x_1y_1 + x_2y_2 - x_4y_4 + x_5y_5,$$

analogously for Q_2 and Q_3. The radicals of Q_i are $Rad(Q_i) = \langle e_{i+2} \rangle, i = 1,2,3$. In particular the restriction of Q_i to H_i is non-degenerate. As -1 is a non-square, it follows from Theorem 1 that $Var(Q_i) \cap H_i$ is an ovoid, in particular a cap in $H_i, i = 1,2,3$. We start from the point set $(Var(Q_1) \cap H_1) \cup (Var(Q_2) \cap H_2) \cup (Var(Q_3) \cap H_3)$ of $O(3q^2)$ points. Removing the points in the intersections $H_i \cap H_j$ does not change the asymptotic size. In the resulting set any 3 collinear points must be on a line l, which is not contained in any of the hyperplanes H_i (a **generic** line). The plan is to find a subset $U \subset Var(Q_3)$ of size $O(0.5q^2)$ such that no generic line l meets $Var(Q_1) \cup Var(Q_2) \cup U$ in 3 points.

Let l be a generic line and $P_i = l \cap H_i, i = 1,2,3$. Assume $P_i \in Var(Q_i)$, write $P_i = \langle v_i \rangle$. We can choose the representative v_i such that $v_1 + v_2 + v_3 = 0$. We have

$$\begin{array}{rcccl} v_1 & = & x & = & (x_1, x_2, 0, x_4, x_5) \\ v_2 & = & y & = & (y_1, y_2, y_3, 0, y_5) \\ v_3 & = & z & = & (z_1, z_2, z_3, z_4, 0) \end{array}$$

Recall $x + y + z = 0$ and $Q_1(x) = Q_2(y) = Q_3(z) = 0$. The equation $2Q_1(x) + 2Q_2(y) - Q_3(z) = 0$ shows $(x_1 - y_1)^2 = -(x_2 - y_2)^2$. As -1 is a non-square we must have $x_1 = y_1, x_2 = y_2$. Relation $Q_1(x) - Q_2(y) = 0$ yields

$$z_3^2 + z_4^2 = 2x_5^2.$$

This is impossible provided $2(z_3^2 + z_4^2)$ is a non-square. Let U consist of all $P = (z_1 : z_2 : z_3 : z_4 : 0)$ such that $2(z_3^2 + z_4^2)$ is non-square and $Q_3(P) = z_1^2 + z_2^2 + 2z_3^2 - 2z_4^2 = 0$. We have to show $|U| = O(0.5q^2)$ (as a function of q, where $q \equiv 3(\mathrm{mod}\ 4)$). We can impose the conditions $z_3z_4 \neq 0$ and $z_3^2 - z_4^2 \neq 0$ without changing the asymptotics. For each of the $(q-1)/2$ non-squares u there are $O(q)$ pairs (z_3, z_4) such that $z_3^2 + z_4^2 = 2u$ (recall that $x^2 + y^2$ is anisotropic). For each such choice of u, z_3, z_4 there are $O(q)$ pairs (z_1, z_2) such that $z_1^2 + z_2^2 = 2z_4^2 - 2z_3^2$. The number of (projective) points in U is therefore $O(0.5q^2)$. This proves Theorem 3 when $q \equiv 3(\mathrm{mod}\ 4)$. In case $q \equiv 1(\mathrm{mod}\ 4)$ the construction is similar. Precise values and an extension construction can be found in [5].

4 Recursive constructions

We start from a slight generalization of Mukhopadhyay's general product construction from [32].

Theorem 4. *If there is an n-cap $\mathcal{A} \subset AG(k,q)$ and an m-cap $\mathcal{B} \subset PG(l,q)$, then we can construct an nm-cap in $PG(k+l,q)$. Moreover, if $\mathcal{A}$ is avoided by $i \geq 1$ hyperplanes in general position and $\mathcal{B}$ is avoided by $j \geq 0$ hyperplanes in general position, then the product cap is avoided by $i+j-1$ hyperplanes in general position.*

Proof. Let $(a|1)$ be the typical representative of the affine cap, and b the typical representative of the cap in $PG(l,q)$. Here $a \in \mathbb{F}_q^k, b \in \mathbb{F}_q^{l+1}$. The typical representative of a point of the product cap is $(a|b)$. Assume $\sum_{i=1}^3 \lambda_i(a_i|b_i) = 0$. The second coordinate section shows $b_1 = b_2 = b_3$ and $\lambda_1 + \lambda_2 + \lambda_3 = 0$. This shows $\sum_{i=1}^3 \lambda_i(a_i|1) = 0$, contradiction.

An affine cap is a cap, which is avoided by a hyperplane. We can represent the cap by a matrix with a row all of whose entries are nonzero. If $\mathcal{A}$ is avoided by i hyperplanes in general position, we can represent it by a matrix which possesses i rows all of whose entries are nonzero, likewise for $\mathcal{B}$. This shows the second assertion. ∎

Two points on the projective line form a 2-cap. This leads to the most elementary application of Theorem 4: if there is an n-cap in $PG(l, q)$, there is a $2n$-cap in $AG(l+1, q)$. Also, the ovals or hyperovals in $PG(2, q)$ clearly are affine. They are in fact avoided by $i = 3$ lines (=hyperplanes) in general position. Application of the product construction yields among others $(q+1)(q^2+1)$-caps in $AG(5, q)$ when q is odd and $(q+2)(q^2+1)$-caps in $AG(5, q)$ in characteristic 2.

The following generalization of the product construction is from [18]:

Theorem 5. *Assume there is an n-cap $\mathcal{A} \subset AG(k, q)$ intersecting a hyperplane in $n - w$ points, and an m-cap $\mathcal{B} \subset PG(l, q)$. We can construct an $\{wm + (n - w)\}$-cap in $PG(k + l, q)$.*

Proof. With notation as in Theorem 4 the $(a|b)$ where $(a|1)$ varies over the affine points of $\mathcal{A}$, form the product cap, a wm-cap. The $(\alpha|\mathbf{0})$, where $(\alpha|0)$ varies over the points of $\mathcal{A}$ from the hyperplane, extend it to a $\{wm+(n-w)\}$-cap. ∎

If in Theorem 5 we choose $\mathcal{A}$ to be an ovoid (a (q^2+1)-cap in $PG(3, q)$ intersecting a hyperplane in 1 point), then a classical construction by Segre [38] is obtained: if there is an n-cap in $PG(k, q)$, then there is an $\{q^2n+1\}$-cap in $PG(k + 3, q)$.

Theorem 6. *Assume there is an n-cap $\mathcal{A} \subset AG(k, q)$ possessing a tangent hyperplane, and an m-cap $\mathcal{B} \subset PG(l, q)$ possessing a tangent hyperplane. We can construct an $\{nm - 1\}$-cap in $PG(k + l, q)$.*

Proof. A **tangent hyperplane** is a hyperplane containing precisely one point of the cap. With notation as before let $(a|1)$ and $(b|1)$ be the affine points of $\mathcal{A}$ and $\mathcal{B}$, respectively. Denote by $(\alpha|0)$ the point of $\mathcal{A}$ on the tangent hyperplane, $(\beta|0)$ the point of $\mathcal{B}$ on the tangent hyperplane. The points of the cap in $PG(k + l, q)$ are those of the form

$$(a|b|1),\ (a|\beta|0) \text{ and } (\alpha|b|0).$$

■

Application to ovoids yields a $\{q^4+2q^2\}$-cap in $PG(6,q)$. The construction in Theorem 6 shows that this cap has a hyperplane intersection of size q^2+1. An application of Theorem 5 with an ovoid as second ingredient yields a $q^2(q^2+1)^2$-cap in $PG(9,q)$.

Another construction from [18] based on elliptic quadrics in $PG(3,q)$ produces $\{(q+1)(q^2+3)\}$-caps in $PG(5,q)$. This is interesting only in odd characteristic as in characteristic 2 we have $\{(q+2)(q^2+1)\}$-caps in $PG(5,q)$ from the product construction.

Another rather specialized construction from [20] improves upon the doubling construction in certain cases. An application to the elliptic quadric in $PG(3,5)$ produces a 66-cap in $PG(4,5)$. This cap can in turn be used as an ingredient in Theorem 6 to obtain a 1715-cap in $PG(7,5)$ and a 4355-cap in $PG(8,5)$.

5 The Hill cap

Consider the elliptic quadric $Q_5^-(q)$ in $PG(5,q)$ where q is odd. We have

$$e(6,q)=h(2,0)+(q-1)(q+1)h(2,c)=(q^3+q^2-q+(q^2-1)(q^3-q)=q^5+q^3-q^2$$

(for $c\neq 0$), hence

$$|Q_5^-(q)|=(e(6,q)-1)/(q-1)=(q+1)(q^3+1).$$

In the ternary case we obtain $|Q_5^-(3)|=112$. This is not a surprise as the corresponding quadratic form can be represented by $Q(x)=\sum_{i=1}^{6}x_i$ (the Gram matrix has determinant 1). It follows that the 1-dimensional subspace $\langle x\rangle$ generated by vector $x=(x_1,x_2,\dots,x_6)$ belongs to $Var(Q)=Q_5^-(3)$ if and only if x has weight 3 or 6. As there are $8\binom{6}{3}=160$ vectors of weight 3 and $2^6=64$ vectors of weight 6 in $V(6,3)$, we obtain $|Q_5^-(3)|=80+32=112$, as predicted.

We wish to partition $Q_5^-(3)$ into caps. How do 2-dimensional totally isotropic subspaces of Q (lines of $PG(5,3)$ all of whose points belong to $Q_5^-(3)$) look like? It is clear that each such subspace contains at least two points P_1,P_2 generated by vectors of weight 3. Let P_1,P_2 be such points. The line l defined by P_1,P_2 will be totally isotropic (contain only points of weight

3 or 6) if the supports of P_1 and P_2 either are complementary or intersect in cardinality. Typical examples are the lines

$$(1:1:1:0:0:0),(0:0:0:1:1:1),(1:1:1:1:1:1),(1:1:1:2:2:2)$$

for the first case and

$$(1:1:1:0:0:0),(1:2:0:1:0:0),(2:0:1:1:0:0),(0:2:1:2:0:0)$$

for the second. This indicates how $Q_5^-(3)$ can be partitioned into two caps. It suffices to choose the partition such that each totally isotropic line has 2 points in each part. This can be done as follows:

consider the action of the group $PSL(2,5) \cong A_5$ on the projective line whose points we identify with coordinates of $V(6,3) = \mathbb{F}_3^6$. As the permutation action of $PSL(2,5)$ is 2-transitive, each orbit defines a 2-design. Let $\mathcal{D}$ be the design corresponding to the orbit containing $\{1,2,3\}$. Obvious counting shows $|\mathcal{D}| = 10$, and $\mathcal{D}$ is a design $2-(6,3,2)$. The complement of a block is not a block. Let $\overline{\mathcal{D}}$ consist of the complements of the blocks of $\mathcal{D}$, equivalently: the blocks of $\overline{\mathcal{D}}$ consist of the 3-subsets of $\{1,2,3,4,5,6\}$, which are not blocks of $\mathcal{D}$. Denote by D the set of vectors of weight 3 whose support is a block of $\mathcal{D}$, analogously for $\overline{D}$. Let $\langle D\rangle$ and $\langle\overline{D}\rangle$ be the corresponding points in $PG(5,3)$.

Let R be the union of vectors of weight 6 whose representatived have an even number of entries 2, and $\overline{R}$ the remaining weight 6 vectors. As before $\langle R\rangle, \langle\overline{R}\rangle$ denote the sets of corresponding points in $PG(5,3)$. We have partitioned the points of $Q_5^-(3)$ in the form

$$Q_5^-(3) = \langle D\rangle \cup \langle\overline{D}\rangle \cup \langle R\rangle \cup \langle\overline{R}\rangle$$

where each of $\langle D\rangle, \langle\overline{D}\rangle$ has 40 points, each of $\langle R\rangle, \langle\overline{R}\rangle$ has 16 points. The description of totally isotropic lines shows that each of

$$\langle D\rangle \cup \langle R\rangle, \langle D\rangle \cup \langle\overline{R}\rangle, \langle\overline{D}\rangle \cup \langle R\rangle, \langle\overline{D}\rangle \cup \langle\overline{R}\rangle$$

is a cap (observe that each set of elements contains precisely 2 blocks of $\mathcal{D}$ and 2 blcoks of $\overline{\mathcal{D}}$).

Theorem 7. *The 112 points of $Q_5^-(3)$ can be partitioned into two 56-caps. In particular there is a 56-cap in $PG(5,3)$.*

The 56-cap in $PG(5,3)$ is essentially uniquely determined. It is known as the Hill cap, see [25]. The existence of the Hill cap is the main reason why the ternary case displays a particular behaviour in most asymptotic questions concerning caps.

Consider the hyperplane S defined by $\sum_{i=1}^{6} x_i = 0$. The only point from $\langle R\rangle$ on S is $(1:1:1:1:1:1)$, and for each block of $\mathcal{D}$ there is precisely one point on S having the block as its support. It follows that $\langle D\rangle \cup \langle R\rangle$ intersects the hyperplane S in 11 points. The corresponding 45-cap in $AG(5,3)$ will be called the affine Hill cap. The affine 45-caps contained in a fixed copy of the Hill cap form an orbit under the automorphism group of the Hill cap. We will see in Section 10 that the affine Hill cap is the only 45-cap in $AG(5,3)$.

The doubling of the Hill cap, a 112-cap in $AG(6,3)$, can be represented as the points represented by all vectors of the form $(1,D)$ and $(1,R)$. Doubling again yields a 224-cap in $AG(7,3)$. We can do better by using the set U of vectors of weight 1 in $\mathbb{F}_3^6$. The following represent the points of a 236-cap in $AG(7,3)$:

$$(1,0,D)\ (1,0,R)\ (1,1,\overline{D}\ (1,1,R)\ (1,2,U)$$

This is the Calderbank-Fishburn cap from [9]. It was observed in [20] that the union of the Calderbank-Fishburn cap and the points of type $(0,1,U)$ form a 248-cap in $PG(7,3)$.

6 An asymptotic problem

We formulate a rather general version of the problem, valid for general linear codes.

Definition 2. *Fix q and t. Denote by $n_{t,q}(k)$ the maximal length n of a code $[n,n-k,t+1]_q$, equivalently the largest length of a linear orthogonal array of dimension k and strength t. Define*

$$\lambda(t,q) = lim\ sup_{k\to\infty}\frac{log_q(n_{t,q}(k))}{k}$$

The problem is to determine $\lambda(t,q)$. The sphere packing bound from coding theory and primitive cyclic codes yield the general bounds

$$\frac{1}{t-1} \leq \lambda(t,q) \leq \frac{1}{\lfloor t/2\rfloor}.$$

In the binary case the construction from primitive cyclic codes does in fact yield $\lambda(t,2)=1/\lfloor t/2\rfloor$, so once again assume $q>2$. Clearly $\lambda(t,q)$ is a non-increasing function of t, and $\lambda(2,q)=1$. The case of caps corresponds to $\lambda(3,q)$. It is an important open problem to bound $\lambda(3,q)$ away from 1.

Problem 4. *Prove for some or all $q>2$ that $\lambda(3,q)<1$.*

If $\lambda(3,q)=1$, then in an asymptotic sense the largest cap in $PG(k,q)$ would be as large as the space itself, for large k. This is not expected to be true, but it cannot be excluded either.

It is clear that the same asymptotic value is obtained if we base ourselves on caps in $AG(k,q)$ instead of caps in $PG(k,q)$. Let now an n-cap in $AG(k,q)$ be given. The product construction Theorem 4 shows that there exist an n^l-cap in $AG(kl,q)$. This shows $\lambda(3,q)\geq log_q(n)/k$. We conclude that every affine cap yields a lower bound on the asymptotic value $\lambda(3,q)$. The affine ovoids (q^2-caps in $AG(3,q)$) yield $\lambda(3,q)\geq 2/3$.

We saw in Section 4 that an application of Theorem 6 to ovoids yields a $\{q^4+2q^2\}$-cap in $PG(6,q)$ with a hyperplane intersection of size q^2+1. This yields a $\{q^4+q^2-1\}$-cap in $AG(6,q)$, for every q. The resulting bound

$$\lambda(3,q)\geq\frac{log_q(q^4+q^2-1)}{6}$$

seems to be the best lower bound known for general q.

Cases $q=3$ and $q=4$ are special. We start from a cap in $PG(5,4)$ due to David Glynn [22]. The description follows [20]. Consider the trace and norm $T,N:\mathbb{F}_{q^2}\rightarrow\mathbb{F}_q$ and the mapping $\gamma:(\mathbb{F}_{q^2})^3\rightarrow\mathbb{F}_q^6$ defined by

$$\gamma(a,b,c)=(N(a),N(b),N(c),T(ab^q),T(ac^q),T(bc^q)).$$

Then γ induces a mapping : $PG(2,q^2)\rightarrow PG(5,q)$. Let B be the standard Baer subplane of $PG(2,q^2)$ (whose points are $(a:b:c)$ such that $a,b,c\in\mathbb{F}_q$). The Frobenius homomorphism ϕ fixes the points of B, and has orbits of length 2 (conjugate points) on exterior points (points $\notin B$). Let $\Gamma_q\subset PG(5,q)$ be the image of γ when restricted to exterior points. We have $\gamma(P)=\gamma(Q)$ for exterior points P,Q if and only if $Q=P$ or $Q=P^q$. This shows $|\Gamma_q|=(q^4-q)/2$. The set Γ_4 is a cap, a 126-cap in $PG(5,4)$. The intersection with hyperplane $x_1=0$ consists of all points $\gamma(0:b:1)$, where $\notin\mathbb{F}_4$. It follows that this hyperplane intersection has $(16-4)/2=6$ points. The resulting 120-cap in $AG(5,4)$ yields the lower bound $\lambda(3,4)\geq log_4(120)/5=0.6906\ldots$

The doubled Hill cap (a 112-cap in $AG(6,3)$) yields $\lambda(3,3) \geq 0.7158\ldots$ Improvements upon this lower bound will be discussed in the following section.

7 A generalized product construction

The results in this section are from [17]. Starting point is the idea to modify the product construction Theorem 4 such that the resulting cap can be extended even when the ingredients of the product construction are complete caps. Here is the variant of the product construction, which will allow extensions:

Theorem 8. *Let $A_1, \ldots, A_c$ be subsets of $\mathbb{F}_q^n$ such that $(1 : A_i)$ is a cap in $AG(n,q)$ for all i, and $B \subset \mathbb{F}_q^{m+1}$ a set of representatives for a cap $\langle B \rangle \subset PG(m,q)$, partitioned as $B = B_1 \cup \cdots \cup B_c$. Then $\bigcup_{i=1}^{c}(A_i : B_i)$ is a cap in $PG(n+m,q)$.*

The proof is identical to the proof of Theorem 4.

When will $(u : v)$ be an extension point? Case $v = 0$ is not very fruitful as $(u : 0)$ is an extension point of the generalized product cap if and only if $(0 : u)$ is an extension of the affine cap $(1 : A_i)$ for all i. Assume $v \neq 0$ and $u \neq 0$. Then $(u : v)$ is not an extension point if and only if there are scalars λ, λ' such that

$$(u,v) = \lambda(a,b) + \lambda'(a',b'),$$

where $a \in A_i, b \in B_i, a' \in A_j, b' \in B_j$. The following strategy will make sure that this cannot happen. At first choose u and the A_i such that $\langle u \rangle \notin \langle A_i \rangle$ for all i (observe that this happens in $PG(n-1,q)$) and such that for $i \neq j$ and $\langle a \rangle \neq \langle a' \rangle$ the points $\langle u \rangle, \langle a \rangle, \langle a' \rangle$ are not collinear. If this is satisfied we must have $i = j$ in the relation above. In practice we will choose $c = 2$ and A_1, A_2 as isomorphic copies of a large cap. These have to be chosen such that there exist many candidates u satisfying the above conditions.

Finally v has to chosen such that $\langle v \rangle \notin \langle B \rangle$ and $\langle B_i \rangle \cup \{\langle v \rangle\}$ is a cap, for each i.

If these conditions are satisfied, $(u : v)$ is an extension point of the generalized product cap. An advantage of this method is that the conditions on the two coordinate sections are independent of one another. In order to obtain large extensions one needs sets U, V such that not only $(u : v)$ is an extension point for each $u \in U, v \in V$ but $(U : V)$ extends the generalized product cap. The additional conditions guaranteeing this are rather obvious. One fertile source is the Hill cap. We can use $A_1 = D \cup R$ and $A_2 = \overline{D} \cup R$ as two versions of the doubled Hill cap in $AG(6, 3)$, and U the set of weight 1 vectors. Here we use the terminology of Section 5.

A ternary construction for the second coordinate section occurs in dimension $m = 3$, where the ovoid can be partitioned into two parts, and there exists an 8-cap V each of whose points is an extension point of each of the parts of the ovoid. In this situation the generalized product cap (1120 points in $PG(9, 3)$) can be extended by the $12 \cdot 8$ points from $(U : V)$, yielding a 1216-cap in $PG(9, 3)$.

Another low-dimensional ternary application of this construction occurs when $m = 5$. We can partition representatives of the Hill cap as $B_1 = R, B_2 = D$. Then $V = \overline{R}$ satisfies the conditions for the second coordinate section. This yields a cap of $112 \cdot 56 + 12 \cdot 16 = 6464$ points in $PG(11, 3)$.

The main result of [17] is the construction of ternary affine caps, which yield improved lower bounds on $\lambda(3, 3)$ (see Section 6). They generalize and strengthen earlier results by Calderbank-Fishburn. The best lower bound from [9] is $\lambda(3, 3) \geq 0.7218\ldots$ A cap in $AG(62, 3)$ constructed in [17] yields $\lambda(3, 3) \geq 0.723779\ldots$ The best bound from [17] is $\lambda(3, 3) \geq 0.724851\ldots$ It is based on a cap in $AG(480, 3)$.

8 General upper bounds

We start from a general upper bound on affine caps. In this section denote by $C_k(q)$ the maximum size of a cap in $AG(k, q)$, and by $c_k(q) = C_k(q)/q^k$ its relative size. As $AG(k, q)$ is the disjoint union of q copies of $AG(k-1, q)$, it follows that $C_k(q) \leq qC_{k-1}(q)$, hence $c_k(q) \leq c_{k-1}(q)$. Obserce $c_3(q) = 1/q$. We will derive a lower bound on $c_{k-1}(q) - c_k(q)$. This shows in particular that a maximal cap in $AG(k, q)$ cannot intersect each hyperplane in a maximal cap.

As usual assume $q = p^f > 2$. Let $A \subset AG(k, q)$ a cap. As $q > 2$ we can find nonzero elements $\lambda_i \in \mathbb{F}_q$ such that $\lambda_1 + \lambda_2 + \lambda_3 = 0$. The λ_i are fixed throughout the proof. Let $V = \mathbb{F}_q^k = AG(k, q)$ and $T : \mathbb{F}_q \longrightarrow \mathbb{F}_p$ the trace function. Put $Q = |V| = q^k$. Finally, $\zeta = exp(2\pi i/p)$. We aim at an upper bound on $|A|$. Consider the complex number

$$S = \sum_{y \in V \setminus \{0\}} \sum_{a_1, a_2, a_3 \in A} \zeta^{T((\sum_i \lambda_i a_i) \cdot y)}.$$

This number is easily determined: reverse the order of summation and extend the inner sum over all $y \in V$ (the additional term corresponding to $y = 0$ is easy to compute). As the sum over all powers of ζ vanishes, the inner sum will vanish unless $a_1 = a_2 = a_3$. We obtain

$$S = |A|(Q - |A|^2).$$

Now we obtain an upper bound on $|S|$. Let $0 \neq \lambda \in \mathbb{F}_q$ and $0 \neq y \in V$. Consider the complex number $U(\lambda)_y = \sum_{a \in A} \zeta^{T((\lambda a) \cdot y)}$. Let $u(\lambda)_y = |U(\lambda)_y|$. We define a real vector $u(\lambda)$ of length $Q - 1$ whose coordinates are parametrized by the $0 \neq y \in V$, the corresponding entry being $u(\lambda)_y$. We have $S = \sum_{y \neq 0} U(\lambda_1)_y U(\lambda_2)_y U(\lambda_3)_y$, in particular

$$|S| \leq \sum_{y \neq 0} u(\lambda_1)_y u(\lambda_2)_y u(\lambda_3)_y.$$

What do we know about the real vectors $u(\lambda)$? A calculation similar to the determination of S shows that we know the length of these vectors:

$$\|u(\lambda)\|^2 = |A|(Q - |A|)$$

The combinatorial information is in the following lemma, an upper bound on the entries $u(\lambda)_y$:

Lemma 1. *Let $0 \neq \lambda \in \mathbb{F}_q$ and $0 \neq y \in V$. Then*

$$u(\lambda)_y \leq qC_{k-1}(q) - |A| = c_{k-1}(q)Q - |A|.$$

Proof. As λA is a cap we can assume $\lambda = 1$. Denote by ν_c the number of elements $a \in A$ such that $a \cdot y = c$. As the $v \in V$ satisfying $v \cdot y = c$ form a subspace $AG(k-1, q)$, we have $\nu_c \leq C_{k-1}(q)$. It follows

$$u(\lambda)_y = |\sum_{c \in \boldsymbol{F}_q} \nu_c \zeta^{T(c)}| = |\sum_{c \in \boldsymbol{F}_q} (C_{k-1}(q) - \nu_c) \zeta^{T(c)}|$$

$$\leq \sum_c (C_{k-1}(q) - \nu_c) = qC_{k-1}(q) - |A|.$$

■

Now we can obtain an upper bound on $|S|$, using the bound from the preceding lemma and Cauchy-Schwartz:

$$|S| \leq (c_{k-1}(q)Q - |A|)(|A|(Q - |A|)).$$

Comparison of this upper bound and the precise value of $|S|$ yields the following bound on $C_k(q)$, which is the main result in this section.

Theorem 9. *Let $q > 2$ be a prime-power. If $k \geq 3$, then*

$$c_k(q) \leq \frac{q^{-k} + c_{k-1}(q)}{1 + c_{k-1}(q)},$$

equivalently

$$(1 - c_k(q))(c_{k-1}(q) - c_k(q)) \geq c_k^2 - q^{-k}.$$

In particular we have the desired lower bound on the decrease $c_{k-1}(q) - c_k(q)$. Theorem 9 was first obtained by Meshulam [31] in odd characteristic, using the mechanism of the Fourier transform. The direct approach sketched in this section is from [6]. It covers also the characteristic 2 case.

A slight generalization of Theorem 9 is now obvious:

Theorem 10. *Let $q > 2$ be a prime-power, $k \geq 3$ and $A \subset AG(k, q)$ a cap such that $|A| \geq \sqrt{q^k}$ and A intersects each hyperplane in $\leq C$ points. Let $c = C/q^{k-1}$. Then*

$$\frac{|A|}{q^k} \leq \frac{q^{-k} + c}{1 + c}.$$

An asymptotic bound that can be derived from Theorem 9 is

Theorem 11. *Let $q > 2$ and $k \geq 3$. Then*

$$c_k(q) \leq \frac{k+1}{k^2}.$$

While Theorem 11 is the best known asymptotic bound it falls short from solving Problem 4. Instead of of a bound of the form $c_k(q) \leq 1/k$ we would need $c_k(q) \leq q^{-k\delta}$ for a constant $\delta > 0$ for that purpose.

The bounds on $C_k(q) = m_2(AG(k,q))$ for concrete small values k, q derivable from Theorem 9 or Theorem 10 seem to be good only in the ternary case. Yves Edel observes that we can derive good asymptotic bounds on $m_2(k,q) = m_2(PG(k,q))$ as well. In fact, the doubling construction from Section 4 yields $2m_2(k,q) \leq C_{k+1}(q)$. By Theorem 11 we have $C_{k+1}(q) \leq q^{k+1}\frac{k+2}{(k+1)^2}$.

Theorem 12. *Let $q > 2$ and $k \geq 3$. Then*

$$m_2(k,q) \leq q^{k+1}\frac{k+2}{2(k+1)^2}.$$

For $q > 3$ we can improve upon Theorem 12. Use the obvious relation $m_2(k,q) \leq C_k(q) + m_2(k-1,q)$ and Theorems 11, 12. This yields $m_2(k,q) \leq \frac{3(k+1)}{2k^2}q^k$. We can use this as bound on the second term in the recursion and obtain the following:

Theorem 13. *For $q > 3$ and $k \geq 3$ we have*

$$m_2(k,q) \leq (\frac{k+1}{k^2} + \frac{3k}{2q(k-1)^2})q^k.$$

9 Large groups of automorphisms

There seems to be a tendency that exceptional objects admit a large group of symmetries. In our context this is clearly visible. The quadrics have orthogonal groups as groups of automorphisms, and the Tits ovoids admit the Suzuki groups. As there are no canonical models for large caps in projective dimensions larger than 3 it cannot be expected that the automorphism group are just as rich as in dimension 3. Still there are many examples of large groups of symmetries.

The construction of the Hill cap given in Section 5 shows the presence of a semidirect product $E_{16} \cdot A_5$ in the automorphism group. The full group of automorphisms (the stabilizer in $PGL(6,3)$) is much larger. It has order 8! and contains the simple group $PSL(3,4)$ as a subgroup of index 2.

Glynn's 126-cap in $PG(5,4)$ (see Section 6) by construction admits $PGL(3,4)$ as a group of automorphisms. The 66-cap in $PG(4,5)$ from [20] mentioned at the end of Section 4 has an automorphism group of order 480, which contains A_5.

A 40-cap in $AG(4,4)$

We construct a 40-cap in $AG(4,4)$, which has a semidirect product $E_{16} \cdot A_5$ as full group of automorphisms. The construction starts from an embedding of this group in $SL(5,4)$. Write $\mathbb{F}_4 = \{0, 1, \omega, \overline{\omega}\}$.

Let $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL(2,4)$. The mapping

$$A \mapsto \iota(A) = \left(\begin{array}{cc|cc|c} a & b & 0 & 0 & (ab)^2 \\ c & d & 0 & 0 & (cd)^2 \\ \hline 0 & 0 & a^2 & b^2 & ab \\ 0 & 0 & c^2 & d^2 & cd \\ \hline 0 & 0 & 0 & 0 & 1 \end{array}\right)$$

describes an embedding $\iota : SL(2,4) \rightarrow SL(5,4)$. Let $W(B) = \begin{pmatrix} I & B \\ 0 & I \end{pmatrix} \in SL(5,4)$, where B is a $(2,3)$-matrix. Then $W = \{W(B)\}$ is an elementary abelian group of order 4^6 and $W(B_1)W(B_2) = W(B_1 + B_2)$. We have

$$\iota(A)^{-1} W(\begin{pmatrix} u & v & x \\ w & x & u \end{pmatrix}) \iota(A) = W(\begin{pmatrix} U & V & X \\ W & X & U \end{pmatrix})$$

where

$$X = ad^2x + b^2cu + cd^2v + ab^2w, \ U = bc^2x + a^2du + c^2dv + a^2bw,$$

$$V = bd^2x + b^2du + d^3v + b^3w, \ W = ac^2x + a^2cu + c^3v + a^3w$$

This describes the action of $\iota(SL(2,4)) \subset SL(5,4)$ on the elementary abelian group W.

Lemma 2. *Consider the standard action of $SL(2,4)$ on a 2-dimensional $I\!F_4$-vector space S with basis v_1, v_2 :*

$$Av_1 = av_1 + cv_2,\ Av_2 = bv_1 + dv_2$$

and let $\phi(A)$ be the image of A under the Frobenius (squaring each entry). The tensor product $S \otimes S$ is a 4-dimensional $I\!F_4$-vector space with basis $v_1 \otimes v_1, v_2 \otimes v_2, v_1 \otimes v_2, v_2 \otimes v_1$. Let $SL(2,4)$ acts on $S \otimes S$ such that A acts on the first component and $\phi(A)$ acts on the second component ($v \otimes w \mapsto (Av) \otimes (\phi(A)w)$).

This action of $SL(2,4)$ is similar to the permutation action of $\iota(SL(2,4))$ on the $W(\begin{pmatrix} u & v & x \\ w & x & u \end{pmatrix}$. The $SL(2,4)$-equivariant isomorphism is given by

$$w(v_1 \otimes v_1) + v(v_2 \otimes v_2) + x(v_1 \otimes v_2) + u(v_2 \otimes v_1) \mapsto W(\begin{pmatrix} u & v & x \\ w & x & u \end{pmatrix}$$

Because of Lemma 2 each additive subgroup of $S \otimes S$, which is invariant under the action of $SL(2,4)$, describes a semidirect product embedded in $SL(5,4)$.

Lemma 3. *Let $\mathcal{V}$ be the $I\!F_2$-submodule (additive subgroup) of order 16 generated by $\overline{\omega}(v_1 \otimes v_1), \overline{\omega}(v_2 \otimes v_2)$ and the $\overline{\omega}\delta(v_1 \otimes v_2) + \overline{\omega}\delta^2(v_2 \otimes v_1)$. Then $\mathcal{V}$ is an $SL(2,4)$-module under the action of $SL(2,4)$ from Lemma 2.*

Corollary 1. *The group $\iota(SL(2,4))$ acts by conjugation on the elementary abelian subgroup $\mathcal{V}$ consisting of $W(\begin{pmatrix} u & v & x \\ w & x & u \end{pmatrix})$ where $v, w \in \{0, \overline{\omega}\}$ and $(x,u) = \overline{\omega}(\delta, \delta^2)$ for some $\delta \in I\!F_4$. Let G be the semidirect product $\mathcal{V} \cdot SL(2,4) \subset SL(5,4)$.*

Definition 3. *Let C be the orbit of $P = (0:0:0:0:1)^T$ under G.*

Lemma 4. *We have $|C| = 40$, and C consists of the points $Q = (\overline{\omega}a\delta + \overline{\omega}b\delta^2 + (ab)^2 : \overline{\omega}c\delta + \overline{\omega}d\delta^2 + (cd)^2 : ab : cd : 1)$, where $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL(2,4)$ and $\delta \in \mathbb{F}_4$.*

Proof. Application of $W(B)$ to P yields $(\overline{\omega}\delta : \overline{\omega}\delta^2 : 0 : 0 : 1)^T$. Its image under $\iota(A)$ is

$$Q = (\overline{\omega}a\delta + \overline{\omega}b\delta^2 + (ab)^2 : \overline{\omega}c\delta + \overline{\omega}d\delta^2 + (cd)^2 : ab : cd : 1).$$

Assume $Q = P$. Then $ab = cd = 0$, which means that A is in a subgroup $SL(2,2)$. The first coordinates show $\delta(a + b\delta) = \delta(c + d\delta) = 0$. If $\delta \neq 0$ we obtain the contradiction $det(A) = 0$. It follows that the stabilizer of P in G consists of those elements $\iota(A)W(B)$, where $\delta = 0$ and $ab = cd = 0$. This group has order $4 \cdot 6$. The length of the orbit of P under G is therefore 40. ■

It is easy to see that C is a cap. We can describe C in terms of ovoids in hyperplanes. Consider the hyperplanes

$$H_1 = (x_3 = 0),\ H_2 = (x_4 = 0),\ H_3 = (x_3 + x_4 + x_5 = 0),$$

$$H_4 = (\omega x_3 + \overline{\omega}x_4 + x_5 = 0),\ H_5 = (\overline{\omega}x_3 + \omega x_4 + x_5 = 0).$$

Then $\mathcal{H} = \{H_1, H_2, H_3, H_4, H_5\}$ form an orbit under G. Here $\mathcal{V}$ is the kernel of the permutation representation and $\iota(SL(2,4))$ acts as A_5. The intersection $C \cap H_1$ is an affine ovoid:

$$C \cap H_1 = (x_3 = 0) \cap (x_5 = 1) \cap Var(2X_1^2 + X_4^2 + X_2X_5 + X_1X_4).$$

The action of G shows that $C \cap H_i$ is an affine ovoid for all $i = 1, \ldots, 5$. In fact $C = \cup_{i=1}^5 (C \cap H_i)$, and each point of C is in precisely two of the hyperplanes H_i. Further $H_i \cap H_j \cap C$ has precisely 4 points whenever $i \neq j$, and C is the disjoint union of $H \cap H' \cap C$, where $\{H, H'\}$ varies over the pairs of hyperplanes from $\mathcal{H}$.

10 Exact values

It has been noted before that the precise values of $m_2(k,q)$ and of $m_2(AG(k,q))$ $(q>2)$ are known for projective dimension $k\leq 3$. Only a small number of these values are known for $k>3$ (and $q>2$). Pellegrino [35] determined all 20-caps in $PG(4,3)$ and established $m_2(4,3)=m_2(AG(4,3))=20$. It is then easy to prove that the Hill cap is optimal in $PG(5,3): m_2(5,3)=56$. In fact the Hill cap is the only 56-cap in $PG(5,3)$ [25]. It is a recent result from [21] that $m_2(AG(5,3))=45$ and the affine 45-cap is uniquely determined: it is contained in the Hill cap. There is hope to go one further step in the ternary case. Doubling the Hill cap yields an 112-cap in $AG(6,3)$, and Theorem 9 yields $m_2(AG(6,3))\leq 114$. It should be possible to decide the question of the existence of a 113-cap in $AG(6,3)$.

In the quaternary case it is known that $m_2(4,4)=41$ [19] and $m_2(AG(4,4))=40$. In the preceding section we constructed a very symmetric 40-cap in $AG(4,4)$. The proof of optimality will be given in a forthcoming joint paper with Y.Edel.

To the best of the author's knowledge no more precise values $m_2(k,q)$ or $m_2(AG(k,q))$ are known.

Unicity of the affine Hill cap

It has been proved in [21] that the affine Hill cap is the only 45-cap in $AG(5,3)$. In this subsection we sketch a somewhat different proof. Let $A\subset AG(5,3)$ be a cap of $m_2(AG(5,3))$ points. The Hill cap shows $m_2(AG(5,3))\geq 45$. By a computer result of Y.Edel A cannot have a hyperplane intersection of more than 18 points. At this point Theorem 10 shows $|A|\leq 45$. We have $m_2(AG(5,3))=45$. As we have equality, the method of Section 8 yields more: the code $\mathcal{C}$ generated by A (a $[45,6,27]_3$-code) has weight distribution

$$A_{27}=220\ A_{30}=396\ A_{36}=110\ A_{45}=2$$

We work in $PG(5,3)$. The points of A avoid precisely one hyperplane H_0. The strategy is the following: show that there are 11 points in H_0 which extend A to a 56-cap in $PG(5,3)$. Because of the unicity of the Hill cap as a 56-cap in $PG(5,3)$ we are done once this is shown.

Let $E\subset H_0$ be a plane. The **intersection square** determined by E consists of the numbers $|S\cap A|$, where S varies over the 9 solids $(PG(3,3))$

$\not\subset H_0$, which contain E. These numbers add up to 45. Also, as the 12 hyperplanes $\neq H_0$ containing E come in four parallel classes of 3 each, the numbers $|S \cap A|$ are naturally represented in a $(3,3)$-square, where each row, column, parallel to the main diagonal and parallel to the antidiagonal corresponds to a hyperplane. Observe also that the intersection of any two non-parallel hyperplanes $\neq H_0$ meets H_0 in a plane. Two such hyperplanes therefore determine an intersection square. The intersection square has **type** T_i if E is contained in i parallel classes of 15-hyperplanes. Clearly $0 \leq i \leq 4$. There are 1210 planes in H_0, and therefore there are 1210 intersection squares.

Observe that each parallel class of hyperplanes meets A either in $9, 18, 18$ points or in $15, 15, 15$ points.

Let $S \not\subset H_0$ be a solid intersecting the cap in s points and consider an intersection square of type i containing S. As the affine part of the ovoid is the largest cap in $AG(3,3)$ we have $s \leq 9$. There are 4 hyperplanes containing the solid, i of which are 15-hyperplanes. As $9, 15, 18$ are the only hyperplane intersections and $15 \equiv 6(\bmod 9)$ whereas the other two numbers are divisible by 9, we obtain

$$s + i(6 - s) + (4 - i)(-s) = 3(2i - s) \equiv 0(\bmod 9)$$

equivalently $s \equiv 2i(\bmod 3)$. The same counting argument shows that $s = 0$ and $s = 9$ do not occur in type T_3 and $s = 2, s = 8$ are impossible in type T_4.

We have shown the following:

Lemma 5. *The possibilities for entries s in intersection squares of type T_i are the following:*

i	s
0	$0, 3, 6, 9$
1	$2, 5, 8$
2	$1, 4, 7$
3	$3, 6$
4	5

Theorem 14. *The possible intersection squares are equivalent to one of the following:*

$$T_0 = \begin{array}{|c|c|c|} \hline 9 & 0 & 9 \\ 3 & 3 & 3 \\ 6 & 6 & 6 \\ \hline \end{array} \qquad T_1 = \begin{array}{|c|c|c|} \hline 2 & 2 & 5 \\ 2 & 8 & 8 \\ 5 & 8 & 5 \\ \hline \end{array} \qquad T_2 = \begin{array}{|c|c|c|} \hline 1 & 4 & 4 \\ 4 & 7 & 7 \\ 4 & 7 & 7 \\ \hline \end{array}$$

$$T_3 = \begin{array}{|c|c|c|} \hline 3 & 3 & 3 \\ 6 & 6 & 6 \\ 6 & 6 & 6 \\ \hline \end{array} \qquad T_4 = \begin{array}{|c|c|c|} \hline 5 & 5 & 5 \\ 5 & 5 & 5 \\ 5 & 5 & 5 \\ \hline \end{array}$$

Proof. Cases T_4 and T_3 follow directly from Lemma 5. In case T_2 choose notation such that the sums in the first row and in the first column are 9. Then the entries in the southeastern $(2,2)$-matrix are 7 and the square is uniquely determined. For type T_1 let the first row and first column sum be 0 and let all the parallels to the main diagonal sum to 15. The entries in the first row are $2,2,5$, likewise for the first column. The northwestern entry cannot be 5 as this would force all the entries in the southeastern $(2,2)$-matrix to be 8. So we have entry 2 in the northwestern corner. The rest of the square is uniquely determined. Consider finally type T_0. There are two solids, which do not occur in any of the four 9-hyperplanes. These have entry 9. We choose these to be the northern corners. This gives us the top row $(9,0,9)$. The completion is unique. ∎

Let $\mathcal{C}$ be the code $[45,6,36]_3$ generated by A, that is by the $(6,45)$-matrix whose columns are the points of the A, with the all-1-vector as last row. Lemma 14 shows that $\mathcal{C}$ is self-orthogonal.

Assume there is a hyperplane $H \neq H_0$ with a parallel class of solids meeting H in $0,9,9$ points of A. In particular H is contained in an intersection square of type T_0, and such a hyperplane exists if and only if intersection squares of type T_0 exist. As $H \cap H_0$ is a $PG(3,3)$, we have that H is contained in 40 intersection squares. Denote by $a_i = a_i(H)$ the number of planes $E \subset H \cap H_0$ (equivalently: the number of intersection squares containing H) of type T_i. Clearly $a_4 = 0$, as an intersection square of type T_4 does not contain 18-hyperplanes. We have

$$a_0 + a_1 + a_2 + a_3 = 40 \text{ and } a_0 > 0.$$

Each 15-hyperplane (there are $198 = 3 \cdot 66$ such hyperplanes) generates an intersection square with H. Each such intersection square of type T_i contains $3i$ of the 15-hyperplanes. This yields $\sum_i 3ia_i = 3 \cdot 66$, or

$$a_1 + 2a_2 + 3a_3 = 66.$$

This information helps us to compute the weight distribution of the code of length 18 given by the points of $A \cap H$. We do this in geometric language. Let n_i be the number of hyperplanes of H intersecting $A \cap H$ in i points. One of these is $H \cap H_0$, with 0 points. The remaining 120 hyperplanes of H come in 40 parallel classes of 3 each. The intersection squares they belong to give information on the n_i.

The choice of H means that there is a plane $E_0 \subset H \cap H_0$ of type T_0 such that the corresponding parallel class of solids intersects H in $0, 9, 9$ points, respectively. We speak of an intersection square (or of a plane $E \subset H \cap H_0$) of **partition** (x_1, x_2, x_3) if the corresponding parallel class of solids meets $A \cap H$ in x_1, x_2 and x_3 points (clearly $x_1 + x_2 + x_3 = 18$). Plane E_0 has partition $(0, 9, 9)$. This shows $n_0 \geq 2$ (recall $H \cap H_0$) and $n_9 \geq 2$. Assume $n_9 > 2$. Such a solid would have at least 5 points in common with one of the solids given by E_0. The intersection is a plane containing ≥ 5 points of the cap A, contradiction. We conclude $n_9 = 2$. The typology shows that also $n_0 = 2$.

Each plane of type T_3 has partition $(6, 6, 6)$ and each plane of type T_2 has partition $(4, 7, 7)$. If E has type T_1, then two possibilities arise: E is of partition either $(2, 8, 8)$ or $(5, 5, 8)$. Let b_1 be the number of planes of partition $(2, 8, 8)$ and b_2 the number of planes of partition $(5, 5, 8)$. In particular $b_1 + b_2 = a_1$. Each plane $E \neq E_0$ of type T_0 must have partition $(6, 6, 6)$, because of $n_9 = 2$. We can add up and obtain the numbers n_i in terms of the a_i, b_i :

$$n_0 = 2, n_1 = 0, n_2 = b_1, n_3 = 0, n_4 = a_2,$$

$$n_5 = 2b_2, n_6 = 3(a_3 + a_0 - 1), n_7 = 2a_2, n_8 = 2b_1 + b_2, n_9 = 2.$$

Only two of the obvious equations on the n_i will be needed. As each pair of points in $A \cap H$ is on precisely 13 solids in H we have $\sum_i \binom{i}{2} n_i = \binom{18}{2} \cdot 13$. Counting triples one obtains $\sum_i \binom{i}{3} n_i = \binom{18}{3} \cdot 4$. Combining these equations with the earlier established relations leads to $a_0 = 0$, which is a contradiction.

This method of excluding T_0 was coined by Y.Edel. Now that we know T_0 does not occur counting gets easier. We can apply Edel's method to determine the weight distribution of the corresponding codes as well as the numbers a_i, which determine in how many intersection squares of a given type a given hyperplane is contained.

Lemma 6. *Let H be a 9-hyperplane. Then H is contained in 18 intersection squares of type T_1, in 18 intersection squares of type T_2 and in 4 intersection squares of type T_3.*

The following lemma part of which concerns the structure of the ternary Golay code can be proved using a computer program:

Lemma 7. *Define an (n, m)-set in $PG(k, q)$ as a set of n points such that no more than m are on a hyperplane. The following holds:*

Each $(9, 5)$-set in $AG(4, 3)$ is embeddable in an $(11, 5)$-set.

Each $(18, 8)$-set in $AG(4, 3)$ can be extended to a $(20, 8)$-set.

In both cases the extension points are uniquely determined. They are in the hyperplane at infinity.

Definition 4. *Let H be a 9-hyperplane of $PG(5, 3)$. Define the* **shadow** *$S(H)$ as the set of points $S \in H \cap H_0$ such that S together with $H \cap A$ forms an $(10, 5)$-set in H.*

Let $E \subset H_0 \cap H$ be one of the 18 planes of type T_1. As some hyperplane through E intersects $A \cap H$ in 5 points we have $E \cap S(H) = \emptyset$. On the other hand the number of planes $H_0 \cap H$ avoiding two given points is the same as the number of points not in the union of two given planes, hence is $= 40 - 2 \cdot 13 + 4 = 18$. This shows $|S(H)| \leq 2$ and in case of equality we have that the planes E of type T_1 are precisely those 18 planes in $H \cap H_0$ which are disjoint from $S(H)$. It follows from Lemma 7 that $|S(H)| = 2$ for every 9-hyperplane H.

Proposition 2. *Let H be a hyperplanes of $PG(5,3)$ intersecting A in 9 points, and let H' be a hyperplane not parallel to H. The intersection square generated by H, H' is of type T_1 if and only if the plane $H_0 \cap H \cap H'$ has trivial intersection with $S(H)$.*

Clearly one can go on counting like that. Consider one of the 18 intersection squares of type T_2 that contain H. The corresponding plane $E \subset H_0$ must intersect $S(H)$ in at most 1 point, by Proposition 2 it intersects in precisely one point. On the other hand, there are precisely 18 such subplanes in $H \cap H_0$.

Proposition 3. *Let H be a hyperplanes of $PG(5,3)$ intersecting A in 9 points, and let H' be a hyperplane not parallel to H. The intersection square generated by H, H' is of type T_2 if and only if the plane $H_0 \cap H \cap H'$ intersects $S(H)$ in precisely one point.*

Proposition 4. *Let H be a hyperplanes of $PG(5,3)$ intersecting A in 9 points, and let H' be a hyperplane not parallel to H. The intersection square generated by H, H' is of type T_3 if and only if the plane $H_0 \cap H \cap H'$ contains $S(H)$.*

Analogous counting arguments can be applied to 18-hyperplanes.

Definition 5. *Let H be a 18-hyperplane of $PG(5,3)$. Define the* **shadow** *$S(H)$ as the set of points $S \in H \cap H_0$ such that S together with $H \cap A$ forms an $(19,8)$-set in H.*

Just as in the case of 9-hyperplanes we see that $E \cap S(H) = \emptyset$ if $E \subset H \cap H_0$ has type T_1. As there are 18 such planes it follows $|S(H)| \leq 2$. Lemma 7 implies that $|S(H)| = 2$ and that plane E has type T_1 if and only if it avoids $S(H)$.

Proposition 5. *Let H be a 18-hyperplane of $PG(5,3)$. Then $|S(H)| = 2$ and these points extend $A \cap H$ to a $(20,8)$-set in $PG(4,3)$. A plane $E \subset H \cap H_0$ has type T_1 if it avoids $S(H)$, type T_2 if it meets $S(H)$ in one point and type T_3 if it contains $S(H)$.*

Consider one of the 55 parallel classes (H_1, H_2, H_3) of hyperplanes intersecting A in $9, 18, 18$ points. As the planes of given type uniquely determine the shadow, both in the case of 9-hyperplanes and in the case of 18-hyperplanes, we see that $S(H_1) = S(H_2) = S(H_3)$. The four planes of type T_3 with respect to our parallel class are precisely the planes through the line which contains $S(H_1)$. We see that $A \cup S(H_1)$ is a 47-cap.

Definition 6. *Let S be the union of the shadows $S(H)$, where H varies over the 55 hyperplanes intersecting A in 9 points. For each such H let $l(H)$ be the line in H_0 through $S(H)$.*

We want to show that $|S| = 11$ and that S is a cap. Each $Q \in S$ extends A to a 46-cap.

Lemma 8. *Each line in H_0 is contained in a 9-hyperplane.*

Proof. Assume this is not the case for some line l in H_0. By our typology this means that each plane E, where $l \subset E \subset H_0$, must have type T_4. Equivalently, every solid through l either is contained in H_0 or meets A in precisely 5 points. Consider now a plane B through l, which is not contained in H_0. Then each of the 13 solids containing B has 5 points of A. If $|B \cap K| = i$, the equation $45 = i + 13(5 - i)$ must hold, which is impossible. ∎

Let now $Q_1, Q_2 \in S$ and l the line through Q_1, Q_2. By Lemma 8 there is a 9-hyperplane $H \supset l$. It follows that $(H \cap A) \cup \{Q_1, Q_2\}$ is a cap. As these two extension points are uniquely determined it follows $\{Q_1, Q_2\} = S(H)$ and $l = l(H)$. This also shows that no three points of S are collinear and that the lines $l(H)$ are pairwise different. As there are $55 = \binom{11}{2}$ such lines we must have $|S| = 11$. We are done.

Theorem 15. *The only* 45*-cap in* $AG(5,3)$ *is the affine Hill cap.*

11 High-dimensional codes

A natural context for the duals of caps (codes with $d = 4$) are codes with high dimension and small value of d. Let us concentrate on case $d = 5$. A survey is attempted in [2]. The geometric description for a linear code $[n, n-k, 5]_q$ (the analog to the notion of a cap when $d = 4$, see Proposition 1) is the following: a set of n points in $PG(k-1, q)$ such that no 4 are in a plane, equivalently: any 4 points must be in general position. In some cases more is known on the strength 4 version of the asymptotic problem from Section 6 than in the cap case. The upper bound is $\lambda(4, q) \leq 1/2$. There is a family of cyclic codes showing $\lambda(4, 3) = 1/2$. A family of constacyclic codes shows $\lambda(4, 4) = 1/2$, see [15]. Constructions showing general bounds

$$\lambda(4, q) \geq 3/7 \text{ and } \lambda(5, q) \leq 1/3$$

are from [15] as well.

Binary linear codes of minimum distance 5 have found an interesting application in the cryptographic problem of **fingerprinting.** For an introduction see Boneh-Shaw [8] In the old times tables of logarithms were fingerprinted by introducing tiny errors in some randomly chosen values. In the era of electronic documents there is the danger that two owners of fingerprinted copies detect the location of the fingerprints (these are the locations where the documents differ) and make them unreadable. Let $x, y \in \mathbb{F}_2^n$ be the versions of the document. The owners will produce a document $\zeta(x, y) = z \in \{0, 1, \epsilon\}^n$ where $z_i = x_i = y_i$ when $x_i = y_i$ and $z_i = \epsilon$ when $x_i \neq y_i$. These pirates will then distribute the new document $\zeta(x, y)$ hoping these copies cannot be traced back to them. The system designer will choose the fingerprints in such a way that each pirate copy $\zeta(x, y)$ generated by collusion of two owners can be traced back to one of the owners. This leads to a variant of a famous combinatorial-number theoretic problem, as follows: interpret the binary digits $0, 1$ as natural numbers. Then knowledge of $\zeta(x, y) \in \{0, 1, \epsilon\}^n$ is equivalent to knowledge of the integer sum $x + y \in \mathbb{Z}^n$. We want to choose the fingerprints in $\{0, 1\}^n$ such that each pair of different fingerprints generates a different sum. Such sets of tuples are known as **Sidon sets.**

Definition 7. *Let* $A = \{0, 1\} \subset \mathbb{Z}$*. Let* S_n *be the maximum size of a subset* $S \subset A^n$ *(a Sidon set) such that* $x + y = u + v$ *for* $x, y, u, v \in S$ *implies either* $x = y, u = v$ *or* $\{x, y\} = \{u, v\}$*. Let* $\sigma = lim_{n\rightarrow\infty}\frac{log_2(S_n)}{n}$.

The best known lower bound is $\sigma \geq .5$ The construction is due to B.Lindström and uses cyclic codes of minimum distance 5. In fact it is easy to construct binary linear codes of length $2^m - 1$, dimension $1 + 2m$ and strength 4. The 2^{2m+1} corresponding integer $(2^m - 1)$-tuples clearly form a Sidon set. A recent improvement of the upper bound is in [14]: $\sigma \leq 0.5753$.

12 Covering arrays

Orthogonal arrays have multiple applications in statistics and theoretical computer science. Let an orthogonal array of strength t be given (in the linear case this is equivalent to the dual of a code with $d \geq t + 1$). Write the elements of the array as rows of a matrix (array). Interpret the rows as elements of a sample space with uniform distribution, and each of the columns as a random variable. The defining property of an orthogonal array is then equivalent to the statistical property that any t of our random variables are statistically independent. In the linear case we have that linear independence implies statistical independence.

It is a recurrent theme in the applications to replace the requirement of t-wise statistical independence by more relaxed conditions which allow more efficient constructions while still admitting the desired application. Among the notions which fit this description we find universal hash classes, perfect hash classes, almost unbiased and t-wise weakly dependent families of random variables. We consider here just one useful notion:

Definition 8. *An* $(n, N, t)_q-$**covering array** *is an array* $\mathcal{A}$ *with* n *rows and* N *columns, with entries taken from an alphabet of size* q*, such that in every projection onto* t *columns every* t*-tuple occurs at least once.*

Here t is the **strength** of the covering array. This notion is an extremely weak version of the notion of an orthogonal array. Here is a construction for covering arrays, which is based on linear codes. We give only the strength 3 version as it makes direct use of caps.

Theorem 16. *Let q be a prime-power and $Q = q^m$. Let the following be given:*

- *A code $[n, k, d]_Q$, where $d/n \geq 1 - q^{-3}$.*
- *An N-cap in $PG(k-1, q)$.*

Then we can construct an $(Qn, N, 3)_q$−covering array.

Proof. Let $v(1), v(2), \ldots, v(k)$ be a basis of the $\mathbb{F}_Q$−linear code. Form a (Qn, k)−matrix B with rows indexed by the pairs (i, u), where i varies over the n coordinates of the code and $u \in \mathbb{F}_Q$, columns indexed by the $v(j), j = 1, 2, \ldots, k$ and corresponding entries $tr(v_i(j)u)$. Here T is the trace
$: \mathbb{F}_Q \longrightarrow \mathbb{F}_q$ and $v_i(j)$ is the entry in coordinate i of the code-word $v(j)$.
Let $H = (h_{jl})$ represent the cap: the columns of H represent the points of the cap. We claim that $A = BH$ is the desired covering array. The entry in row (i, u) and column l of A is

$$\sum_{j=1}^{k} T(v_i(j)u)h_{jl} = T(u \sum_{j=1}^{k} v_i(j)h_{jl})$$

We have to show that every 3-tuple with entries in $\mathbb{F}_q$ occurs in any set of 3 columns of A. To simplify notation we consider the first 3 columns. Let $(\alpha_1, \alpha_2, \alpha_3) \in \mathbb{F}_q^3$ be given. We have to find a pair (i, u) such that

$$T(u \sum_{j=1}^{k} v_i(j)h_{jl}) = \alpha_l, \text{ for } l = 1, 2, 3.$$

When i is given a proper $u \in \mathbb{F}_Q$ can be chosen for all $(\alpha_1, \alpha_2, \alpha_3)$ if and only if the elements $m_{il} = \sum_{j=1}^{k} v_i(j)h_{jl}$ are linearly independent over $\mathbb{F}_q$. We claim that there is an index i such that $m_{il}, l = 1, \ldots, t$ are indeed linearly independent. Define the codewords $w(l) = \sum_{j=1}^{k} v(j)h_{jl}, l = 1,2,3$. As any 3 columns of H are linearly independent the $w(l)$ are linearly independent. Let W by the $\mathbb{F}_q-$span of the $w(l)$. Then W is an $\mathbb{F}_q-$vector space of dimension 3. Every nonzero codeword has at most n/q^3 zeroes. As there are $q^3 - 1$ nonzero words in W it follows that there must exist a coordinate i such that no nonzero word in W vanishes at i. Assume the $m_{il}, l = 1,2,3$ are linearly dependent, $\sum_{l=1}^{3} \beta_l m_{il} = 0$. Then the nonzero word $\sum_{l=1}^{3} \beta_l w(l) \in W$ vanishes at i, contradiction. ■

13 Large sets of caps

It is a natural problem to partition the points of $PG(n,q)$ or $AG(n,q)$ into a small number of caps. We may call such a partition a **large set of caps** in analogy with large sets of designs, a notion popularized by Luc Teirlinck, see [40] and the section on t-designs in the *Handbook of Combinatorial Designs* [24]. Another application of the notion of a large set is Stinson's discovery [39] that resilient functions are equivalent to large sets of orthogonal arrays.

Definition 9. *Let $\kappa(PG(n,q))$ be the minimal number of caps into which $PG(n,q)$ can be partitioned. $\kappa(AG(n,q))$ is defined analogously.*

Clearly $PG(n,q)$ can be partitioned into l caps if and only if there is a mapping $f : PG(n,q) \rightarrow \{1,2,\ldots,l\}$ such that whenever P_1, P_2, P_3 are different points in $PG(n,q)$ such that $f(P_1) = f(P_2) = f(P_3)$, the P_i are not collinear, equivalently: in the restriction of f to a line no more than two points have the same value.

Once again the case of projective dimension ≤ 3 is easiest. A basic result is the following theorem by Ebert [16]:

Theorem 17. *$PG(3,q), q > 2$ can be partitioned into $q+1$ ovoids, hence $\kappa(PG(3,q)) = q+1$.*

Proof. Let $F = \mathbb{F}_{q^4}$ and $T, N : F \longrightarrow \mathbb{F}_{q^2}$ the trace and norm. Consider the multiplicative subgroup U of order $(q-1)(q^2+1)$ of those nonzero elements satisfying $N(x) \in \mathbb{F}_q$. Observe that U is the union of q^2+1 points in $PG(3,q)$. It suffices to prove that this point set is a cap. The cosets are then caps as well and form the desired partition.

Assume three points of U are collinear. We can choose 1 to be one of them. This yields the equation

$$1 + ax = by$$

where $a, b \in \mathbb{F}_q \setminus \{0\}$ and $x, y \in U$ such that $1, x, y$ generate three different points of $PG(3,q)$. Apply the norm:

$$(1+ax)(1+ax)^{q^2} = 1 + a^2N(x) + aT(x) = b^2N(y) \in \mathbb{F}_q.$$

It follows $T(x) = x + x^{q^2} \in \mathbb{F}_q$. Let $N(x) = \lambda$. Then $T(x) = x + \lambda/x \in \mathbb{F}_q$. It follows $x \in \mathbb{F}_{q^2}$ and $N(x) = x^2 \in \mathbb{F}_q$. We have $x \notin \mathbb{F}_q$. This yields a contradiction in characteristic 2. So let q be odd. Then $T(x) = 2x \in \mathbb{F}_q$. We obtain the same contradiction $x \in \mathbb{F}_q$. ■

Intersection with a plane shows that $PG(2,q)$ can be partitioned into q conics and a point. For odd q this shows $\kappa(PG(2,q)) = q+1$, whereas in characteristic 2 it is conceivable that $\kappa(PG(2,q)) = q$.

Problem 5. *Can $PG(2,q), q$ even be partitioned into q caps?*

Theorem 18. *We have $\kappa(AG(2,q)) = q$ if q is odd, and $\kappa(AG(2,q)) = q-1$ if q is even. In fact $AG(2,q)$ can be partitioned in $q-1$ conics and a point. In characteristic 2 we can partition $AG(2,q)$ into $q-2$ conics and a hyperoval.*

Proof. The upper bounds are obvious. Consider the $q-1$ conics $Var(X^2 + tf(Y,Z))$, where $f(Y,Z)$ is anisotropic and $0 \neq t \in \mathbb{F}_q$. These $q-1$ quadrics are pairwise disjoint. The $q+2$ points of $PG(2,q)$, which are on none of these quadrics, consist of the points on the line $X=0$ and of the isolated point $(1:0:0)$. Choose $X=0$ as line at infinity. This shows that $AG(2,q)$ can be partitioned in $q-1$ conics and a point. Let q be a power of 2. Then $(1:0:0)$ is the nucleus of each of our conics. ■

Theorem 19. $\kappa(AG(3,q)) = q$.

Proof. Consider the hyperplane $H = (x:y:z:0)$ in $PG(3,q)$ and let $\mathcal{O}$ be an ovoid such that $(0:0:1:0) \in \mathcal{O}$ and H is a tangential hyperplane. The points outside H form an affine ovoid, which can be written in the form

$$X_0 = \{(a:b:f(a,b):1\}$$

for some function $f: \mathbb{F}_q^2 \longrightarrow \mathbb{F}_q$. In fact, assume two points of X agree in the first two coordinates. Then these points are linearly dependent of $(0:0:1:0)$, contradiction. Let

$$X_\alpha = \{(a:b:f(a,b)+\alpha:1\}$$

Then the X_α partition the affine space and each X_α is a cap. ■

Theorem 20. *Let the following be given:*

- *A partition of $PG(n,q)$ in k caps C_i.*
- *A partition of $AG(m,q)$ in l caps D_j.*

Then $PG(n+m,q) \setminus PG(m-1,q)$ can be partitioned into $k \cdot l$ product caps.

Proof. Write the elements of $PG(n,q)$ as $(n+1)-$tuples in standardized form, with first nonzero entry $=1$. Write the elements of $AG(m,q)$ as $m-$tuples. The fact that D_j is an affine cap is equivalent to the fact that the $(m+1)-$tuples $(1,x)$, where $x\in D_j$, represent a cap in $PG(m,q)$. The product construction Theorem 4 says that (C_i,D_j) represents a cap in $PG(n+m,q)$. The union of these caps partitions all of $PG(n+m,q)$, except for a subspace $PG(m-1,q)$. ■

Theorem 20 is a straightforward generalization of a construction by Grannell et.al. [23]. We obtain the following:

Theorem 21. *We have*

$$\begin{aligned}\kappa(AG(n+m,q)) &\leq \kappa(AG(n,q))\cdot\kappa(AG(m,q))\\ \kappa(PG(n+m,q)) &\leq \kappa(PG(n,q))\cdot\kappa(AG(m,q))+\kappa(PG(m-1,q))\end{aligned}$$

Definition 10. *Let*

$$\kappa_q = lim_{n\to\infty}\frac{log_q(\kappa(PG(n,q))}{n} = lim_{n\to\infty}\frac{log_q(\kappa(AG(n,q))}{n}.$$

It is a natural asymptotic problem to determine κ_q. Theorem 21 shows that κ_q is well-defined and that each value $\kappa(AG(k,q))$ in a fixed dimension k yields a lower bound on κ_q :

Corollary 2. *For every k and q we have*

$$\kappa_q \leq \frac{log_q(\kappa(AG(k,q))}{k}.$$

Clearly $\kappa(AG(k,q)\cdot m_2(AG(k,q))\geq q^k$. Comparison with Section 6 shows

$$\kappa_q \geq 1-\lambda(3,q).$$

Theorem 19 (or Theorem 17) implies that $\lambda_q \leq 1/3$ for all q. Once again more is known in the ternary case. The best lower bound known on κ_3 is derived from the 5-dimensional case.

Theorem 22. *Let $PG(k,3)$ be partitioned into $2l$ caps. Then $AG(k+2,3)$ can be partitioned into $3l$ caps.*

Proof. Let A_i and $B_i, i = 1, 2 \ldots, l$ be the caps partitioning $PG(k,3)$. For each i consider the three caps

$(1, \pm A_i, 0)$ $(1, \pm B_i, 1)$
$(1, \pm A_i, 1)$ $(1, \pm B_i, 2)$
$(1, \pm A_i, 2)$ $(1, \pm B_i, 0)$

These partition $AG(k+2,3)$ with the exception of the three points $(1, 0, c)$. Clearly these can be amalgamated to some of the caps above. ∎

Theorem 22 implies $\kappa(AG(5,3)) = 6$. Corollary 2 yields the bound $\kappa_3 \leq \frac{log_3(6)}{5}$ from [23].

It seems that B.Kestenband first studied large sets of caps. She also used mixed partitions of projective geometries (partitions into subvarieties of various kinds) as a tool. Baker et.al. [1] partition $PG(5,q)$ into two skew planes and $q^3 - 1$ caps.

Next we show how $PG(3r-1,q)$ can be partitioned into a $(2r-1)$-space, an $(r-1)$-space and $q^r - 1$ cyclic caps. This is from [4]. Let $F = \mathbb{F}_{q^{2r}}$ and $L = \mathbb{F}_{q^r}$, where $r \geq 2$. Consider the direct sum $V = F \bigoplus L$, an $3r-$dimensional vector space over $\mathbb{F}_q$. We write the elements of the corresponding $PG(3r-1,q)$ with homogeneous coordinates $(a : b)$, where $a \in F, b \in L$. Let α be a primitive element of F. The action of the Singer cycle determined by α lifts to V as follows:

$$g : (a, b) \mapsto (a\alpha^{q^{r-1}+1}, b\alpha^{q^r+1}).$$

This induces an action on $PG(3r-1,q)$ in the canonical way. The Singer cycle has order $(q^{2r} - 1)/(q - 1)$ both in its action on $PG(2r-1,q)$ and in the lifted action on $PG(3r-1,q)$.

The orbit containing $(a:b)$, where $ab \neq 0$, will be denoted by $\mathcal{O}(a:b)$. Let $N, T: F \longrightarrow L$ be norm and trace, respectively. The projective subspaces spanned by F and L are denoted $PG(F), PG(L)$. The subgroup of order u of the multiplicative group of F is denoted $Z(u)$. The group $Z(q^r+1)$ consists of the elements of norm $N=1$. Let $Q=q^r$ and $U=F^{*(q+1)}=Z((q^{2r}-1)/(q+1))$.

Theorem 23. *For every $0 \neq a \in F$, $0 \neq b \in L$, the orbit $\mathcal{O}(a:b)$ containing $(a:b) \in PG(3r-1,q)$ under the lifted action of the Singer cycle has full length $(q^{2r}-1)/(q-1)$ and is a cap.*

Proof. Assume $\mathcal{O}(a:b)$ is not a cap. There must be three collinear points

$$(a:b), (ax^{q^{r-1}+1} : bx^{q^r+1}), (ay^{q^{r-1}+1} : by^{q^r+1})$$

in $\mathcal{O}(a:b)$. As these points are different, we have $x, y \notin \mathbb{F}_q$ and $x/y \notin \mathbb{F}_q$. There are coefficients $\lambda_i \in \mathbb{F}_q$ (by force all nonzero), such that

$$\boxed{\begin{array}{ccccccc} a\lambda_1 & + & a\lambda_2 x^{q^{r-1}+1} & + & a\lambda_3 y^{q^{r-1}+1} & = & 0 \\ b\lambda_1 & + & b\lambda_2 N(x) & + & b\lambda_3 N(y) & = & 0 \end{array}}$$

Obviously we may as well assume $a=b=1$. Choosing $\lambda_3=-1$ and reordering we obtain

$$\boxed{\begin{array}{ccccc} y^{q^{r-1}+1} & = & \lambda_2 x^{q^{r-1}+1} & + & \lambda_1 \\ N(y) & = & \lambda_2 N(x) & + & \lambda_1 \end{array}}$$

We compute $N(y^{q^{r-1}+1})$ in two ways. Using the second equation we obtain

$$N(y^{q^{r-1}+1}) = N(y)^{q^{r-1}+1} = (\lambda_2 N(x)^{q^{r-1}} + \lambda_1)(\lambda_2 N(x) + \lambda_1) =$$

$$= \lambda_2^2 N(x)^{q^{r-1}+1} + \lambda_1\lambda_2(N(x)^{q^{r-1}} + N(x)) + \lambda_1^2.$$

The first equation yields

$$N(y^{q^{r-1}+1}) = N(\lambda_2 x^{q^{r-1}+1} + \lambda_1) = (\lambda_2 x^{q^r(q^{r-1}+1)} + \lambda_1)(\lambda_2 x^{q^{r-1}+1} + \lambda_1) =$$

$$= \lambda_2^2 N(x)^{q^{r-1}+1} + \lambda_1\lambda_2(x^{q^r(q^{r-1}+1)} + x^{q^{r-1}+1}) + \lambda_1^2.$$

Comparing these expressions and eliminating the obvious common terms we obtain

$$x^{q^{r-1}(q^r+1)} + x^{q^r+1} = x^{q^r(q^{r-1}+1)} + x^{q^{r-1}+1}.$$

Collect all terms on one side, eliminate the common factor $x^{q^{r-1}+1}$. Fortunately the polynomial factors:

$$0 = x^{q^{2r-1}+q^r-q^{r-1}-1} - x^{q^{2r-1}-1} - x^{q^r-q^{r-1}} + 1 = (x^{q^r-q^{r-1}} - 1)(x^{q^{2r-1}-1} - 1).$$

If the first factor vanishes, then $x^{q-1} = 1$, hence $x \in \mathbb{F}_q$, contradiction. Assume the second factor vanishes. As $gcd(q^{2r}-1, q^{2r-1}-1) = gcd(q^{2r-1}-1, q-1) = q-1$ we obtain the same contradiction. ■

As the union of a cap in $PG(F)$ and a cap in $PG(L)$ clearly is a cap we obtain

$$\kappa(PG(3r-1,q)) \leq q^r - 1 + \kappa(PG(2r-1,q)).$$

In case $r = 2$ this yields $\kappa(PG(5,q)) \leq q^2 - 1 + (q+1) = q^2 + q$. For even q it is better to apply Theorem 21 with $n = 3, m = 2$. This yields $\kappa(PG(5,q)) \leq (q-1)(q+1) + \lceil (q+1)/2 \rceil = q^2 + q/2$.

14 Caps and additive codes in computer memory systems

Codes with small distances have a long history in computer memory systems. As we know linear codes with minimal distance $d = 4$ are equivalent to caps. The points of the cap are described by the columns of the code's check matrix

H. The type of application which we consider in this section not only is an application of caps, it also motivates various fruitful generalizations and variations: linear codes with small minimal distances like $d = 5$, additive codes and codes (caps) with a large group of symmetries.

In this literature the binary codes with $d = 4$ are known as SEC-DED codes (*single error-correcting and double error-detecting*). Naturally these are derived by shortening from codes $[2^r, 2^r - (r+1), 4]_2$ (the extended binary Hamming codes). Hsiao has given a construction of codes with these parameters, which is more symmetric than adding a parity check bit to the Hamming codes. These **odd-weight column codes** (the name describes the construction) *have been widely implemented by IBM and the computer industry worldwide* (see [13]).

An interesting situation arises when a multiple-bit-per-chip organization is used. In this case the bits are grouped together in **bytes,** where each byte has m bits. The codes can then be considered as defined over an alphabet with 2^m elements. The class of SBC-DBD codes (*single byte error-correcting and double byte error-detecting*) are by definition 2^m-ary additive codes of minimum distance $d = 4$. We give a more general definition:

Definition 11. *An $\mathbb{F}_q$-linear q^m-ary additive code $[n, k, d]_{q^m}$ is a code whose entries form an m-dimensional vector space over $\mathbb{F}_q$, and which is $\mathbb{F}_q$-linear. If we write the set of entries as $\mathbb{F}_q^m$, then each word is an n-tuple of q-ary m-tuples and can therefore be seen as a q-ary nm-tuple. Here k is the q^m-ary dimension (the number of codewords is q^{km}). Because of $\mathbb{F}_q$-linearity d equals the minimum weight: each nonzero codeword has entries $\neq 0$ in at least d of its n coordinate sections. Observe that k can be rational, but km is integer.*

The additive codes from Definition 11 form a natural generalization of linear codes (linear codes correspond to the special case $m = 1$). Observe that we have a natural notion of duality, with respect to the dot product in $\mathbb{F}_q^{nm}$. It is clear that the dual of an $\mathbb{F}_q$-linear $[n, k, 4]_{q^m}$-code is a q-linear $[n, n-k]_{q^m}$-code, which is an orthogonal array of strength 3. Such codes form natural generalizations of caps. An extension of the mechanism of cyclic codes from the linear to the additive case is in [3].

Most constructions in the computer memory literature use $\mathbb{F}_{2^m}$-linearity.

In this case we have equivalence with caps in characteristic 2. The idea is that some errors tend to occur in bursts. We want to be able to correct several errors if only they occur within the same byte. That is what q-ary codes with distance ≥ 3 do. Assume $d > 3$. If decoding does not work, then more than one byte must be in error. In this sense these codes (caps) will in the same process correct one byte error and detect two byte errors. Part of the theory of caps and of high-dimensional codes has been developed in parallel in this literature. For example, we find construction Y_1 from coding theory in [13]. Paper [10] contains a construction of the ovoids as well as the product construction and in particular the doubling construction for caps.

The following basic construction seems to be due to C.L.Chen [11]:

Theorem 24 (Chen projection). *If there is a q^m-ary $q-$linear code $[n,k,d]$ with $m > 1$, there is a q^{m-1}-ary $q-$linear code $[n, k - \dfrac{n-k-1}{m-1}, d]$.*

Proof. Let $\mathcal{C}$ be a q^m-ary $q-$linear code $[n,k,d]$. Application of an arbitrary regular (m,m)-matrix in each coordinate yields a code, which is equivalent to $\mathcal{C}$. We can therefore assume that $\mathcal{C}^\perp$ contains a word, which in each coordinate has as entry either $(0,\dots,0,1)$ or $(0,\dots,0,0)$. The q-ary dimension of $\mathcal{C}$ is km. Consider the subcode $\mathcal{D} \subset \mathcal{C}$ consisting of those words, which vanish in the last position of each coordinate. We have $dim_q(\mathcal{D}) \geq km - (n-1)$. Clearly we can omit this last position in each coordinate and obtain a q^{m-1}-ary $q-$linear code of q^{m-1}-ary dimension $\geq \frac{km-(n-1)}{m-1} = k - \frac{n-1-k}{m-1}$. ∎

Application of Chen projection to hyperovals and ovoids yields additive codes with $d = 4$ and very high dimension. Here are some examples of $\mathbb{F}_2$-linear code parameters constructed in this way:

$$[65, 59\frac{1}{2}, 4]_4,\ [1025, 1016\frac{1}{2}, 4]_4,$$

$$[18, 14\frac{1}{3}, 4]_8,\ [257, 252, 4]_8,\ [1025, 1019, 4]_8,$$

$$[34, 30\frac{1}{2}, 4]_{16}, [1025, 1020\frac{1}{4}, 4]_{16}.$$

For example, compare the last two 8-ary additive codes above with corresponding 8-ary linear codes. The largest caps known have 208 points in $PG(4,8), 695$ points in $PG(5,8)$. Equivalently this yields linear codes $[208,203,4]_8, [695,689,4]_8$, much weaker parameters than those of the additive codes derived from caps via Chen projection. Some of these codes have found multiple applications in computer memory systems, see [11, 12].

Another interesting feature is the use of symmetry. Kaneda-Fujiwara [28] show how certain symmetries can be used to partition the encoding-decoding circuitry into identical modules and to parallelize the computations. We conclude that practical needs demand the construction of caps and of high-dimensional codes with large groups of automorphism.

15 tms-nets

$(t,m,s)-$nets were defined by Niederreiter [34] in the context of quasi-Monte Carlo methods of numerical integration. Close links to combinatorial structures had been noticed right from the start and were further explored in [29, 33, 37]. Our setting is inspired by Rosenbloom-Tsfasman [36].

Let $\Omega = \Omega^{(T,s)}$ be a set of Ts elements, partitioned into s **blocks** $B_i, i = 1, 2 \dots, s$, where $B_i = \{\omega_1^{(i)}, \dots, \omega_T^{(i)}\}$. Each block carries a total ordering:

$$\omega_1^{(i)} < \omega_2^{(i)} \dots < \omega_T^{(i)}.$$

This gives Ω the structure of a partially ordered set, the union of s totally ordered sets of T points each. We consider Ω as a basis of a $Ts-$dimensional vector space $\mathbb{F}_q^{(T,s)}$. An **ideal** in Ω is a set of elements closed under predecessors. An **antiideal** is a subset closed under followers, equivalently the complement of an ideal.

Visualize elements $x = (x_j^{(i)}) \in \mathbb{F}_q^{(T,s)}, i = 1, \dots, s; j = 1, \dots, T$ as matrices with T rows and s columns. The **Rosenbloom-Tsfasman metric** is defined as follows: if in each block the leading zeroes evaporate, the number of remaining cells is the **weight** $\rho(x)$. The **distance** between x and y is then $\rho(x-y)$. The **minimum weight** (=minimum distance) of a subspace $\mathcal{C} \subseteq \mathbb{F}_q^{(T,s)}$ is the minimum among the weights of its nonzero members.

A linear subspace (code) $\mathcal{C} \subseteq \mathbb{F}_q^{(T,s)}$ has **strength** $k = k(\mathcal{C})$ if k is maximal such that the projection from $\mathcal{C}$ to any ideal of size k is onto. We also call such a subspace an **ordered orthogonal array** OOA, which is

$q-$linear, has **length** s, **depth** T, **dimension** $m = dim(\mathcal{C})$ and strength k. Duality is defined with respect to the symmetric bilinear form

$$\langle x, y\rangle = \sum_{i=1}^{s} x_1^{(i)} y_T^{(i)} + x_2^{(i)} y_{T-1}^{(i)} + \cdots + x_T^{(i)} y_1^{(i)}.$$

These notions are justified by the following generalization of the duality principle for linear codes.

Theorem 25. *Let $\mathcal{C} \subseteq \mathbb{F}_q^{(T,s)}$ be a linear subspace (code). Then*

$$\rho(\mathcal{C}^{\perp}) = k(\mathcal{C}) + 1.$$

We call $\mathbb{F}_q^{(T,s)}$ with these notions of duality, strength and distance the Niederreiter-Rosenbloom-Tsfasman space, short **NRT-space.** Observe that in case $T = 1$ we obtain the Hamming space of coding theory.

In order to understand the application to quasi-Monte Carlo methods of numerical integration interpret $x \in \mathbb{F}_q^{(T,s)}$ as a point in the $s-$dimensional unit cube by reading the $x_j^{(i)}$ for fixed i as the T first digits of the $q-$ary expansion of a real number between 0 and 1. As an example, the point $\begin{array}{|c|c|c|c|}\hline 0 & 0 & 1 & 1 \\ \hline 1 & 1 & 1 & 0 \\ \hline 1 & 0 & 0 & 1 \\ \hline \end{array}$ in $\mathbb{F}_2^{(3,4)}$ is mapped to the point $(\frac{3}{8}, \frac{1}{4}, \frac{3}{4}, \frac{5}{8}) \in [0, 1)^4$. This also motivates the hierarchical ordering inside the blocks.

The aim is to construct point sets in the unit cube of s-dimensional Euclidean space, which in some sense are almost uniformly distributed. A code of strength k in NRT-space corresponds to a set of points in the s-dimensional unit cube, which is almost uniformly distributed: we control the first k digits in q-adic expansion. This is why **tms-nets** are the most important objects in this theory. By definition a linear $(m-k, m, s)_q$-net is equivalent to an $m-$dimensional code $\mathcal{C} \subseteq \mathbb{F}_q^{(k,s)}$ of strength k. OOA of strength 3 in NRT-space may be seen as the most natural generalization of the notion of a cap under our present perspective.

As NRT-space is a generalization of Hamming space, and NRT-space of depth 1 is identical to Hamming space, it is a natural strategy to generalize methods from coding theory. A natural problem is the problem of **net-embeddability:** given an m-dimensional linear orthogonal array of strength k and length s (the dual of a code $[s, s-m, k+1]$ if $s > m$), is it possible to construct an m-dimensional OOA of strength k in NRT-space of depth k (equivalently: a tms-net), which projects to the given OA? In [7] we used Gilbert-Varshamov type arguments to prove net-embeddability under certain general numerical conditions. It turns that each s-cap in $PG(m-1,q)$ is net-embeddable provided $1+(s-1)(q-1) < q^{m-1}$. This was first proved in [37]. To give just one example, the Hill cap yields a $(3,6,56)_3$-net.

References

[1] R.D.Baker,A.Bonisoli,A.Cossidente and G.L.Ebert: *Mixed partitions of* $PG(5,q)$, *Discrete Mathematics* **208/209** (1999),23-29.

[2] L.M.Batten: *Determining sets, Australasian Journal of Combinatorics* **22** (2000), 167-176.

[3] J.Bierbrauer: *The theory of cyclic codes and a generalization to additive codes, Designs, Codes and Cryptography,* to appear.

[4] J.Bierbrauer,A.Cossidente and Y.Edel: *Caps on classical varieties and their projections, European Journal of Combinatorics* **22** (2001), 135-143.

[5] J.Bierbrauer and Y.Edel *A family of caps in projective 4-space in odd characteristic, Finite Fields and Their Applications* **6** (2000),283-293.

[6] J.Bierbrauer and Y.Edel *Bounds on affine caps,* to appear in *Journal of Combinatorial Designs.*

[7] J.Bierbrauer, Y.Edel and W.Ch. Schmid: *Coding-theoretic constructions for* (t,m,s)*-nets and ordered orthogonal arrays,* submitted to *Journal of Combinatorial Designs.*

[8] D.Boneh and J.Shaw: *Collusion-secure fingerprinting for digital data, IEEE Transactions on Information Theory* **44** (1998), 1897-1905.

[9] A.R. Calderbank and P.C. Fishburn: *Maximal three-independent subsets of* $\{0,1,2\}^n$, *Designs, Codes and Cryptography* **4** (1994),203-211.

[10] C.L.Chen: *Byte-oriented error-correcting codes for semiconductor memory systems, IEEE Transactions on Information Theory* **35** (1986),646-648.

[11] C.L.Chen: *Symbol error-correcting codes for computer memory systems, IEEE Transactions on Computers* **41**(1992),252-256.

[12] C.L.Chen and L.E.Grosbach: *Fault-tolerant memory design in the IBM Application System/400,* Digest of Papers, *The 21-th International Symposium on Fault-Tolerant Computing* (1991),393-400.

[13] C.L.Chen and M.Y. Hsiao: *Error-correcting codes for semiconductor memory applications: a state-of-the-art review, IBM Journal Res. Develop.* **2**(1984),124-134.

[14] G. Cohen, S.Litsyn and G. Zémor: *Binary B_2-sequences: a new upper bound, Journal of Combinatorial Theory A* **94** (2001),152-155.

[15] I.Dumer: *Nonbinary double-error-correcting codes designed by means of algebraic verieties, IEEE Transactions on Information Theory* **41**(1995),1657-1666.

[16] G.L. Ebert, *Partitioning projective geometries into caps, Canadian Journal of Mathematics* **37** (1985), 1163-1175.

[17] Yves Edel: *Extensions of generalized product caps,* submitted to *Designs, Codes and Cryptography.*

[18] Y.Edel and J.Bierbrauer, *Recursive constructions for large caps, Bulletin of the Belgian Mathematical Society - Simon Stevin* **6** (1999), 249-258.

[19] Y.Edel and J.Bierbrauer, *41 is the largest size of a cap in $PG(4,4)$, Designs, Codes and Cryptography* **16** (1999),151-160.

[20] Y.Edel and J.Bierbrauer, *Large caps in small spaces, Designs, Codes and Cryptography* **23** (2001),197-212.

[21] Y.Edel, S.Ferret, I.Landgev and L.Storme: *The classification of the largest caps in $AG(5,3)$*, submitted to *Journal of Combinatorial Theory A.*

[22] D.Glynn and Te Tari Tatau: *A* 126*-cap of* $PG(5,4)$ *and its corresponding* $[126,6,88]$*-code, Utilitas Mathematica* **55** (1999),201-210.

[23] M.Grannell,T.Griggs and R.Hill: *The triangle chromatic index of Steiner triple systems,* Australasian Journal of Combinatorics **23** (2001),217-230.

[24] The CRC Handbook of Combinatorial Designs, C.J. Colbourn and J.H.Dinitz (eds.), CRC Press 1996.

[25] R.Hill: *The largest size of cap in* $S_{5,3}$, *Rend. Acc. Naz. Lincei (8)* **54** (1973), 378-384.

[26] J.W.P. Hirschfeld: *Finite projective spaces of three dimensions,* Clarendon, Oxford 1985.

[27] J.W.P. Hirschfeld and L.Storme: *The packing problem in statistics, coding theory and finite geometry: update 2001,* Finite Geometries, Developments of Mathematics, *Kluwer 2001*, 201-246.

[28] S.Kaneda and E.Fujiwara: *Single-byte error-correcting - double byte error detecting codes for memory systems, IEEE Transactions on Information Theory* **31** (1982),596-602.

[29] K. M. Lawrence: *A combinatorial characterization of* (t,m,s)*-nets in base b,* Journal of Combinatorial Designs **4** (1996),275-293.

[30] B. Lindström: *Determination of two vectors from the sum,* Journal of Combinatorial Theory **6** (1969), 402-407.

[31] R.Meshulam: *On subsets of finite abelian groups with no 3-term arithmetic progression,* Journal of Combinatorial Theory A **71**(1995),168-172.

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

[33] G. L. Mullen and W. Ch. Schmid: *An equivalence between* (t,m,s)*-nets and strongly orthogonal hypercubes,*
Journal of Combinatorial Theory A **76** (1996), 164-174.

[34] H.Niederreiter: *Point sets and sequences with small discrepancy, Monatshefte Mathematik* **104**(1987),273-337.

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

[36] M.Yu. Rosenbloom and M.A.Tsfasman: *Codes for the m-metric, Problems of Information Transmission* **33**(1997),45-52, translated from *Problemy Peredachi Informatsii* **33**(1996),55-63.

[37] W.Ch.Schmid: (T, M, S)*-nets: digital construction and combinatorial aspects,* PhD dissertation, Salzburg (Austria), 1995.

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

[39] D.R.Stinson: *Resilient functions and large sets of orthogonal arrays, Congressus Numerantium* **92** (1993), 105-110.

[40] L.Teirlinck: *Large sets of disjoint designs and related structures,* in *Contemporary Design Theory: A Collection of Surveys (J.H.Dinitz and D.R.Stinson, eds) Wiley 1992*, 561-592.

[41] J. Tits, *Ovoides et groupes de Suzuki, Archiv der Mathematik* **13** (1962), 187-198.