A family of caps in projective 4-space in characteristic 2

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 15, 2002

Riassunto

Si costruiscono calotte di cardinalità $2q^2+q+9$ negli spazi di Galois $PG(4,q)$ 4-dimensionali per ogni $q = 2^f > 4$.

Abstract

We construct $(2q^2+q+9)$-caps in projective 4-space $PG(4,q)$ in characteristic two for every $q > 4$.

Key words

Caps, Galois geometries, codes, ovals, ovoids.

AMS classification

51E22,94B05.

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. It follows that a set of n points in $PG(k-1,q)$, which form a cap, is equivalent to a q-ary linear code $[n, n-k, 4]_q$. Denote by $m_2(k,q)$ the maximum cardinality of a cap in $PG(k,q)$. In the binary case this is a trivial problem. In fact, choosing all nonzero k-tuples as columns we obtain a binary $(k, 2^k-1)$-matrix of strength 2 (meaning that no two columns are linearly dependent), where the number of rows is clearly maximal. The dual is a binary code $[2^k-1, 2^k-(k+1), 3]_2$. Addition of a parity-check bit yields $[2^k, 2^k-(k+1), 4]_2$. We conclude

$$m_2(k,2) = 2^k.$$

We can and will assume $q > 2$ in the sequel. For dimensions ≤ 3 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. We start in section 2 by describing conic sections and elliptic quadrics in terms of quadratic field extensions

(Theorem 2). Tallini [2] studied caps in $PG(4,q)$ containing elliptic quadrics in two hyperplanes. His results in the case when $q > 2$ is even may be summarized as follows: A cap in $PG(4,q)$ intersecting each of two different hyperplanes in an elliptic quadric can have at most $2q^2+q+5$ points. Such (necessarily complete) $(2q^2+q+5)$-caps do in fact exist.
In section 3 we give a concrete description of $(2q^2+q+5)$-caps satisfying Tallini's properties in $PG(4,q)$, for every even $q > 2$. This description uses the terminology of section 2. In section 4 we start from Tallini's cap $\mathcal{Q}$ as described in

section 3. There is a plane S intersecting $\mathcal{Q}$ in 6 points. We remove these 6 points from $\mathcal{Q}$ and add a set $\mathcal{D}$ of 10 different points of S to $\mathcal{Q}$. Nine of these ten points are on a conic section $V(Q)$, the tenth point is the nucleus of $V(Q)$. The resulting set $(\mathcal{Q} \setminus S) \cup \mathcal{D}$ is a $(2q^2+q+9)$-cap in $PG(4,q)$, thus proving the following:

Theorem 1

$$m_2(4,q) \geq 2q^2+q+9 \text{ if } q = 2^f > 4.$$

For the state of the art and further references we refer to [1]. For calculations in $PG(3,q)$ we use homogeneous coordinates. Points are $(x_1 : x_2 : x)$, where $x \in \mathbb{F}_{q^2}$. $PG(4,q)$ is coordinatized in an analogous way: the points are quadruples $(x_1 : x_2 : x_3 : x)$.

2 Ovals and ovoids

We start by giving a concrete description of the classical ovals and ovoids.

Theorem 2 *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 $PG(3,q)$.*

Proof: 1. It is clear that no two of our columns are multiples of each other. Assume $\sum_{i=1}^{3} \lambda_i(1, b_i) = 0$. We know that the $\lambda_i \in I\!F_q$ are nonzero and the b_i are pairwise different. The first coordinate shows $\sum_i \lambda_i = 0$, hence

$$\lambda_3^2 = \lambda_1^2 + \lambda_2^2 + 2\lambda_1\lambda_2.$$

The last set of coordinates shows $-\lambda_3 b_3 = \lambda_1 b_1 + \lambda_2 b_2$. Raising this to the $(q+1)^{th}$ power we obtain

$$\lambda_3^2 a = (\lambda_1 a/b_1 + \lambda_2 a/b_2)(\lambda_1 b_1 + \lambda_2 b_2).$$

After removal of the common factor a this yields $\lambda_3^2 = \lambda_1^2 + \lambda_2^2 + \lambda_1\lambda_2(x + 1/x)$, where $x = b_1/b_2 \neq 1$. Comparison with the expression of λ_3^2 given above yields $2 = x + 1/x$. Multiply by x, collect all terms on one side. This yields $0 = x^2 - 2x + 1 = (x-1)^2$. We obtain the contradiction $\zeta_1 = \zeta_2$.
2. It is easy to see that e_2 is not linearly dependent of any two of the remaining columns. Assume $\sum_{i=1}^{3} \lambda_i(1, au_i^{q+1}, u_i) = 0$, where the u_i are three different elements of $I\!F_{q^2}$. Clearly we can assume without restriction that $a = 1$. We proceed as before, observing at first that the coefficients λ_i are nonzero. The first coordinate shows $-\lambda_3 = \lambda_1 + \lambda_2$, the second coordinate shows

$$-\lambda_3 u_3^{q+1} = \lambda_1 u_1^{q+1} + \lambda_2 u_2^{q+1}.$$

We start from the last coordinate. Raising the corresponding equation to the $(q+1)^{th}$ power yields

$$\lambda_3^2 u_3^{q+1} = (\lambda_1 u_1^q + \lambda_2 u_2^q)(\lambda_1 u_1 + \lambda_2 u_2) =$$
$$= \lambda_1^2 u_1^{q+1} + \lambda_2^2 u_2^{q+1} + \lambda_1\lambda_2(u_1 u_2^q + u_2 u_1^q).$$

Comparison with the first two coordinates yields $u_1^{q+1} + u_2^{q+1} = u_1 u_2^q + u_2 u_1^q$. This last equation is equivalent to $(u_1 - u_2)^{q+1} = 0$. We obtain the contradiction $u_1 = u_2$.■

Corollary 1 *The ovoids described in Theorem 2 can be decomposed into two points and $q-1$ disjoint ovals.*

Proof: Consider the ovoid as described in part 2. of Theorem 2. We fix the two points e_2 and $e_1 = (1 : 0 : 0 : \mathbf{0})$. For every $\alpha \in I\!F_q^*$ the set $Q_\alpha = \{(1 : a\alpha : u) \mid u^{q+1} = \alpha\}$ is contained in the plane with equation $x_2/x_1 = a\alpha$ and forms an oval.■

Lemma 1 *Let q be a power of 2. The nucleus N of the oval given in Theorem 2 is $N = (1 : 0 : \mathbf{0})$.*

Proof: Assume vectors $(1 : 0 : \mathbf{0}), (1 : b_1)$ and $(1 : b_2)$ are linearly independent. Then $b_2 = \lambda \cdot b_1, \lambda \in I\!F_q$. It follows $1 = \lambda^{q+1} = \lambda^2$, hence $\lambda = 1$. This yields $b_1 = b_2$.■

3 Tallini's caps

Definition 1 *Let $q > 2$ be a power of 2. Choose $z \in I\!F_q \setminus I\!F_4$, put $\alpha = 1/\sqrt{1 + z + 1/z}$. Define the point set*

$$\mathcal{Q} = \mathcal{Q}_1 \cup \mathcal{Q}_2 \cup \mathcal{U}_1 \cup \mathcal{U}_2 \cup \mathcal{R}.$$

Here

$$\mathcal{Q}_1 = \{(0 : 0 : 1 : \mathbf{0})\} \cup \{(1 : 1 : a : b) \mid b^{q+1} = a\},$$

$$\mathcal{Q}_2 = \{(0 : 1 : 1 : \mathbf{0})\} \cup \{(1 : c : c : d) \mid d^{q+1} = c\},$$

$$\mathcal{U}_1 = \{(1 : 0 : 1 : \zeta) \mid \zeta^{q+1} = 1\}, \mathcal{U}_2 = \{(1 : \alpha : 1 : f) \mid f^{q+1} = \alpha^2\},$$

and $\mathcal{R} = \{(1 : r_1 : 1 : \mathbf{0}), (1 : r_2 : 1 : \mathbf{0})$.

Theorem 3 *Let $q > 4$ be a power of 2. Choose $r_1, r_2 \notin I\!F_2 \cup \{\alpha/(\alpha + 1)\}$. Then the point set $\mathcal{Q}$ of Definition 1 is a $\{2q^2 + q + 5\}$-cap in $PG(4, q)$.*

Proof: We have $\mathcal{Q}_1 \subset H_1$, where H_1 is the solid with equation $x_1 = x_2$. It follows from Theorem 2 that $\mathcal{Q}_1$ is an ovoid. Analogously, $\mathcal{Q}_2$ is an ovoid in $H_2 = (x_2 = x_3)$. Let $E = H_1 \cap H_2$. Then $\mathcal{C} = \mathcal{Q}_1 \cap \mathcal{Q}_2 = \mathcal{Q}_1 \cap E = \mathcal{Q}_2 \cap E = \{(1 : 1 : 1 : \zeta) \mid \zeta^{q+1} = 1\}$. It follows that $\mathcal{Q}_1 \cup \mathcal{Q}_2$ is a cap and $\mathcal{Q}$ has $2q^2 + q + 5$ elements. All the points of $\mathcal{Q}$ not in H_1 or H_2 are in the solid H_3 with equation $x_1 = x_3$. Our proof will naturally fall into two parts: We show at first that $\mathcal{Q} \cap H_3$ is a cap.
$\mathcal{Q} \cap H_3$ is a cap: In this part of the proof we omit a redundant coordinate by writing $(1 : a : b)$ instead of $(1 : a : 1 : b)$. We have $\mathcal{Q} \cap H_3 = \mathcal{C} \cup \mathcal{U}_1 \cup \mathcal{U}_2 \cup \mathcal{R}$ (consisting of $3q - 1$ points). We observe that each of $\mathcal{C}, \mathcal{U}_1, \mathcal{U}_2$ is an oval, these ovals live in different planes and do not share points with any line of intersection between two such planes. It follows that a line containing more

than two points of $\mathcal{Q} \cap H_3$ cannot contain more than one point of each of these ovals. Let l be a line containing at least 3 points of $\mathcal{Q} \cap H_3$. The last coordinate section shows that l does not contain both points of $\mathcal{R}$.
Assume point $(1 : r_1 : \mathbf{0}) \in l$. We have an equation

$$(1, r_1, \mathbf{0}) = \lambda_2(1, a_1, b_1) + \lambda_3(1, a_2, b_2).$$

The first coordinate shows $\lambda_2 + \lambda_3 = 1$. The last coordinate yields, after raising to power $(q+1)$, that $b_2^{q+1} = b_1^{q+1} \cdot \frac{\lambda_2^2}{\lambda_3^2}$. If $b_2^{q+1} = b_1^{q+1}$, then the contradiction $\lambda_2 = \lambda_3$ would follow. It follows that we can choose without restriction $a_1 = \alpha$ and $(1 : \alpha : 1 : b_1) \in \mathcal{U}_2, b_2^{q+1} = 1$ and $a_2 \in \{0, 1\}$. We obtain $\lambda_2 = 1/(\alpha+1), \lambda_3 = \alpha/(\alpha+1)$. The second coordinate shows $r_1 = \alpha/(\alpha+1) + a_2\lambda_3$. If $a_2 = 1$, then $r_1 = 0$, contradiction. If $a_2 = 0$. then $r_1 = \alpha/(\alpha+1)$, contradiction again.
It follows that l must pick one point from each of our three ovals. We must therefore have an equation of the form

$$(1, 0, b_1) = \lambda_2(1, 1, b_2) + \lambda_3(1, \alpha, b_3),$$

where $b_1^{q+1} = b_2^{q+1} = 1, b_3^{q+1} = \alpha^2$. The first two coordinates show $\lambda_2 = \alpha/(\alpha+1), \lambda_3 = 1/(\alpha+1)$. The last coordinate yields $b_3 = (\alpha+1)b_1 + \alpha b_2$. Raising to power $q+1$ yields $\alpha^2 = 1 + \alpha(\alpha+1)(x + 1/x)$, where $x = b_1/b_2$. Multiply by x, reorder terms. We obtain $x^2 + (1 + 1/\alpha)x + 1 = 0$. By our choice of α we have $1 + 1/\alpha = z_0 + 1/z_0$, where $z_0 = \sqrt{z}$. The equation above splits: $(x + z_0)(x + 1/z_0) = 0$. Assume $x = z_0$. Then $1 = x^{q+1} = z_0^2$. It follows $z = z_0 = 1$, hence $\alpha = 1$, contradiction. In case $x = 1/z_0$ the same contradiction is obtained.
Main part of the proof: Let l be a line containing three points of $\mathcal{Q}$. By what we have shown above the only possibility is that each $H_i \setminus E$ contributes one point of $\mathcal{Q} \cap l$. Put $\{P_i\} = l \cap H_i \subset \mathcal{Q}$. The first three coordinates show that $P_1 = (0, 0, 1, \mathbf{0}), P_2 = (0, 1, 1, \mathbf{0})$ is impossible. Assume $P_1 = (0, 0, 1, \mathbf{0})$. Then $P_2 = (1, a, a, b), P_3 = (1, c, 1, d)$. The first two coordinates show $c = a$. The last coordinate yields then $d = b$. As $b^{q+1} = a$, we have $d^{q+1} = c$. The definition of $\mathcal{Q} \cap H_3$ shows that $c = 1$, hence $P_3 \in E$, contradiction.
The next case $P_2 = (0, 1, 1, \mathbf{0}), P_1 = (1, 1, a, b), P_3 = (1, c, 1, d)$ leads to a contradiction in a completely analogous way.
We are in the generic case

$$P_1 = (1, 1, a_1, b_1), P_2 = (1, a_2, a_2, b_2), P_3 = (1, c, 1, d).$$

Assume $\sum_{i=1}^{3} \lambda_i P_i = 0$. Recall that none of a_1, a_2, c equals 1. The first three coordinates yield $c(a_1 + a_2) = a_1 a_2 + 1$. We can choose $\lambda_3 = 1$. Then $\lambda_1 = (c+1)/(a_1+1), \lambda_2 = (c+a_1)/(a_1+1)$.
Assume $a_1 = a_2$. Then $a_1 a_2 + 1 = 0$. It follows $a_1 = a_2 = 1$, contradiction. It follows

$$c = (a_1 a_2 + 1)/(a_1 + a_2)$$

and consequently

$$c + 1 = (a_1 + 1)(a_2 + 1)/(a_1 + a_2), c + a_1 = (a_1 + 1)^2/(a_1 + a_2).$$

Assume $d = 0$. Then $(b_1/b_2) = (c + a_1)/(c + 1)$. Raising to power $q + 1$ yields $a_1/a_2 = (c + a_1)^2/(c + 1)^2 = (a_1^2 + 1)/(a_2^2 + 1)$. Solving this yields $(a_1 + a_2)(1 + a_1 a_2) = 0$. This shows $c = 0$, contradiction.
Assume now $c = 0$. We have $a_1 a_2 = 1, d^{q+1} = 1$. The last coordinates show $(a_1 + 1)d = b_1 + a_1 b_2$. It follows

$$a_1^2 + 1 = (a_1/b_1 + a_1 a_2/b_2)(b_1 + a_1 b_2) = x + a_1^2/x,$$

where $x = b_1/b_2$. After multiplication by x and reordering we obtain $0 = x^2 + (a_1^2 + 1)x + a_1^2 = (x + 1)(x + a_1^2)$. Case $x = 1$ leads to the contradiction $a_1 = a_2$. We must have $x = (b_1/b_2) = a_1^2$. Raising this to power $q + 1$ we obtain $a_1/a_2 = a_1^4$, or $1 = a_2 a_1^3 = a_1^2$, and hence the contradiction $a_1 = 1$.
Only one case remains: $c = \alpha, d^{q+1} = \alpha^2$. The last coordinates show $(a_1 + a_2)d = (a_2 + 1)b_1 + (a_1 + 1)b_2$. Raise this to power $q + 1$ and simplify. We obtain

$$1 + a_1^2 a_2^2 = ((a_2 + 1)a_1/b_1 + (a_1 + 1)a_2/b_2)((a_2 + 1)b_1 + (a_1 + 1)b_2) =$$

$$= a_1(1 + a_2^2) + a_2(1 + a_1^2) + a_1(a_1 + 1)(a_2 + 1)b_2/b_1 + a_2(a_1 + 1)(a_2 + 1)b_1/b_2.$$

After reordering we obtain $(a_1 + 1)(a_2 + 1)$ as a common factor. Removal of this nonzero factor leaves us with $a_1 a_2 + 1 = a_1/x + a_2 x$, where $x = b_1/b_2$. After multiplation with x this equation factors: $(x + a_1)(x + 1/a_2) = 0$. It follows that either $x = a_1$ or $x = 1/a_2$. In both cases we obtain $a_1 a_2 = 1$, which leads to the contradiction $c = \alpha = 0$.■
In order to be complete we describe a 41-cap in $PG(4, 4)$ as well. In the terminology of Definition 1 one should replace $\mathcal{U}_2$ by $\mathcal{U}_2' = \{(0 : 1 : 0 : b) \mid b^5 = 1\}$ and the two additional points R_i by $R_1' = (1 : \omega : 1 : \mathbf{0}), R_2' = (1 : \omega^2 : 1 : \mathbf{0})$. This yields a 41-cap $\mathcal{Q}_1 \cup \mathcal{Q}_2 \cup \mathcal{U}_1 \cup \mathcal{U}_2' \cup \mathcal{R}'$ in $PG(4, 4)$. Here $I\!F_4 = \{0, 1, \omega, \omega^2\}$.

4 A new family of caps

We start from the cap $\mathcal{Q} \subset PG(4,q)$ for even $q > 4$ as described in Definition 1 and Theorem 3. It follows from [2] that $\mathcal{Q}$ is a complete cap. Let S be the plane with equation $x_4 = x_5 = 0$. Our strategy will be to take away the points of $\mathcal{Q} \cap S$ from $\mathcal{Q}$ and replace them by some other points in S.

Definition 2 *Under the assumptions of Definition 1 define*
the $(2q^2+q-1)$*-cap* $\mathcal{Q}' = \mathcal{Q} \setminus (S \cap \mathcal{Q})$. *Then* $\mathcal{Q}'$ *arises from* $\mathcal{Q}$ *by omitting the points from* $\mathcal{R}$ *and the points* $(1:1:0:\mathbf{0}), (0:0:1:\mathbf{0}), (1:0:0:\mathbf{0}), (0:1:1:\mathbf{0})$.

The following easily proved Lemma will be useful:

Lemma 2 *Exchanging the first and third coordinates induces an involutory automorphism on* $\mathcal{Q}'$.

We describe points $P \in S$, such that $\mathcal{Q}' \cup \{P\}$ is a cap.

Lemma 3 *The following points* $P \in S$ *have the property that* $\mathcal{Q}' \cup \{P\}$ *is a cap:*

1. $e_1 = (1:0:0:\mathbf{0})$ *and* $e_3 = (0:0:1:\mathbf{0})$.
2. $(1:x:1:\mathbf{0})$, *where* $x \notin \{0, 1, \alpha/(\alpha+1)\}$.
3. $(x:1:0:\mathbf{0})$ *and* $(0:1:x:\mathbf{0})$, *where* $x \notin \{0, \alpha+1, (\alpha+1)/\alpha\}$.
4. $(x:0:1:\mathbf{0})$, *where* $x \notin I\!F_2$.
5. $(u:v:w:\mathbf{0})$, *where* $uvw \neq 0, u+v+w = 0$.

Proof: Observe that none of the points in the statement of the Lemma is in E. Let l be a line containing P and at least two points of $\mathcal{Q}'$. Assume l is contained in one of the $H_i, i = 1, 2, 3$. The existence of $\mathcal{Q}$ and the automorphism described in Lemma 2 show that this is not the case. It follows that l must pick up its points $Q_1, Q_2 \in \mathcal{Q}'$ from two different H_i. Cases 1. and 2. are done because of the description of $\mathcal{Q}$.
3. Without restriction $P = (x:1:0:\mathbf{0})$, where $x \notin \{0, 1, \alpha+1, (\alpha+1)/\alpha\}$.

Assume first $Q_1 \in H_1, Q_2 \in H_2$. This shows that a matrix $\begin{pmatrix} x & 1 & 1 \\ 1 & 1 & a_2 \\ 0 & a_1 & a_2 \\ \mathbf{0} & b_1 & b_2 \end{pmatrix}$ is singular, where $b_i^{q+1} = a_i$ and $a_i \notin I\!F_2$. Add x times the second row to the first row. In the resulting matrix, there is only one nonzero entry in the first column. We consider the second and third columns, where the entries in the second row have been removed. These vectors must be scalar multiples of each other. We will write $s \sim s'$ to denote that vector s' is a scalar multiple of s. In our case we obtain $(x+1, a_1, b_1) \sim (a_2x+1, a_2, b_2)$. The last coordinates show $(a_1/b_1) = (a_2/b_2)$, hence $b_1^q = b_2^q$ and consequently $b_1 = b_2, a_1 = a_2$. The first coordinate shows $x + 1 = xa_1 + 1$. We obtain the contradiction $a_1 = 1$.
We will use a similar procedure in all cases. Assume next $Q_1 \in H_1, Q_2 \in H_3$. Our singular matrix is $\begin{pmatrix} x & 1 & 1 \\ 1 & 1 & c \\ 0 & a_1 & 1 \\ \mathbf{0} & b_1 & d \end{pmatrix}$. We obtain $(x+1, a_1, b_1) \sim (cx+1, 1, d)$. As $a_1 \neq 0$ we have $b_1 \neq 0$, consequently $d \neq 0$. The description of $\mathcal{Q}' \cap S \setminus E$ shows that we must have $d^{q+1} = \alpha^2, c = \alpha$. The last coordinates show $b_1 = a_1 d$, hence $a_1 = a_1^2\alpha^2$ and $a_1 = 1/\alpha^2$. The first coordinate shows, after solving for x, that $x = (\alpha + 1)/\alpha$.
Let finally $Q_1 \in H_2, Q_2 \in H_3$. Our matrix is $\begin{pmatrix} x & 1 & 1 \\ 1 & a & c \\ 0 & a & 1 \\ \mathbf{0} & b & d \end{pmatrix}$, leading to $(ax + 1, a, b) \sim (cx + 1, 1, d)$. We have $c = \alpha, d^{q+1} = \alpha^2$. As before we obtain $a = 1/\alpha^2$. The first coordinate yields $(\alpha x+1)/(x/\alpha^2+1) = \alpha^2$, which leads to the contradiction $x = \alpha + 1$. By symmetry we are done with 3.
4. We have $P = (x, 0, 1, \mathbf{0})$. Assume first $Q_1 \in H_1, Q_2 \in H_2$. This shows that a matrix $\begin{pmatrix} x & 1 & 1 \\ 0 & 1 & a_2 \\ 1 & a_1 & a_2 \\ \mathbf{0} & b_1 & b_2 \end{pmatrix}$ is singular, as usual. It follows $(a_1x+1, 1, b_1) \sim (a_2x+1, a_2, b_2)$. The last coordinates show $b_2 = a_2b_1$, hence $a_2 = a_2^2a_1$ and consequently $a_1a_2 = 1$. The first coordinate yields $a_2x+1 = a_2(a_1x+1) = x+a_2$. This leads to the contradiction $x = 1$.
Because of the symmetry given in Lemma 2 the only case that remains to be

considered is $Q_1 \in H_1, Q_2 \in H_3$. Our singular matrix is $\begin{pmatrix} x & 1 & 1 \\ 0 & 1 & c \\ 1 & a_1 & 1 \\ \mathbf{0} & b_1 & d \end{pmatrix}$. We obtain $(a_1x + 1, 1, b_1) \sim (x + 1, c, d)$. In particular $c \neq 0$, hence $c = \alpha$. The last coordinates yield $d = \alpha b_1$, hence $\alpha^2 = \alpha^2 a_1$ and $a_1 = 1$, contradiction.
5. We can choose notation such that $P = (1 : v : w : \mathbf{0})$, where $v + w = 1, vw \neq 0$. Assume first $Q_1 \in H_1, Q_2 \in H_2$. The singular matrix is matrix $\begin{pmatrix} 1 & 1 & 1 \\ v & 1 & a_2 \\ w & a_1 & a_2 \\ \mathbf{0} & b_1 & b_2 \end{pmatrix}$. Replace the third row by the sum of the first three rows, then add v times the first row to the second. This leads to $(v + 1, a_1, b_1) \sim (v + a_2, 1, b_2)$. When the usual procedure is applied to the later coordinates be obtain $b_1 = a_1 b_2$, hence $a_1 = a_1^2 a_2$ and $a_1 a_2 = 1$. The first coordinate gives $v + 1 = a_1(v + a_2) = a_1 v + 1$. We obtain the contradiction $a_1 = 1$.
By symmetry it suffices to consider one remaining case: $Q_1 \in H_1, Q_2 \in H_3$. Our singular matrix is $\begin{pmatrix} 1 & 1 & 1 \\ v & 1 & c \\ w & a_1 & 1 \\ \mathbf{0} & b_1 & d \end{pmatrix}$. The same procedure as in the preceding case leads to $(v + 1, a_1, b_1) \sim (v + c, c, d)$. As $c \neq 0$ we have $c = \alpha$. The last two coordinate sections show $(d/b_1) = (c/a_1)$, hence $\alpha^2/a_1 = \alpha^2/a_1^2$ and thus $a_1 = 1$, contradiction.■
Denote by $\mathcal{P}$ the set of points given in Lemma 3. If $\mathcal{D} \subseteq \mathcal{P}$ is an arc in the projective plane S, then $\mathcal{Q}' \cup \mathcal{D}$ is a cap. In order to obtain a large arc $\mathcal{D}$ we use quadratic forms. Recall from geometric algebra that the quadratic form

$$Q(X_1, X_2, X_3) = a_1X_1^2 + a_2X_2^2 + a_3X_2^2 + a_{12}X_1X_2 + a_{13}X_1X_3 + a_{23}X_2X_3$$

is non-degenerate if and only if

$$a_1a_{23}^2 + a_2a_{13}^2 + a_3a_{12}^2 + a_{12} \cdot a_{13} \cdot a_{23} \neq 0.$$

If this is satisfied, then its singular points form an oval. Together with its nucleus $(a_{23} : a_{13} : a_{12})$ a hyperoval is obtained ($q + 2$ points, no three on a line). We choose some $a \in \mathbb{F}_q^*$ and consider

$$Q(x, y, z) = x^2 + ay^2 + z^2 + axy + (a + 1/a)xz + ayz.$$

This will be non-degenerate if and only $a \notin \mathbb{F}_2$. Observe that interchanging the first and third coordinates is an automorphism of Q. The nucleus is $N = (a : a + 1/a : a) = (a^2 : a^2 + 1 : a^2)$. We have $N \in \mathcal{P}$ if and only if $(a^2 + 1)/a^2 \neq \alpha/(\alpha + 1)$, which is equivalent to $a \neq \sqrt{\alpha} + 1$.
The following are points in $V(Q) \cap \mathcal{P}$:

$$(a : 0 : 1), (1 : 0, a), (a : a + 1 : 1), (1 : a + 1 : a).$$

We have $(1 : 1 + 1/a : 1) = (a : a + 1 : a) \in V(Q)$. It is in $\mathcal{P}$ if and only if $1 + 1/a \neq \alpha/(\alpha + 1)$, equivalently $a \neq \alpha + 1$. We have $(1 : y : 0) \in V(Q)$ if and only if $y^2 + y + 1/a = 0$. We assume therefore $tr(1/a) = 0$ and choose b such that $b^2 + b = 1/a$. We conclude that

$$(1 : b : 0), (1 : b + 1 : 0), (0 : b : 1) \text{ and } (0 : b + 1 : 1)$$

belong to $V(Q)$. Assume $(1 : b : 0) = (1/b : 1 : 0) \notin \mathcal{P}$. Then $1/b = \alpha + 1$ or $1/b = (\alpha + 1)/\alpha$, equivalently $b = 1/(\alpha + 1)$ or $b = \alpha/(\alpha + 1)$. It follows $1/a = b^2+b = \alpha/(\alpha^2+1)$. The remaining three points give the same condition, of course. We have seen the following:

Theorem 4 *Let $q > 4$ be a power of 2. Choose $z \in \mathbb{F}_q \setminus \mathbb{F}_4$, put $\alpha = 1/\sqrt{1 + z + 1/z}$. Let further $a \in \mathbb{F}_q \setminus \mathbb{F}_2$ such that $tr(1/a) = 0$. Here $tr : \mathbb{F}_q \longrightarrow \mathbb{F}_2$ is the absolute trace. Write $1/a = b^2 + b$. Moreover a has to be chosen different from $\alpha + 1, \sqrt{\alpha} + 1$ and $\alpha + 1/\alpha$. Then the set*

$$\mathcal{D} = \{(a : 0 : 1), (1 : 0 : a), (a : a + 1 : a), (a : a + 1 : 1), (1 : a + 1 : a),$$

$$(1 : b : 0), (1 : b + 1 : 0), (0 : b : 1), (0 : b + 1 : 1), (a^2 : a^2 + 1 : a^2)\}$$

is a 10-arc in $PG(2, q)$. If we embed this plane in $PG(4, q)$ such that $x_4 = x_5 = 0$, then $\mathcal{D}$ complements the cap $\mathcal{Q}'$ from Definition 2 to a $(2q^2 + q + 9)$-cap.

The conditions on α and a can always be satisfied. In fact, let α be chosen, $q = 2^f$. There are at least $2^{f-1} - 2$ elements $a \notin \mathbb{F}_2$ such that $tr(1/a) = 0$. As a has to satisfy only three more conditions and $2^{f-1} - 5 > 0$ if $f \geq 4$ we are done in these cases. Remains case $q = 8$. We describe $\mathbb{F}_8$ as an extension of $\mathbb{F}_2$ by $\mathbb{F}_8 = \mathbb{F}_2(\epsilon)$, where

$$1 + \epsilon + \epsilon^5 = 1 + \epsilon^2 + \epsilon^3 = 1 + \epsilon^4 + \epsilon^6 = 0.$$

Choose $z = \epsilon$, hence $\alpha = 1/\sqrt{1 + z + 1/z} = \epsilon^2$. We have $\sqrt{\alpha}+1 = \epsilon^5, \alpha+1 = \epsilon^3, \alpha + 1/\alpha = \epsilon^4$. As $tr(\epsilon) = 1, tr(\epsilon^3) = 0$, we can choose $a = \epsilon^2 = \alpha$. This concludes the proof of Theorem 1.

References

[1] J.W.P. Hirschfeld, L.Storme: *The packing problem in statistics, coding theory and finite projective spaces,* to appear in *Journal of Statistical Planning and Inference.*

[2] G.Tallini: *Calotte complete di $S_{4,q}$ contenenti due quadriche ellittiche quali sezioni iperpiane, Rend.Mat e Appl.* **23** (1964),108-123.