A class of k-caps having $k-2$ points in common with an elliptic quadric and two points on an external line

Fernanda Pambianco and Emanuela Ughi*

Dipartimento di Matematica, Università degli Studi di Perugia
Via Vanvitelli 1, 06123 Perugia (Italy)
e-mail: fernanda@dipmat.unipg.it, ughi@dipmat.unipg.it

Abstract

The main problem on caps, posed originally by Segre in the fifties, is to determine the values of k for which there exists a complete k-cap. In the present paper, we construct in $PG(3,q)$, for odd prime q, a family of $\frac{1}{2}(q^2+7)$-caps which have 2 points on a line external to an elliptic quadric E and the remaining points on E. We conjecture that they are complete.

1 Introduction

The general aim is to construct, for small enough k, complete k-caps, having $k-2$ points in common with a quadric and 2 points in common with an external line l. We refer to [4], [6], [7], [5], [1] and [2] for detailed information on caps and earlier results obtained in this direction.

In [3], a class of complete $k-$caps was obtained in the case of q being an odd prime, and the line l being a tangent to an elliptic quadric; in [8] and [9], the construction was modified to all cases with q odd. These papers provided the impetus to the investigation of the following problem: find constructions of complete caps, based on geometrical configurations which are the possible intersections of a line with an elliptic quadric. In the present paper, we consider the case of the line being external. More precisely, we construct $\frac{1}{2}(q^2+7)$-caps in $PG(3,q)$, q an odd prime, which have two points on a line external to an elliptic quadric and the remaining points on the quadric. We conjecture that they are complete.

*Research supported by Italian M.U.R.S.T. and by G.N.S.A.G.A. (C.N.R.).

2 Construction

Let E be an irreducible elliptic quadric of $PG(3,q)$, q an odd prime. Without loss of generality, the equation of E may be taken as

$$x_1^2 - \alpha x_2^2 + x_3^2 - 2x_0x_3 = 0,$$

where α is a non-square element of $GF(q)$. Consider the points $P = (0,1,0,0)$ and $Q = (0,0,1,0)$. The line PQ has equations $x_0 = x_3 = 0$, and is external to E . Of the $q+1$ planes of the pencil on PQ,

$$\{x_0 = kx_3 : \ k \in GF(q)\} \cup \{x_3 = 0\},$$

two are tangents to E at the points of E given by $\pi_P \cap \pi_Q \cap E$, where π_P and π_Q are the polar planes of P and Q, respectively. Thus, the points of contact are $T = (1,0,0,0)$ and $T_1 = (\frac{1}{2}(q+1),0,0,1)$, and the two tangent planes τ and τ' are given by,

$$\tau : \ x_3 = 0 \qquad \text{and} \qquad \tau' : \ x_0 = \frac{q+1}{2}x_3,$$

respectively. Let the plane π_k , with equation $x_0 = kx_3$, $k \in GF(q)\backslash\{\frac{1}{2}(q+1)\}$, intersect E in the conic C_k, then

$$C_k = \left\{(k, \sqrt{\alpha x_2^2 + 2k - 1}, x_2, 1) : \ x_2 \in U\right\},$$

where U is the set of those values of $GF(q)$ for which $\alpha x_2^2 + 2k - 1$ is a square.

Given $\bar{x}_2 \in U$, write $u^2 = \alpha\bar{x}_2^2 + 2k - 1$. The following set of four points of C_k are then uniquely determined:

$$\begin{aligned} A_1 &= (k, u, \bar{x}_2, 1) \\ A_2 &= (k, -u, \bar{x}_2, 1) \\ A_3 &= (k, u, -\bar{x}_2, 1) \\ A_4 &= (k, -u, -\bar{x}_2, 1). \end{aligned}$$

From each such set, select two points as follows:
If $\bar{x}_2 \in H_1 = \{1, ..., \frac{1}{2}(q-1)\}$, select from $\{A_1, A_2\}$ the point whose second coordinate belongs to H_1, and select from $\{A_3, A_4\}$ the one whose second coordinate belongs to $H_2 = \{\frac{1}{2}(q+1), ..., q-1\}$.
If $\bar{x}_2 \in H_2$, select from $\{A_1, A_2\}$ the point whose second coordinate belongs to H_2, and from $\{A_3, A_4\}$ the point whose second coordinate belongs to H_1.

Let A denote the set of points so selected.

For a given $\bar{x}_2 \neq 0$, the expression,

$$\alpha\bar{x}_2^2 + 2k - 1,$$

(i) is equal to $\alpha\bar{x}_2^2$ if $k = \frac{1}{2}(q+1)$, and hence is a non-square

and

(*ii*) assumes all the values of $GF(q)$ as k varies in $GF(q)$.

In particular, for appropriate values of $k \in GF(q)\setminus\{\frac{1}{2}(q+1)\}$, all the squares of $GF(q)$ can be obtained from this expression.

We now prove that $|\mathsf{A}| = \frac{1}{2}(q-1)^2$.

For a given $\bar{x}_2 \neq 0$, there correspond $\frac{1}{2}(q-1)$ squares of type $\alpha\bar{x}_2^2 + 2k - 1$, and each such square gives rise to 2 points of A, of type $(k, \bar{x}_1, \bar{x}_2, 1)$ and $(k, -\bar{x}_1, -\bar{x}_2, 1)$. Thus, A has

$$\left(\frac{q-1}{2} \cdot 2\right) \cdot \frac{q-1}{2} = \frac{1}{2}(q-1)^2$$

points.

Define a set B of points of the quadric E by:

$$\mathsf{B} = \left\{(k, 0, \bar{x}_2, 1) : \bar{x}_2 \in H_1, \quad \alpha\bar{x}_2^2 + 2k - 1 = 0\right\}.$$

Thus $|\mathsf{B}| = |H_1| = \frac{1}{2}(q-1)$.

As k varies in $GF(q)$, $(2k-1)$ assumes all the values of $GF(q)$; in particular, all the squares of $GF(q)$ can be written as $2k-1$ for an appropriate k. Define the set C by:

$$\mathsf{C} = \left\{(k, \sqrt{2k-1}, 0, 1)\right\},$$

where $2k-1$ is a square and $\sqrt{2k-1}$ belongs to H_1. Thus, $|\mathsf{C}| = \frac{1}{2}(q-1)$.

Theorem 1 *The set K of points defined by*

$$K = \mathsf{A} \cup \mathsf{B} \cup \mathsf{C} \cup \{T, T_1, P, Q\}$$

is a $\frac{1}{2}(q^2+7)$−cap .

Proof. By construction, K has $\frac{1}{2}(q^2+7)$ points. Also, apart from the points P, Q, all the other points of K are points of E. Since the line PQ does not intersect E, we need only prove that no pair of points of $K\setminus\{P, Q\}$ are collinear with P or with Q. Now PT, PT_1, QT, QT_1 being tangent lines to E, have no further point in common with K.

Any line l_1 through P, not in the planes τ and τ', has equations of type

$$x_0 = kx_3 \quad \text{and} \quad x_2 = \bar{x}_2 x_3.$$

Such a line l_1 intersects E in the points

$$(k, \sqrt{\alpha\bar{x}_2^2 + 2k - 1}, \bar{x}_2, 1) \quad \text{and} \quad (k, -\sqrt{\alpha\bar{x}_2^2 + 2k - 1}, \bar{x}_2, 1).$$

Only one of these two points lies in K.

Similarly, no line through Q can intersect K in two points.

□

In the case $q = 3$, the construction yields

$$\begin{array}{lll} \mathsf{A} = \{(0,1,1,1),\ (0,2,2,1)\}, & & \\ \mathsf{B} = \{(1,0,1,1)\}, & P = (0,1,0,0), & T = (1,0,0,0), \\ \mathsf{C} = \{(1,1,0,1)\}, & Q = (0,0,1,0),, & T_1 = (2,0,0,1). \end{array}$$

Direct calculation shows that this 8−cap of $PG(3,3)$ is complete and it is projectively equivalent to the 8-cap furnished in [5]. Further, it can be observed that in this case:

(i) each of the planes $x_2 = 0$ and $x_2 = x_3$ intersect K in 4 points, which constitute an irreducible conic, and hence form a complete arc, and

(ii) the plane $x_2 = 2x_3$ intersect K in three points, namely P, T, and $(0,2,2,1)$; these three points constitute an incomplete $q-$arc.

The above observations suggest the following question:

For what values of $q \geq 5$ is the $k-$cap K such that

(I) *the points lying in the plane $x_2 = \lambda x_3,\ \lambda \in H_1 \cup \{0\}$, constitute a complete arc, and*

(II) *the points lying in the plane $x_2 = \lambda x_3,\ \lambda \in H_2$, form a $q-$arc?*

As shall be explained at the end of this paper, we conjecture that (I) and (II) are satisfied for $q \geq 19$; for $q \leq 19$, (I) is satisfied only for $q = 7, 13, 17$.

3 Completeness

We determine a condition that ensures that the $\frac{1}{2}(q^2+7)-$cap K is complete.

We say that a point A of $PG(3,q)$ is saturated by K if there exists at least one 2-secant of K through A. Thus, K is complete, if and only if, all the points of the planes on PT are saturated by K.

Of the planes on PT, τ is tangent to E, and the others are secant to E and have equations of type $x_2 = \lambda x_3,\ \lambda \in GF(q)$. In τ, there are three points of K, namely P, Q, and T. The points of K in the plane $x_2 = \bar{\lambda} x_3$, with $\bar{\lambda} \neq 0$, are of type

$$(f(x_1, \bar{\lambda}), x_1, \bar{\lambda}, 1),$$

where,

(i) if $\bar{\lambda} \in H_1$, these points are contained in $\mathsf{A} \cup \mathsf{B}$ and $x_1 \in H_1 \cup \{0\}$.

(ii) if $\bar{\lambda} \in H_2$, these points are contained in A and $x_1 \in H_2$.

If $\bar{\lambda} = 0$, the points of K in the plane $x_2 = 0$, other than P and T, are those of the set $\mathsf{C} \cup \{T_1\}$.

Consider $\pi_{\bar{\lambda}}$, a secant plane of equation,

$$x_2 = \bar{\lambda} x_3\ , \qquad \bar{\lambda} \in H_1 \cup \{0\}\ .$$

Such a plane is saturated if all of its lines through T are saturated. Clearly, the line TP, being a 2-secant of K is saturated by K. The other lines, m_τ, in the plane $\pi_{\bar{\lambda}}$, through T, have equations,

$$x_2 = \bar{\lambda} x_3, \qquad x_1 = \tau x_3 \qquad (\tau \in GF(Q)).$$

If $\tau \in H_1 \cup \{0\}$, each such line is, by the construction of K, saturated by K.

We need to investigate the lines m_τ for which $\tau \in H_2$. Let the points of K with $x_3 \neq 0$ be,

$$\left\{(x_0(\lambda,l),l,\lambda,1):\ x_0(\lambda,l)=\frac{l^2+1-\alpha\lambda^2}{2}\right\}.$$

The secant lines of K which meet a line m_τ, $\bar{\lambda} \in H_1 \cup \{0\}$, $\tau \in H_2$ can be divided into four subsets as follows:

(1) 2-secants of K through P in the plane $\pi_{\bar{\lambda}}$. These have equations

$$x_2 = \bar{\lambda}x_3\,, \qquad x_0 = \tfrac{1}{2}(l^2+1-\alpha\bar{\lambda}^2)x_3 \qquad l \in H_1 \cup \{0\}\,;$$

(2) lines joining two points of K, distinct from P and T, lying in $\pi_{\bar{\lambda}}$. If two such points are $(\frac{1}{2}(1+l_1^2-\alpha\bar{\lambda}^2), l_1, \bar{\lambda}, 1)$ and $(\frac{1}{2}(1+l_2^2-\alpha\bar{\lambda}^2), l_2, \bar{\lambda}, 1)$, then the line joining them has equations

$$x_2 = \bar{\lambda}x_3\,, \qquad x_0 = \frac{1-l_1l_2+\tau(l_1+l_2)-\alpha\bar{\lambda}^2}{2}x_3\,.$$

(3) lines joining $Q=(0,0,1,0)$ and a point of K of type

$$\left(\frac{l^2+1-\alpha\lambda^2}{2}, l, \lambda, 1\right).$$

These lines have equations

$$x_1 = lx_3\,, \qquad x_0 = \frac{l^2+1-\alpha\lambda^2}{2}x_3\,.$$

Such a line intersects m_τ iff $l=\tau$. In such a case, it follows that $\lambda \in H_2$.

(4) lines in the plane $x_1 = \tau x_3$, joining two points of K, other than Q or T. Since $\tau \in H_2$, it follows that $\lambda \in H_2$. These lines join points of K of type $(\frac{1}{2}(1+\tau^2-\alpha\beta_1^2), \tau, \beta_1, 1)$ and $(\frac{1}{2}(1+\tau^2-\alpha\beta_2^2), \tau, \beta_2, 1)$ with $\beta_1 \neq \beta_2$. Hence their equations are of type

$$x_1 = \tau x_3, \qquad x_0 = \frac{1+\tau^2+\alpha\beta_1\beta_2}{2}x_3 - \frac{\alpha(\beta_1+\beta_2)}{2}x_2\,.$$

One such line meets the plane $x_2 = \bar{\lambda}x_3$ in the point with coordinates,

$$\left(\frac{1+\tau^2+\alpha\beta_1\beta_2}{2} - \frac{\alpha(\beta_1+\beta_2)\bar{\lambda}}{2}, \tau, \bar{\lambda}, 1\right).$$

We note that the q points of m_τ, distinct from T, are given by,

$$(x_0, \tau, \bar{\lambda}, 1)\,, \qquad x_0 \in GF(q).$$

To prove that the points of m_τ are saturated by K, it suffices to show that the first coordinates of the points of intersection of m_τ and the lines of the above-mentioned four subsets cover $GF(q)$. This needs to be shown for all $\bar{\lambda} \in H_1 \cup \{0\}$, $\forall \tau \in H_2$. In other words, saturation of points of m_τ requires that the following *condition A* be satisfied:

Condition A:

$\forall \tau \in H_2$, $\forall \lambda \in H_1 \cup \{0\}$,

$$GF(q) = \{\tfrac{1}{2}(l^2+1-\alpha\lambda^2) : \ l \in H_1 \cup \{0\}\}$$
$$\cup \{\tfrac{1}{2}(1-l_1l_2+\tau(l_1+l_2)-\alpha\lambda^2) : \ l_i \in H_1 \cup \{0\}, \ \ l_1 \neq l_2\}$$
$$\cup \{\tfrac{1}{2}(\tau^2+1-\alpha\delta^2) : \ \delta \in H_2\}$$
$$\cup \{\tfrac{1}{2}(1+\tau^2+\alpha\beta_1\beta_2-\alpha(\beta_1+\beta_2)\lambda) : \ \beta_i \in H_2, \ \ \beta_1 \neq \beta_2\}.$$

Similarly, consider the plane π_λ, with $\lambda \in H_2$.
Saturation of points of these planes by K requires *condition B* be satisfied:
Condition B:
$\forall \tau \in H_1 \cup \{0\}, \forall \lambda \in H_2$,

$$GF(q) = \{\tfrac{1}{2}(l^2+1-\alpha\lambda^2) : \ l \in H_2\}$$
$$\cup \{\tfrac{1}{2}(1-l_1l_2+\tau(l_1+l_2)-\alpha\lambda^2) : \ l_i \in H_2, \ \ l_1 \neq l_2\}$$
$$\cup \{\tfrac{1}{2}(\tau^2+1-\alpha\delta^2) : \ \delta \in H_1 \cup \{0\}\}$$
$$\cup \{\tfrac{1}{2}(1+\tau^2+\alpha\beta_1\beta_2-\alpha(\beta_1+\beta_2)\lambda) : \ \beta_i \in H_1 \cup \{0\}, \ \ \beta_1 \neq \beta_2\}.$$

As for the plane τ, the points on the sides of triangle PQT are saturated by K. The remaining points of τ have coordinates of type $(x_0, x_1, 1, 0)$, $x_i \in GF(q)^*$. Such a point is saturated by K if it is collinear with two points of K, of type $(\frac{1}{2}(1+m^2-\alpha\gamma^2)$, $m, \gamma, 1)$ and $(\frac{1}{2}(1+n^2-\alpha\delta^2)$, $n, \delta, 1)$, with $m \neq n$, $\gamma \neq \delta$, and each pair (m, γ) and (n, δ) belonging to $\{H_1 \cup \{0\}\} \times \{H_1 \cup \{0\}\}$ or to $H_2 \times H_2$. It is easy to verify that collinearity of these three points is equivalent to

$$\begin{aligned} \delta &= \gamma + (n-m)/x_1, \\ \gamma &= (-2x_0x_1 + n(x_1^2-\alpha) + m(x_1^2+\alpha))/(2\alpha x_1) \ . \end{aligned} \tag{1}$$

Therefore, a sufficient condition for saturation of the points of the plane τ by K is *Condition C*:

$\forall \ x_0, x_1 \in GF(q)$, $\exists$ two pairs (m, γ) and (n, δ) with $m \neq n$ and $\gamma \neq \delta$ each pair belonging to $\{H_1 \cup \{0\}\} \times \{H_1 \cup \{0\}\}$ or to $H_2 \times H_2$ and such that the above relations (1) hold between $x_0, x_1, m, n, \delta, \gamma$.

We have established the following theorem:

Theorem 2 *If q is prime, α a non-square of $GF(q)$, and if conditions A, B, and C are satisfied, then the $\frac{1}{2}(q^2+7)$−cap K is complete.*

With the help of a computer, it was verified that *conditions A, B, C, are satisfied for* $q = 7$ and $13 \leq q < 931$.

The following was also verified.

Proposition 3 *For q prime, with $19 \leq q < 931$, and α a non-square of $GF(q)$, the following conditions are satisfied:*

(I) *Condition A'*:
$\forall \tau \in H_2, \forall \lambda \in H_1 \cup \{0\}$

$$GF(q) = \{\tfrac{1}{2}(l^2+1-\alpha\lambda^2) : \ l \in H_1 \cup \{0\}\}$$
$$\cup \{\tfrac{1}{2}(1-l_1l_2+\tau(l_1+l_2)-\alpha\lambda^2) : \ l_i \in H_1 \cup \{0\}, \ \ l_1 \neq l_2\} \ ;$$

(II) *Condition* B' :
$\forall \tau \in H_1 \cup \{0\}$, $\forall \lambda \in H_2$

$$GF(q) = \left\{\tfrac{1}{2}(l^2 + 1 - \alpha\lambda^2) : l \in H_2\right\} \cup \left\{\tfrac{1}{2}(1 - l_1 l_2 + \tau(l_1 + l_2) - \alpha\lambda^2) : l_i \in H_2,\ \ l_1 \neq l_2\right\} \cup \left\{\tfrac{1}{2}(1-\alpha)\right\} ;$$

(III) *Condition C.*

We conjecture that this proposition is true for all q.

Remark As λ varies, the situation described by *Condition A* is that of the completeness of the arc obtained as the intersection of K and the relevant plane. The situation described by *Condition B,* is that of an incomplete arc L obtained as the intersection of K and a plane π, where L can be made complete by the adjunction of a unique point S of π, but S can be shown to be saturated by K. Thus, the conjecture can be formulated in the following simpler fashion.

Conjecture 4 *For prime q, $q \geq 19$, α a non-square in $GF(q)$ the following conditions are satisfied*

(I) *Condition* A'' :
$\forall \tau \in H_2$,

$$GF(q) = \left\{\tfrac{1}{2}(l^2 + 1) : l \in H_1 \cup \{0\}\right\} \cup \left\{\tfrac{1}{2}(1 - l_1 l_2 + \tau(l_1 + l_2)) : l_i \in H_1 \cup \{0\},\ \ l_1 \neq l_2\right\} ;$$

(II) *Condition* B'' :
$\forall \tau \in H_1 \cup \{0\}$,

$$GF(q) = \left\{\tfrac{1}{2}(l^2 + 1 - \alpha) : l \in H_2\right\} \cup \left\{\tfrac{1}{2}(1 - l_1 l_2 + \tau(l_1 + l_2) - \alpha) : l_i \in H_2,\ \ l_1 \neq l_2\right\} \cup \left\{\tfrac{1}{2}(1-\alpha)\right\} ;$$

(III) *Condition C.*

As $x \longmapsto x - \frac{\alpha}{2}$ is a bijection of $GF(q)$, *Condition* B'' does not depend on α and can be rewritten as

Condition $\widetilde{B''}$
$\forall \tau \in H_1 \cup \{0\}$,

$$GF(q) = \left\{\tfrac{1}{2}(l^2 + 1) : l \in H_2\right\} \cup \left\{\tfrac{1}{2}(1 - l_1 l_2 + \tau(l_1 + l_2)) : l_i \in H_2,\ \ l_1 \neq l_2\right\} \cup \left\{\tfrac{1}{2}\right\} .$$

We cannot prove conjecture 4, although numerical evidence seems to support it. That is, we are not able to prove the completeness of the arc, however, we can prove that the points not covered by secants of the arc are "few" in the following sense: if we carry out the above construction in $PG(3,q)$, then, as q increases,

$$\lim_{q\to\infty} \frac{\#\text{ points not covered by the arc}}{\#\text{ points of the space}} = 0.$$

This will follow from Propositions 5 and 7.

Let q be an odd prime, $q > 19$. Let τ a fixed value of H_2.

Let

$$X_\tau = \left\{ \frac{1}{2}(l^2+1) : l \in H_1 \cup \{0\} \right\}$$
$$\cup \left\{ \frac{1}{2}(1 - l_1 l_2 + \tau\,(l_1 + l_2)) : l_i \in H_1 \cup \{0\},\ i = 1,2,\ l_1 \neq l_2 \right\}.$$

Proposition 5

$$|GF(q)\backslash X_\tau| < f(q),$$

where $f(q) = (\log_2 q + 1)\,(\log_2 q + 2) + \frac{1}{2}(\sqrt{q}+1)\log_2 q + \frac{1}{2}\sqrt{q} + \frac{3}{2}$.

We observe that $f(q)$ is asymptotic to $\frac{1}{2}\sqrt{q}\log_2 q$, in the sense that

$$\lim_{q\to\infty} \frac{f(q)}{\frac{1}{2}\sqrt{q}\log_2 q} = 1\,.$$

Proof. We prove the proposition by finding a set E such that

1) $|E| \leq f(q)$, and
2) $GF(q)\backslash X_\tau \subseteq E$.

Write $\rho = [\log_2 q]$, so, $\log_2 q \leq \rho < \log_2 q + 1$. We observe that if $q \geq 19$ we have $\rho < (q-1)2$.

Consider the following set of polynomials

$$\begin{aligned} f_1(x) &= 4(\tau^2 - 2x + 1) + 1 \\ f_2(x) &= 4(\tau^2 - 2x + 1) + 4 \\ &\vdots \\ f_\rho(x) &= 4(\tau^2 - 2x + 1) + \rho^2. \end{aligned}$$

Let S be the set of values $t \in GF(q)$, such that $f_i(x)$ is a non-square for every $i = 1, ..., \rho$. We can obtain information about the cardinality of S since the $f_i(x)$ are linear in x and distinct, thus satisfying the hypothesis of the following lemma due to Szonyi [10].

Lemma 6 *Let $f_1(t), ..., f_m(t) \in GF(q)[t]$ be given polynomials. Suppose that no partial product $f_{i_1}(t)...f_{i_j}(t), (1 \le i_1 < i_2 < ... < i_j,\ j \le m)$, can be written as a constant multiple of a square of a polynomial. If*

$$2^{m-1} \sum_{i=1}^{m} \deg(f_i) \le \sqrt{q} - 1$$

then there is a $t_0 \in GF(q)$ such that $f_i(t_0)$ is a non-square for every $i = 1, ..., m$. More precisely, if we denote the number of these t_0 by N, then

$$\left| N - \frac{q}{2^m} \right| \le \sum_{i=1}^{m} \frac{1}{2} \deg(f_i)(\sqrt{q} + 1).$$

We deduce that

$$\begin{aligned} |S| &\le \frac{q}{2^\rho} + \sum \deg(f_i) \frac{\sqrt{q}+1}{2} \\ &\le 1 + (\log_2 q + 1) \frac{\sqrt{q}+1}{2} = 1 + \frac{\sqrt{q}+1}{2} \log_2 q + \frac{\sqrt{q}+1}{2} \\ &= \frac{3}{2} + \frac{\sqrt{q}+1}{2} \log_2 q + \frac{\sqrt{q}}{2}. \end{aligned}$$

Let

$$\begin{aligned} T &= \{(1,0), (1,1), ..., (1,\rho-1), (2,0), ..., (2,\rho-2), ..., (\rho,0)\} \\ &= \{(j,l), j \ge 1, l \ge 0, j + l \le \rho\}. \end{aligned}$$

Let

$U = \left\{\frac{1}{2}(1 + \tau(l-j) + lj) : (j,l) \in T\right\}$ and

$V = \left\{\frac{1}{2}(1 + \tau\left(\frac{1}{2} - j\right) + \left(\frac{1}{2} + l\right)\left[\tau - \left(\frac{1}{2} - j\right)\right]) : (j,l) \in T\right\}$.

It follows that

$|T| = 1 + 2 + ... + \rho = \frac{1}{2}\rho(\rho+1)$,

$|U| \le |T|$

$|V| \le |T|$.

Let $E = S \cup U \cup V$.

Now, let $x \in GF(q)$. To show that $x \in X_\tau$, it is sufficient to find two distinct elements l_1, l_2 of $\mathrm{H}_1 \cup \{0\}$, such that,

$$x = \frac{1 - l_1 l_2 + \tau(l_1 + l_2)}{2},$$

or, equivalently

$$l_2 = \frac{2x - 1 - \tau l_1}{\tau - l_1},$$

where $\tau \ne l_1$, since $\tau \in H_2$ and $l_1 \in \mathrm{H}_1 \cup \{0\}$.

Let f be the bijective function

$$f : GF(q)\setminus\{\tau\} \to GF(q)\setminus\{\tau\}\ ,$$

defined by

$$u \longmapsto \frac{2x-1-\tau u}{\tau-u}.$$

We are looking for an element $l_1 \in H_1 \cup \{0\}$ such that $f(l_1) \in H_1 \cup \{0\}$, $f(l_1) \neq l_1$. If such an element l_1 exists, then the pair $(l_1, f(l_1))$ proves that $x \in X_\tau$.

Write $\delta = \tau - l_1$. Then we have

$$f(\tau-\delta) = \tau - \frac{\tau^2-2x+1}{\delta}.$$

It is easy to show that f has at most 2 fixed points. Let F denote the set of fixed points of f.

Now, suppose that x $\notin X_\tau$. Then x must be such that the function f, when restricted to $H = H_1 \cup \{0\}\setminus F$, induces a bijection between H and its image $f(H)$, and $f(H) \subseteq (H_2\setminus\{\tau\})$. Since

$$|H_1 \cup \{0\}| = \frac{q-1}{2} + 1, \text{ and}$$

$$|H_2\setminus\{\tau\}| = \frac{q-1}{2} - 1,$$

it is clear that, as $x \notin X_\tau$, f necessarily has two fixed points P_1 and P_2, each in $H_1 \cup \{0\}$. So f gives a bijection,

$$f\ : H_1 \cup \{0\}\setminus\{P_1, P_2\}) \ \to H_2\setminus\{\tau\}$$

Now, suppose that $x \notin S$, so that there exists an integer l, with $1 \leq l \leq \rho$, such that $4(\tau^2-2x+1)+l^2$ is a square or 0 in $GF(q)$. Therefore there is at least one solution, y_1, of the equation

$$f(y) = y + l\,.$$

Thus, $y_1 \in GF(q)\setminus\{\tau, P_1, P_2\}$.
If $y_1 \in H_1 \cup \{0\}\setminus\{P_1, P_2\}$, then $f(y_1) \in H_2\setminus\{\tau\}$, so

$$y_1 = -j \in \left\{\frac{q+1}{2} - 1, ..., \frac{q+1}{2} - l\right\}.$$

If $y_1 \in H_2\setminus\{\tau\}$, then $f(y_1) \in H_1 \cup \{0\}$, so

$$y_1 = -j \in \{-1, -2, ..., -l\}\,.$$

In the first case, at least one of the following conditions is satisfied

$f(\frac{q+1}{2}-1) \in \left\{\frac{q+1}{2}, \frac{q+1}{2}+1, .., \frac{q+1}{2}+\rho-1\right\}$
$f(\frac{q+1}{2}-2) \in \left\{\frac{q+1}{2}, \frac{q+1}{2}+1, .., \frac{q+1}{2}+\rho-2\right\}$
$\vdots$
$f(\frac{q+1}{2}-\rho) \in \left\{\frac{q+1}{2}\right\}$

while in the second case, at least one of the following conditions is satisfied

$f(-1) \in \{0, 1, .., \rho-1\}$
$f(-2) \in \{0, 1, .., \rho-2\}$
$\vdots$
$f(-\rho) \in \{0\}$.

A simple calculation shows that, if $f(-j) = l$, with $(j, l) \in T$ then x$\in U$, while if $f(\frac{q+1}{2}-j) = \frac{q+1}{2}+l$, with $(j, l) \in T$ then x $\in V$.

The proof of Proposition 5 now follows easily.

□

Now, let $\tau \in H_1 \cup \{0\}$ and

$Y_\tau = \left\{\frac{1}{2}(l^2+1) : l \in H_2\right\} \cup \left\{\frac{1}{2}(1 - l_1 l_2 + \tau(l_1 + l_2)) : l_i \in H_2,\ l_1 \neq l_2\right\} \cup \left\{\frac{1}{2}\right\}$.

In an analogous way, we can prove:

Proposition 7

$$|GF(q)\backslash Y_\tau| \leq (\log_2 q + 1)(\log_2 q + 2) + \frac{\sqrt{q}+1}{2}\log_2 q + \frac{\sqrt{q}}{2} + \frac{3}{2}.$$

References

[1] Faina G.: *Complete caps having less than $(q^2+1)/2$ points in common with an elliptic quadric of $PG(3, q)$.* Rend. Mat. Appl. **8** (1988), 277-281.

[2] Faina G.: *Complete k-caps* in $PG(3, q)$ *with* $k < (q^2+q+4)/2$. Ars Combinatoria **33** (1992), 311-317

[3] Faina G. and Pambianco F.: *A class of complete k-caps in $PG(3, q)$ for q an odd prime.* Journal of Geometry **57** (1996), 93-105.

[4] Faina G. and Pambianco F.: *On the spectrum of the values k for which a complete k-cap in $PG(n, q)$ exists.* Journal of Geometry **62** (1998), 84-98.

[5] Hirschfeld J.W.P.: *Finite Projective Spaces of three Dimensions,* Oxford University Press, Oxford 1985.

[6] Hirschfeld J.W.P and Storme L.: *The packing problem in statistics, coding theory and finite projective spaces,* to appear in the Proceedings of the Bose Memorial Conference (Colorado, June 7-11, 1995), J. Stat. Plann. Infer.

[7] Hirschfeld J.W.P and Thas J.A.: *General Galois Geometries*, Oxford University Press, Oxford (1991).

[8] Pambianco F.: *A class of complete k-caps of small cardinality in projective spaces over fields of characteristic three.* To appear in Discrete Mathematics.

[9] Pambianco F.: *A class of complete k-caps of small cardinality in* $PG(3,q)$ *for* $q = p^h$, $p \neq 3$ prime odd. Preprint.

[10] Szonyi T.: *Note on the existence of large minimal blocking sets in Galois planes,* Combinatorica, **12** (1992), 227-235.

(Received 19/4/99)