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

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

July 15, 2002

Abstract

We construct caps in projective 4-space $PG(4, q)$ in odd characteristic, whose cardinality is $O(\frac{5}{2}q^2)$.

Key words

Caps, Galois geometries, codes, quadratic forms, ovals, ovoids, Hasse-Weil bound.

AMS classification

51E22, 94B05.

1 Introduction

Let $PG(r, q)$ be the projective space of dimension r over the Galois field $\mathbb{F}_q = GF(q)$ of order q. An n-cap $\mathcal{O}$ in $PG(r, q)$ is a set of n points, no three of which are collinear. The maximum value of n for which there exists an n-cap in $PG(r, q)$ is denoted by $m_2(r, q)$ (see [4]). The number $m_2(r, q)$ is only known, for arbitrary q, when $r = 2$ and $r = 3$. To be precise $m_2(2, q) = q + 1$ if q is odd, $m_2(2, q) = q + 2$ if q is even and $m_2(3, q) = q^2 + 1, q > 2$. Caps in $PG(3, q)$ of size $q^2 + 1$ are called **ovoids.** Apart from $m_2(r, 2) = 2^r$, $m_2(4, 3) = 20$, $m_2(5, 3) = 56$ [4, p.285], and $m_2(4, 4) = 41$ [2], for $m_2(r, q)$

only upper bounds are known. It seems that finding the exact value $m_2(r, q)$ for $r \geq 4$ and constructing a cap of size $m_2(r, q)$ are very hard problems.

We study large caps in dimension 4. In [1] we improved a construction due to Tallini and constructed $(2q^2+q+9)$-caps in $PG(4, q)$ for all $q = 2^f > 4$. In this paper we construct large caps in $PG(4, q)$ in odd characteristic. Segre claimed in [6] to have constructed caps of size $(5q^2 - 2q + 1)/2$ in $PG(4, q)$ whenever $q = p^f$, where the prime $p \equiv 7 \pmod 8$ and the exponent f is odd. Segre's construction is not quite correct as it is stated in [6]; to see this, consider for example the collinear points $P_1 = (0, 1, 1, 1, 1, 0), P_2 = (0, 1, 1, -1, 0)$ and $P_3 = (0, -2, -2, 0, 0)$ in the terminology of [6, p.90], in the case when 3 is a non-square. However, his method does produce large caps. We start from a version of Segre's construction, which works for all odd q. This is done in Section 2 for $q \equiv 3 \pmod 4$, and in Section 3 for $q \equiv 1 \pmod 4$. Denote the resulting caps by $\mathcal{C}_q \subset PG(4, q)$. We proceed to show that there is a plane E meeting $\mathcal{C}_q$ in 4 points and a conic section $\mathcal{A} \subset E$ such that $\mathcal{A} \cap \mathcal{C}_q = \emptyset$ and

$$\mathcal{C}_q^* = (\mathcal{C}_q \setminus E) \cup \mathcal{A}$$

is a cap. It is clear that $\mathcal{C}_q^*$ has $q - 3$ points more than $\mathcal{C}_q$. This construction is carried through in Section 4 for $q \equiv 3 \pmod 4$ and in Section 5 for $q \equiv 1 \pmod 4$. The proof in case $q \equiv 1 \pmod 4$ uses a technical lemma (Lemma 1). In Section 6 we give a proof of this lemma. It is based on the Hasse-Weil bound for the number of rational points for algebraic curves. Our main result is as follows.

Theorem 1 *Let q be an odd prime-power. Then $PG(4, q)$ contains a cap $\mathcal{C}_q^*$ of the following cardinality:*

$$\begin{array}{ll} (5q^2 - 2q - 7)/2 & \text{if } q \equiv 1 \pmod 8, \\ (5q^2 - 8q - 13)/2 & \text{if } 3 < q \equiv 3 \pmod 8, \\ (5q^2 - 6q - 11)/2 & \text{if } q \equiv 5 \pmod 8, \\ (5q^2 - 4q - 9)/2 & \text{if } q \equiv 7 \pmod 8. \end{array}$$

It follows from one of the by-laws of quadratic reciprocity (see for example [7]) that 2 is a square if $q \equiv \pm 1 \pmod 8$ and 2 is a nonsquare if $q \equiv \pm 3 \pmod 8$.

We use homogeneous coordinates for $PG(4, q)$. A typical point will be written as $x = (x_1 : x_2 : x_3 : x_4 : x_5)$. Denote by e_i the vector which has $x_i = 1, x_j = 0$ for $j \neq i$. We wish to thank A. Brandis for a helpful discussion.

2 The construction in the case $q \equiv 3 \pmod 4$

In the projective space $PG(4, q)$ consider the hyperplanes H_1 with equation $x_3 = 0, H_2$ with equation $x_4 = 0, H_3$ with equation $x_5 = 0$ and quadrics $Q_i, i = 1, 2, 3$ with the following equations:

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

Observe that the bilinear form (scalar product) corresponding to Q_1 is

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

and analogously for Q_2 and Q_3. The radicals of the quadrics Q_i are

$$\mathrm{Rad}(Q_1) = \langle e_3\rangle,\ \mathrm{Rad}(Q_2) = \langle e_4\rangle,\ \mathrm{Rad}(Q_3) = \langle e_5\rangle.$$

In particular, the restriction of Q_i to H_i is non-degenerate. It follows that $V(Q_i) \cap H_i$, the set of projective points $P \in H_i$ satisfying $Q_i(P) = 0$, is a non-degenerate quadric. The discriminant is -1 in each case, meaning that the Gram matrix has nonsquare determinant. This shows that $V(Q_i) \cap H_i$ has index 1; geometrically, this means that it is an ovoid. The 2-space $\langle e_1, e_2\rangle$ is anisotropic with respect to each Q_i, or equivalently the line corresponding to $\langle e_1, e_2\rangle$ is an exterior line of $V(Q_i)$. Another equivalent expression is: $V(Q_i) \cap H_1 \cap H_2 \cap H_3 = \emptyset$. Call a line l **generic** if it is not contained in any of the H_i, in other words if $l \cap H_i$ consists of one point $P_i, i = 1, 2, 3$. We construct a large subset $U \subset V(Q_3) \cap H_3$ such that no generic line meets $V(Q_1) \cup V(Q_2) \cup U$ in three points.

So let l be a generic line and let $P_i = l \cap H_i, i = 1, 2, 3$. Assume $P_i \in V(Q_i)$. Write $P_i = \langle v_i\rangle$, where notation is chosen such that $v_1 + v_2 + v_3 = 0$. We have

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

As $x + y + z = 0$ we have the following relations:

$$\begin{gathered} z_1 = -(x_1 + y_1), \quad z_2 = -(x_2 + y_2) \\ z_3 = -y_3, \quad z_4 = -x_4, \quad y_5 = -x_5. \end{gathered}$$

Since $P_i \in V(Q_i), i = 1, 2, 3$ we have that $Q_i(v_i) = 0$. Consider the equation $2Q_1(x) + 2Q_2(y) - Q_3(z) = 0$; taking into account the above relations, we obtain

$$(x_1 - y_1)^2 = -(x_2 - y_2)^2.$$

As -1 is a non-square we obtain $x_1 = y_1$ and $x_2 = y_2$. The relation $Q_1(x) - Q_2(y) = 0$ reads as follows:

$$z_3^2 + z_4^2 = 2x_5^2. \tag{1}$$

We have that $V(Q_i) \cap H_i \cap H_j$ is an oval whenever $i \neq j$. Also, these 6 ovals are mutually disjoint. We see that $U_i = (V(Q_i) \cap H_i) \setminus (H_j \cup H_k)$ has $q^2 + 1 - 2(q + 1) = q^2 - 2q - 1$ elements whenever $\{i, j, k\} = \{1, 2, 3\}$.

Put $Q(z_3, z_4) = z_3^2 + z_4^2$. Define

$$U = \{P = (z_1 : z_2 : z_3 : z_4 : 0) \mid P \in V(Q_3), z_3 \cdot z_4 \neq 0, 2Q(z_3, z_4) \text{ non-square in } \mathbb{F}_q\}.$$

If $P = \langle z\rangle \in U$, then equation (1) cannot be satisfied. It follows that $\mathcal{C}_q = U_1 \cup U_2 \cup U$ is a cap.

We have to show that $|U| \geq (q+1)^2/2$ if 2 is a square, and that $|U| \geq (q+1)(q-3)/2$ if 2 is a non-square. For each non-zero square $u \in \mathbb{F}_q$ there are precisely two pairs $(z_3, 0)$ such that $Q(z_3, 0) = u$ and also two pairs $(0, z_4)$ such that $Q(0, z_4) = u$. Non-squares u have no such representation. Define $E = \{(z_3, z_4) \mid z_3 z_4 \neq 0, z_3^2 - z_4^2 = 0\}$. Then $|E| = 2(q-1)$ and it is clear that $P = \langle z \rangle \notin U$ if $(z_3, z_4) \in E$. Moreover for each non-zero element $u \in \mathbb{F}_q$ with the same Legendre symbol as 2 there are precisely 4 pairs $(z_3, z_4) \in E$ such that $Q(z_3, z_4) = u$. An element u whose Legendre symbol is different from that of 2 has no such representation.

Now, let $(z_3, z_4) \in M = (\mathbb{F}_q^* \times \mathbb{F}_q^*) \setminus E$. We have $|M| = (q-1)(q-3)$. As the quadratic form Q is anisotropic it represents each non-zero field element by $q+1$ pairs. Consider at first the case when 2 is a square. The number of pairs $(z_3, z_4) \in M$ such that $Q(z_3, z_4)$ is non-square is $\frac{q-1}{2} \cdot (q+1)$. As $z_3^2 - z_4^2 \neq 0$ for these pairs, there are precisely $q+1$ pairs (z_1, z_2) such that for $z = (z_1, z_2, z_3, z_4, 0)$ we have $Q_3(z) = 0$. This holds for each fixed such pair (z_3, z_4). Hence we have

$$|U| = (q+1) \cdot \frac{q-1}{2} \cdot (q+1)/(q-1) = (q+1)^2/2.$$

Now, let 2 be a non-square. The number of pairs $(z_3, z_4) \in M$ such that $Q(z_3, z_4)$ is square equals $\frac{q-1}{2} \cdot (q+1-4)$. Proceeding as in the former case we conclude that

$$|U| = (q+1) \cdot \frac{q-1}{2} \cdot (q-3)/(q-1) = (q+1)(q-3)/2.$$

3 The construction in the case $q \equiv 1 \pmod 4$

The general build-up is the same as in the case $q \equiv 3 \pmod 4$. We choose a non-square α and use the following quadrics:

$$\begin{aligned} Q_1(x) &= x_1^2 + \alpha x_2^2 + x_4^2 + x_5^2, \\ Q_2(x) &= x_1^2 + \alpha x_2^2 - x_3^2 - x_5^2, \\ Q_3(x) &= x_1^2 + \alpha x_2^2 - 2x_3^2 + 2x_4^2. \end{aligned}$$

As before we see that $V(Q_i) \cap H_i$ describes an ovoid, $i = 1, 2, 3$ and that $\langle e_1, e_2 \rangle$ is anisotropic with respect to each Q_i. Assume a generic line l intersects H_i in P_i, where $P_i \in V(Q_i), i = 1, 2, 3$. Write $P_i = \langle v_i \rangle$, where notation is chosen such that $v_1 + v_2 + v_3 = 0$. We have

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

and the same relations hold as in case $q \equiv 1 \pmod 4$:

$$z_1 = -(x_1 + y_1), \quad z_2 = -(x_2 + y_2),$$
$$z_3 = -y_3, \quad z_4 = -x_4, \quad y_5 = -x_5.$$

As before we use $2Q_1(x) + 2Q_2(y) - Q_3(z) = 0$. This yields

$$(x_1 - y_1)^2 = -\alpha(x_2 - y_2)^2.$$

As $-\alpha$ is a non-square we obtain $x_1 = y_1$ and $x_2 = y_2$.

The relation $Q_1(x) - Q_2(y) = 0$ yields

$$z_3^2 + z_4^2 = -2x_5^2. \tag{2}$$

As before, put $Q(z_3, z_4) = z_3^2 + z_4^2$. This time Q does not describe an anisotropic space but rather a hyperbolic plane. Each non-zero value is represented precisely $q - 1$ times by Q. Put

$$U = \{P = (z_1 : z_2 : z_3 : z_4 : 0) \mid P \in V(Q_3), z_3 \cdot z_4 \neq 0, \\ Q(z_3, z_4) = 0 \text{ or } 2Q(z_3, z_4) \text{ non-square in } I\!\!F_q\}.$$

If $P = \langle z \rangle \in U$, then equation (2) cannot be satisfied. It follows that $\mathcal{C}_q = U_1 \cup U_2 \cup U$ is a cap, where U_1 and U_2 are defined as before. We have that $V(Q_i) \cap H_i \cap H_j$ is an oval whenever $i \neq j$. Moreover these 6 ovals are mutually disjoint. It follows that U_i has $q^2 + 1 - 2(q + 1) = q^2 - 2q - 1$ elements. The number of $P \in U$ such that $Q(z_3, z_4) = 0$ is $2(q - 1)(q + 1)/(q - 1) = 2(q + 1)$. For every non-zero $u \in I\!\!F_q$, which has the same Legendre symbol as 2, there are 4 pairs (z_3, z_4) such that $z_3 z_4 \neq 0, z_3^2 = z_4^2$ and $Q(z_3, z_4) = u$. For each non-zero square u there are 4 pairs $(z_3, z_4) \neq (0, 0)$ such that $z_3 z_4 = 0$ and $Q(z_3, z_4) = u$.

We distinguish between the cases when 2 is a square and when 2 is a non-square. Using the same counting argument as in the preceding section we get in the former case (2 a square)

$$|U| = 2(q + 1) + (q + 1) \cdot \frac{q - 1}{2} \cdot (q - 1)/(q - 1) = (q^2 + 4q + 3)/2.$$

When 2 is non-square we obtain

$$|U| = 2(q + 1) + (q + 1) \cdot \frac{q - 1}{2} \cdot (q - 5)/(q - 1) = (q^2 - 1)/2.$$

4 The extension in the case $q \equiv 3 \pmod 4$

Consider the plane $E = (x_1 = x_2 = 0)$ and the conic section $\mathcal{A} = V(Q_4) \subset E$, where

$$Q_4(x) = x_3^2 + x_4^2 + ax_5^2,$$

and $a \in I\!\!F_q$ is chosen such that a and $2a + 1$ are non-zero squares. $\mathcal{C}_q \cap E$ consists of the four points $(0 : 0 : 0 : 1 : \pm 1)$ and $(0 : 0 : 1 : 0 : \pm 1)$. We have to prove that $\mathcal{C}_q^* = (\mathcal{C}_q \setminus E) \cup \mathcal{A}$ is a cap. As $\mathcal{A}$ is an oval in E it suffices to prove that there is no line l containing a point $W = \langle w \rangle = (0 : 0 : w_3 : w_4 : w_5) \in \mathcal{A}$ and two points P_1, P_2 of $\mathcal{C}_q \setminus E$. Two essentially different cases arise.

The first case

$P_1 = \langle x\rangle \in U_1 \setminus E, P_2 = \langle y\rangle \in U_2 \setminus E$. We have

$$\begin{aligned} x &= (x_1, x_2, 0, x_4, x_5), \\ y &= (y_1, y_2, y_3, 0, y_5), \\ w &= (0, 0, w_3, w_4, w_5), \end{aligned}$$

where $Q_1(x) = Q_2(y) = Q_4(w) = 0$ and notation has been chosen such that $x + y + w = 0$. It follows from $Q_1(x) - Q_2(y) = 0$ that

$$w_3^2 + w_4^2 = x_5^2 + y_5^2. \tag{3}$$

The equation $Q_4(w) = 0$ yields

$$w_3^2 + w_4^2 = -aw_5^2 = -a(x_5^2 + 2x_5y_5 + y_5^2). \tag{4}$$

Subtracting equation (4) from equation (3) we obtain

$$(a + 1)x_5^2 + 2ax_5y_5 + (a + 1)y_5^2 = 0.$$

We see that x_5/y_5 is a solution of the quadratic equation $X^2 + \frac{2a}{a+1}X + 1 = 0$. The discriminant of this equation is $-(2a + 1)/(a + 1)^2$. As this is a non-square we obtain a contradiction.

The second case

$P_1 = \langle x\rangle \in U_1 \setminus E, P_2 = \langle z\rangle \in U \setminus E$. We have

$$\begin{aligned} x &= (x_1, x_2, 0, x_4, x_5), \\ z &= (z_1, z_2, z_3, z_4, 0), \\ w &= (0, 0, w_3, w_4, w_5), \end{aligned}$$

where $Q_1(x) = Q_3(z) = Q_4(w) = 0$ and notation has been chosen such that $x + z + w = 0$. The additional property that $2(z_3^2 + z_4^2)$ is a non-square will not be needed.

Equation $Q_1(x) = Q_3(z)$ yields

$$-2w_3^2 - x_4^2 + 2z_4^2 + w_5^2 = 0.$$

Equation $Q_4(w) = 0$ yields

$$w_3^2 + w_4^2 + aw_5^2 = w_3^2 + x_4^2 + 2x_4z_4 + z_4^2 + aw_5^2 = 0.$$

Consider the equation $Q_1(x) - Q_3(z) + 2Q_4(w) = 0$. Putting $Y = x_4/z_4$ we obtain

$$(Y + 2)^2 + (2a + 1)(w_5/z_4)^2.$$

It follows that $2a + 1$ is a non-square, contradicting our choice.

The third case $P_1 \in U_2 \setminus E, P_2 \in U_2 \setminus E$ is obtained from the second case using the involutorial automorphism, which interchanges the third and fourth coordinates.

In order to complete the proof in this case it suffices to show that we can always find a non-zero square $a \in \mathbb{F}_q$ such that $2a + 1$ is a non-zero square. If the characteristic is not 3 we can choose $a = 4$. Let the characteristic be 3, $q > 3$. Let $a \neq 1$ be a square. We have $2a + 1 = 1 - a \neq 0$. If $1 - a$ is a square we are done. Assume $1 - a$ is a non-square. Put $a' = 1/a$. Then $1 - a' = (a - 1)/a$ is a square and we are done.

5 The extension in the case $q \equiv 1 \pmod 4$

In this section we will assume $q > 9$. Cases $q = 5$ and $q = 9$ will be dealt with in Section 7. Consider the plane $E = (x_1 = x_2 = 0)$ and the conic section $\mathcal{A} = V(Q_4) \subset E$, where

$$Q_4(x) = x_3^2 + x_4^2 + bx_5^2 + 2cx_3x_4.$$

Here the non-zero elements b, c are chosen such that c is a square, $1 - c^2$ is a non-square, $b = (1 \pm c)/2$ is a non-square. The proof that such a choice is possible for $q > 9$ can be found in Section 6. The set $\mathcal{C}_q \cap E$ consists of the four points $(0 : 0 : 0 : 1 : \pm i)$ and $(0 : 0 : 1 : 0 : \pm i)$, where i denotes an element of order 4. We have to prove that $\mathcal{C}_q^* = (\mathcal{C}_q \setminus E) \cup \mathcal{A}$ is a cap. As before it suffices to prove that there is no line l containing a point $W =< w >= (0 : 0 : w_3 : w_4 : w_5) \in \mathcal{A}$ and two points P_1, P_2 of $\mathcal{C}_q \setminus E$. As in the preceding section we have to consider two essentially different cases.

The first case

$P_1 = \langle x \rangle \in U_1 \setminus E, P_2 = \langle y \rangle \in U_2 \setminus E$. We have

$$\begin{aligned} x &= (x_1, x_2, 0, x_4, x_5), \\ y &= (y_1, y_2, y_3, 0, y_5), \\ w &= (0, 0, w_3, w_4, w_5), \end{aligned}$$

where $Q_1(x) = Q_2(y) = Q_4(w) = 0$ and $x + y + w = 0$. Equation $-2b(Q_1(x) - Q_2(y)) + Q_4(w) = 0$ simplifies as follows:

$$(1 - 2b)(w_3^2 + w_4^2) - b(x_5 - y_5)^2 + 2cw_3w_4 = 0.$$

Using $1-2b = \pm c$ we obtain $\pm c(w_3 \pm w_4)^2 = b(x_5 - y_5)^2$. As bc is a non-square we conclude $x_5 = y_5$ and $w_3 = \pm w_4$. Equation $(Q_1(x) + Q_2(y))/2$ yields $x_1^2 + ax_2^2 = 0$, which forces $x_1 = x_2 = 0$ contradicting the assumption that $x \notin E$.

The second case

$P_1 = \langle x \rangle \in U_1 \setminus E, P_2 = \langle z \rangle \in U \setminus E$. We have

$$\begin{aligned} x &= (x_1, x_2, 0, x_4, x_5), \\ z &= (z_1, z_2, z_3, z_4, 0), \\ w &= (0, 0, w_3, w_4, w_5), \end{aligned}$$

where $Q_1(x) = Q_3(z) = Q_4(w) = 0$ and $x+z+w = 0$. Equation $b(Q_1(x)-Q_3(z))-Q_4(w) = 0$ reads as follows:

$$(2b - 1)w_3^2 + (b - 1)w_4^2 - bz_4^2 + 2bw_4z_4 - 2cw_3w_4 = 0.$$

Recall that $b = \frac{1}{2}(1 \pm c)$. Consider the case when $b = \frac{1}{2}(1+c)$. Then $b-1 = \frac{1}{2}(c-1), 2b-1 = c$ and our equation simplifies as follows:

$$c(w_3 - w_4)^2 = \frac{1}{2}(c + 1)(z_4 - w_4)^2 = b(z_4 - w_4)^2.$$

As bc is non-square we conclude $w_3 = w_4 = z_4 = -z_3$. Equation $Q_3(z) = 0$ yields the contradiction $z_1 = z_2 = 0$.

Consider the case when $b = \frac{1}{2}(1-c)$. Then $b - 1 = -\frac{1}{2}(c+1), 2b - 1 = -c$. Our equation simplifies as follows:

$$-c(w_3 + w_4)^2 = \frac{1}{2}(1-c)(z_4 - w_4)^2 = b(z_4 - w_4)^2.$$

As before we conclude $w_4 = z_4 = -w_3 = z_3$. Equation $Q_3(z) = 0$ yields the contradiction $z_1 = z_2 = 0$.

6 A lemma concerning finite fields

Recall the conditions that $b, c \in I\!F_q$ have to satisfy in Section 5: both are non-zero, c a square, $1 - c^2$ non-square, $b = \frac{1}{2}(1 \pm c)$ and b non-square. Assume the square c has been chosen such that $1 - c^2$ is non-square. As the product $\frac{1}{2}(1+c) \cdot \frac{1}{2}(1-c)$ is a non-square it is clear that we are done once the following Lemma is proved:

Lemma 1 *Let q be a prime-power, $q \equiv 1 (mod\ 4), q > 9$. Then there is an element $x \in I\!F_q$ such that $1 - x^4$ is non-square.*

Proof: Assume this is not the case. Consider the homogeneous polynomial

$$F(X, Y, Z) = X^4 + Y^2 Z^2 - Z^4$$

with coefficients in $I\!F_q$. Denote by N the number of its rational points. The only rational point with $z = 0$ is $P_\infty = (0 : 1 : 0)$. The remaining rational points will be written in the form $(x : y : 1)$. If $y = 0$, then $x \in \langle i \rangle$. If $x = 0$, then $y = \pm 1$. Let $x \notin \{0, \pm 1, \pm i\}$. By our assumption $1 - x^4$ is a square. It follows that each such x gives us 2 rational points all of whose coefficients are non-zero. We have seen that $N = 1 + 4 + 2 + 2(q-5) = 2q - 3$. On the other hand the polynomial $F(X, Y, Z)$ of degree 4 determines an algebraic curve of genus $g \leq 3$. As P_∞ is a singular point we have $g \leq 2$. It is not difficult to determine the genus completely. In fact, it follows from [8], Example VI.3.3, that we are in the elliptic case $g = 1$. From the Hasse-Weil formula we have that $N \leq q + 1 + 2\sqrt{q}$ (see [8], for example). We have $2q - 3 \leq q + 1 + 2\sqrt{q}$, equivalently $q \leq 4 + 2\sqrt{q}$, which is not true for $q \geq 13$. □

It may be noted that the statement of Lemma 1 is indeed not true for $q = 5$ and $q = 9$.

7 Small fields

The method of Section 5 works for $q = 5$ and for $q = 9$ as well. The only change is that the constants b, c in the definition of the quadratic form Q_4 have to be chosen in a different way. As the case $q = 5$ is not very interesting we leave it for the reader to check that the choice $b = c = 1$ leads to the desired result. We work out the case $q = 9$. Represent $I\!F_9$

in the form $\mathbb{F}_9 = \mathbb{F}_3(\epsilon)$, where the primitive element ϵ satisfies $\epsilon^2 = -\epsilon + 1$. We choose $b = 1, c = \epsilon$.

In the first case the equation $Q_1(x) - Q_2(y) = 0$ yields

$$w_3^2 + w_4^2 + x_5^2 + y_5^2 = 0.$$

Comparison with $Q_4(w) = 0$ shows that $\frac{x_5 y_5}{w_3 w_4} = \epsilon$. It is easy to show that if the sum of four nonzero squares vanishes in $\mathbb{F}_9$, then the product of these squares is ± 1. This yields a contradiction.

In case 2 we proceed as in Section 5. Consider the equations $Q_1(x) - Q_3(z)$ and $Q_4(w)$. We simplify, divide all the terms by w_4^2 and use the new variables $X = w_3/w_4, Y = z_4/w_4$ and $Z = w_5/w_4$. This leads to the equations

$$\begin{aligned} X^2 - \epsilon X &= Y^2 + Y, \\ X^2 - 1 - Y &= Z^2. \end{aligned}$$

The first of the above equations has only five solutions (x, y), namely either $(x, y) = (\epsilon, -1)$ or $x \in \{-1, -\epsilon^3\}, y \in \{-\epsilon, -\epsilon^2\}$. In each of these cases the second equation cannot be satisfied as $x^2 - 1 - y$ is a non-square. This contradiction concludes the proof.

References

[1] Y. Edel and J. Bierbrauer: *A family of caps in projective* 4*-space in characteristic* 2, manuscript.

[2] Y. Edel and J. Bierbrauer: 41 *is the largest size of a cap in* $PG(4, 4)$, *Designs, Codes and Cryptography* **59** (1999), 151–160.

[3] J.W.P. Hirschfeld and L. Storme: *The packing problem in statistics, coding theory and finite projective spaces, Journal of Statistical Planning and Inference* **72** (1998), 355–380.

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

[5] G. Tallini: *Calotte complete di* $S_{4,q}$ *contenenti due quadriche ellittiche quali sezioni iperpiane, Rendiconti di Matematica Pura ed Applicata* **23** (1964), 108–123.

[6] B. Segre: *Le geometrie di Galois, Annali di Matematica Pura ed Applicata* **48** (1959), 1–97.

[7] J.P. Serre: *Cours d'Arithmétique, Presses Universitaires de France, Paris 1970.*

[8] H. Stichtenoth: *Algebraic Function Fields and Codes, Springer Verlag, Berlin 1993.*