Caps on Classical Varieties and their Projections

Jürgen Bierbrauer, Antonio Cossidente† and Yves Edel

A family of caps constructed by G. L. Ebert, K. Metsch and T. Szonyi [8] results from projecting a Veronesean or a Grassmannian to a suitable lower-dimensional space. We improve on this construction by projecting to a space of much smaller dimension. More precisely, we partition \( PG(3r - 1, q) \) into a \((2r - 1)\)-space, an \((r - 1)\)-space and \(q' - 1\) cyclic caps, each of size \((q^{2r} - 1)/(q - 1)\). We also decide when one of our caps can be extended by a point from the \((2r - 1)\)-space or the \((r - 1)\)-space.

The proof of the results uses several ingredients, most notably hyperelliptic curves.

© 2001 Academic Press

1. INTRODUCTION

Let \( PG(N, q) \) be the projective space of dimension \( N \) over the finite field \( GF(q) \). A \( k \)-cap \( K \) in \( PG(N, q) \) is a set of \( k \) points, no three of which are collinear [14], and a \( k \)-cap is complete if it is maximal with respect to inclusion. The maximum value of \( k \) for which there exists a \( k \)-cap in \( PG(N, q) \) is denoted by \( m_2(N, q) \). The number \( m_2(N, q) \) is only known, for arbitrary \( q \), when \( N \in \{2, 3\} \); namely, \( m_2(2, q) = q + 1 \) if \( q \) is odd, \( m_2(2, q) = q + 2 \) if \( q \) is even, and \( m_2(3, q) = q^2 + 1, q > 2 \). A cap of size \( m_2(3, q) \) in \( PG(3, q) \) is called an ovoid [12]. The only known infinite classes of ovoids are the elliptic quadrics and, if \( q \) is an odd power of 2, the Suzuki–Tits ovoids [18]. Aside of these general results the precise value of \( m_2(N, q) \) is known only in the following cases: \( m_2(N, 2) = 2^N \), \( m_2(4, 3) = 20 \), \( m_2(5, 3) = 56 \) and \( m_2(4, 4) = 41 \) [9]. Finding the exact value for \( m_2(N, q) \), \( N \geq 4 \), and constructing an \( m_2(N, q) \)-cap seems to be a very hard problem [13].

A natural asymptotic problem is the determination of

\[
\mu(q) = \lim_{N \to \infty} \sup \frac{\log_q(m_2(N, q))}{N}.
\]

As a cap cannot be larger than its ambient space, clearly \( \mu(q) \leq 1 \). It is an interesting open problem to decide if \( \mu(q) < 1 \). Segre’s recursive construction [16] yields \( \mu(q) \geq 2/3 \). No better lower bound seems to be known for general \( q \). An exception is the ternary case. It follows from [2] that \( \mu(3) > \log_3(2.21) \).

An interesting method to construct caps is to study intersections of quadrics or of hermitian varieties, or in general of classical varieties such as Veronesean varieties and Segre varieties [4, 5]. In this paper we construct a class of cyclic caps in \( PG(3r - 1, q) \), \( r \geq 2 \), (i.e., caps admitting a regular action of a cyclic group of automorphisms) obtained by projecting certain caps contained in the Grassmannian of lines of \( PG(2r - 1, q) \). These caps have size \((q^{2r} - 1)/(q - 1)\) and it turns out that they are unions of Veronesean varieties. This explicitly constructed family of caps reaches the best known general lower bound \( \mu(q) \geq 2/3 \). These caps are therefore just as large as the largest known caps, in an asymptotical sense. We also study extensions of these caps.

2. SINGER CYCLES AND THEIR LIFTING

Let \( V \) be an \((n + 1)\)-dimensional vector space over the Galois field \( \mathbb{F}_q \), and let \( S \) be a Singer cycle of \( GL(V) \). It is known [15] that \( S \) is conjugate in \( GL(n + 1, q^{n+1}) \) to the diagonal

†Author to whom correspondence should be addressed.

0195-6698/01/020135 + 09 $35.00/0 © 2001 Academic Press
matrix $D = \text{diag}(\alpha, \alpha^q, \ldots, \alpha^{q^n})$, where $\alpha$ is a primitive element of $\mathbb{F}_{q^{n+1}}$. Denote by $^v : GL(V) \to PGL(V)$ the canonical epimorphism. The image of $(S)$ under $^v$ is a subgroup $\langle S \rangle \subset PGL(V)$ of order $(q^{n+1} - 1)/(q - 1)$. Let $N = n(n + 3)/2$. Denote by $V$ the Veronese variety of $PG(N, q)$, namely the Veroneseian of all quadrics of $PG(n, q)$, see [14]. It follows from [14] that $V$ is a $(q^n + q^{n-1} + \cdots + q + 1)$-cap. Moreover, since $\text{Aut}(V)$ is isomorphic to $PGL(n + 1, q)$, each linear collineation of $PG(n, q)$ can be lifted to a collineation of $PG(N, q)$ leaving $V$ invariant, see [4].

Consider the case $n = 3$. The lifting $\hat{S}$ of a Singer cycle $S$ of $GL(4, q)$ to a collineation of $PGL(10, q)$ fixes the Veronese variety $V$ of $PG(9, q)$. The collineation $\hat{S}$ is conjugate to the block diagonal matrix $\text{diag}(S^2, S^{q+1}, T)$, where $T$ is a Singer cycle of $GL(2, q)$. From a geometric point of view, this means that $\hat{S}$ induces a collineation $\psi$ of $PG(9, q)$ which fixes (setwise) two three-dimensional projective subspaces $\Sigma_1$ and $\Sigma_2$ and a line, say $\ell$. The order of $\psi$ is $q^3 + q^2 + q + 1$ and its action outside the fixed subspaces is semiregular. In particular, $\hat{S}$ fixes a five-dimensional subspace $\Sigma_3$, inducing a collineation $\epsilon$ whose matrix representation is $E = \text{diag}(S^{q+1}, T)$. It is easy to see that $E$ is exactly the exterior square $\Lambda^{(2)}(S)$ of $S$, and it fixes (by definition) the Grassmannian $G_{1,3}$ of lines of $PG(3, q)$.

The collineation $\epsilon$ has been studied in [10] and [3]. It has order $q^3 + q^2 + q + 1$, fixes a three-dimensional subspace, the subspace $\Sigma_2$, inducing a collineation of order $q^2 + 1$, whose orbits are elliptic ovoids [7], and a line (the line $\ell$). Each of the remaining orbits of $\epsilon$ on the point set of $\Sigma_3$ is a cap of size $q^3 + q^2 + q + 1$. These are the caps studied by Glynn [10]. Each such Glynn cap is the complete intersection of $G_{1,3}$ with the quadratic cone of vertex the line $\ell$ and basis an elliptic quadric in $\Sigma_2$. In particular, a Glynn cap can be projected onto an elliptic ovoid of $\Sigma_2$ from the line $\ell$. In [4], it has been proved that a Glynn cap is the projection of a Veronese variety of $PG(9, q)$.

Hence, projecting a Veronese variety $V$ of $PG(9, q)$ from a suitable 3-subspace of $PG(9, q)$ disjoint from $V$ we obtain a Glynn cap, and the Glynn cap can be further projected onto an elliptic ovoid.

In [8] the authors, using the geometry of lines of $PG(n, q)$ for arbitrary $n$, generalize Glynn’s construction to any Grassmannian of lines of $PG(n, q)$, obtaining caps of size $q^n + \cdots + q + 1$. We refer to these caps as EMS caps. It was shown in [6] that each EMS cap can in fact be obtained by projecting a suitable Veronese variety.

Unfortunately, EMS caps are very small with respect to their ambient space. We pursue the program sketched in the Introduction and give an equivariant construction by projecting EMS caps to a subspace of small dimension. The general setting is described in the following section. The proof is given in Section 4.

### 3. The General Setting

Let $S$ be a Singer cycle of $GL(2r, q)$, $r \geq 2$. Its canonical form in $GL(2r, q^{2r})$ is $D = \text{diag}(\alpha, \alpha^2, \ldots, \alpha^{q^{2r}-1})$, where $\alpha$ is a primitive element of $\mathbb{F}_{q^{2r}}$. Consider the second exterior square $\Lambda^{(2)}(D)$ of $D$. Then $\Lambda^{(2)}(D)$ is a diagonal matrix whose entries are $\alpha^t + 1$, $1 \leq t \leq r$, and its conjugates over $\mathbb{F}_q$. Note that $\alpha^t + 1$ is an element of $\mathbb{F}_q$. It follows that $\Lambda^{(2)}(S)$ has the rational canonical form $\Lambda^{(2)}(S) = \text{diag}(S^{q+1}, \ldots, S^{q^{2r}-1}, T)$, where $T$ is a Singer cycle of $GL(r, q)$. Then $\Lambda^{(2)}(S)$ induces a linear collineation $\phi$ of $PG(2r^2 - r - 1, q)$ of order $(q^{2r} - 1)/(q - 1)$, fixing the Grassmannian of lines, $G_{1,2r-1}$ of $PG(2r - 1, q)$. Also it fixes $r - 1$ subspaces $\Sigma_1, \ldots, \Sigma_{r-1}$, each of dimension $2r - 1$, and an $(r - 1)$-dimensional subspace $\pi$. Outside the fixed linear spaces (and subspaces generated by them) $\langle \phi \rangle$ acts semiregularly. This means that the orbits of $\langle \phi \rangle$ not in the fixed linear subspaces all have length $(q^{2r} -
1)/(q - 1), and in particular those contained in \( G_{1,2r-1} \) are \(((q^{2r} - 1)/(q - 1))\)-caps \([8]\) (apart from one shorter orbit if \( r - 1 \equiv 2 \) mod 3). We note that \( \phi \) also fixes \( r - 1 \) subspaces of dimension 3r - 1. We improve upon the EMS construction by showing that projection to the subspace, where the collineation group \( \phi \) has matrix representation diag\((SY^{r-1}+1, T)\), produces caps. The details are given in the next section.

4. CONSTRUCTION OF A FAMILY OF CYCLIC CAPS

Let \( F = \mathbb{F}_q^r \) and \( L = \mathbb{F}_q^r \), where \( r \geq 2 \). Consider the direct sum \( V = F \oplus L \), a 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 \( \alpha \) be a primitive element of \( F \). The action of the Singer cycle determined by \( \alpha \) lifts to \( V \) as follows:

\[
g : (a, b) \mapsto (aa^q-1+b, ba^q+1).
\]

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 \( O(a : b) \). Let \( N, T : F \rightarrow L \) 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 \( U = F^{*}q^r+1 = Z((q^{2r}-1)/(q + 1)) \).

THEOREM 1. For every \( 0 \neq a \in F \), \( 0 \neq b \in L \), the orbit \( O(a : b) \) 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 \( O(a : b) \) is not a cap. There must be three collinear points

\[(a : b), (axq^{-1}+1 : bxq^{-1}+1), (ayq^{-1}+1 : byq^{-1}+1)\]

in \( O(a : b) \). 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

\[
a\lambda_1 + a\lambda_2 xq^{-1}+1 + a\lambda_3 yq^{-1}+1 = 0,
b\lambda_1 + b\lambda_2 N(x) + b\lambda_3 N(y) = 0.
\]

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

\[
yq^{-1}+1 = \lambda_2 xq^{-1}+1 + \lambda_1,
N(y) = \lambda_2 N(x) + \lambda_1.
\]

We compute \( N(yq^{-1}+1) \) in two ways. Using the second equation we obtain

\[
N(yq^{-1}+1) = N(yq^{-1}+1) = (\lambda_2 N(x)q^{-1}+1 + \lambda_1)(\lambda_2 N(x) + \lambda_1)
= \lambda_2^2 N(x)q^{-1}+1 + \lambda_1 \lambda_2 (N(x)q^{-1}+1 + N(x) + \lambda_1^2).
\]

The first equation yields

\[
N(yq^{-1}+1) = N(\lambda_2 xq^{-1}+1 + \lambda_1) = (\lambda_2 xq^{-1}+1 + \lambda_1)(\lambda_2 xq^{-1}+1 + \lambda_1)
= \lambda_2^2 N(x)q^{-1}+1 + \lambda_1 \lambda_2 (xq^{-1}+1 + xq^{-1}+1) + \lambda_1^2.
\]
Comparing these expressions and eliminating the obvious common terms we obtain

\[ x^{q'-1}(q'+1) + x^{q'} + 1 = x^{q'}(q'-1+1) + x^{q'-1} + 1. \]

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

\[ 0 = x^{2q'-1} + q' - q' - 1 - x^{2q'-1} - x^{q'} - 1 + 1 = (x^{q'} - q') - 1(x^{2q'-1} - 1). \]

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

In the following sections we determine when a cap \( \mathcal{O}(a : b) \) can be extended by points from \( PG(L) \) or \( PG(F) \).

5. Extensions by Points from the \((r - 1)\)-Space \( PG(L) \)

**Theorem 2.** Let \( r \geq 2 \) and \( \mathcal{O}(a : b) \) be one of the cyclic \( \frac{q^{2r-1}}{q-1} \)-caps in \( PG(3r - 1, q) \) as constructed in Theorem 1. Let \( Q = (0 : d) \in PG(L) \). Then \( \mathcal{O}(a : b) \cup \{Q\} \) is a cap if and only if \( r \) is odd and \( q \) is a power of 2.

**Proof.** Assume that

\[ P_1 = (ay^{q'-1} + 1 : by^{q' + 1}) \quad \text{and} \quad P_2 = (a(xy)^{q'-1} + 1 : b(xy)^{q' + 1}) \]

are collinear with \( Q \). Let \( \lambda_1, \lambda_2, \lambda_3 \in \mathbb{F}_q \) be the coefficients of a linear combination. Here \( y, x \) are arbitrary nonzero elements of \( F \), but we want \( P_1 \neq P_2 \), equivalently \( x \not\in \mathbb{F}_q \). The first coordinate shows that \( \lambda_1 + \lambda_2 x y^{q'-1} + 1 = 0 \). We can choose \( \lambda_2 = -1 \). It follows that \( \lambda_1 = x^{q'-1} + 1 \in \mathbb{F}_q \). Let \( g = \gcd(q^{2r} - 1, q^{2r} + 1) \). Observe that \( x^{q'} = \mathbb{F}_q \). As \( q^{2r} - 1 = (q^{q'-1} + 1)(q^{q'-1} + q^2) + (q^2 - 1) \) we have \( \gcd(q^{2r} - 1, q^{2r} + 1) = \gcd(q^{q'-1} + 1, q^2 - 1) \).

Let \( r \) be odd. We have

\[ \begin{align*}
q^{q'-1} + 1 &= (q^2 - 1)(q^{q'-3} + q^{q'-5} + \cdots + 1) + 2, \\
\end{align*} \]

showing \( \gcd(q^{q'-1} + 1, q^2 - 1) = \gcd(q^2 - 1, 2) \).

Let \( r \) be even. We have

\[ \begin{align*}
q^{q'-1} + 1 &= (q^2 - 1)(q^{q'-3} + q^{q'-5} + \cdots + q) + (q + 1), \\
\end{align*} \]

hence \( \gcd(q^{q'-1} + 1, q^2 - 1) = q + 1 \) in this case. This shows the following lemma.

**Lemma 1.**

\[ g = \gcd(q^{2r} - 1, q^{q'-1} + 1) = \begin{cases} 
q + 1 & \text{if } r \text{ is even} \\
1 & \text{if } r \text{ is odd, } q \text{ is even} \\
2 & \text{if } r \text{ and } q \text{ are odd}. 
\end{cases} \]

Let \( r \) be odd and \( q \) even. We have \( g = 1 \), hence \( x \in \mathbb{F}_q \) and \( P_1 = P_2 \), a contradiction. This shows that each \( Q \in PG(L) \) yields an extension cap.

Let \( r \) and \( q \) both be odd. We have \( x^2 \in \mathbb{F}_q \). It follows that \( x \in \mathbb{F}_q \). As \( x^{q'} = x \) it follows that \( \lambda_1 = x^{q'-1} + 1 = x^2 \) and \( x^{q'-1} + 1 = x^{q'+1} \). The second coordinate section shows that \( (bx^2 - bx^{q+1})N(y) + \lambda_3 d = 0 \), or

\[ \lambda_3 = N(y) \frac{b}{d} (x^{q+1} - x^2) \in \mathbb{F}_q. \]
Choose \( x \) in the cyclic group of order \( 2(q - 1) \), but outside \( \mathbb{F}_q \). Then \( x^2 = \lambda_1 \in \mathbb{F}_q \), \( x^{q+1} - x^2 \not\equiv 0 \). As \( y \) is arbitrary in \( F \), we can choose \( \lambda_3 \) such that \( \lambda_3 \) is indeed in \( \mathbb{F}_q \). This shows that no cap extension is obtained in this case.

Let \( r \) be even. We have \( x^{q+1} \in \mathbb{F}_q \), equivalently \( x \in \mathbb{F}_{q^2} \). It follows that \( \lambda_1 = x^{q+1} \) and \( N(x) = x^2 \). The second coordinate section yields

\[
\lambda_3 = N(y) \frac{b}{d}(x^2 - x^{q+1}) \in \mathbb{F}_q.
\]

Choose \( x \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q \). Then \( x^2 - x^{q+1} \not\equiv 0 \) and we can choose \( y \in F \) such that \( \lambda_3 \in \mathbb{F}_q \). Once again no extension cap is obtained.

\[ \square \]

6. Extensions by Points from the \((2r - 1)\)-Space \( PG(F) \)

**Theorem 3.** Let \( r \geq 2 \) and \( O(a : b) \) be one of the cyclic \( \frac{2r - 1}{2} \)-caps in \( PG(3r - 1, q) \) as constructed in Theorem 1. Extension caps \( O(a : b) \cup \{ Q \}, \) where \( Q = (c : 0) \in PG(F) \), do exist if and only if \( r = 2 \) and \( q \) a power of 2.

The remainder of this section is dedicated to a proof of Theorem 3. Choose \( P_1, P_2 \) and coefficients \( \lambda_1, \lambda_2, \lambda_3 \in \mathbb{F}_q \) as in the proof of Theorem 2. Without restriction \( \lambda_2 = -1 \). The second coordinate section yields

\[
\lambda_1 = N(x) = x^{q+1} \in \mathbb{F}_q.
\]

This shows that \( x \in Z((q^r + 1)(q - 1)) \). The first coordinate section shows that

\[
\lambda_3 = \frac{d}{c} y^{q^{-1}+1}(x^{q^{-1}+1} - x^{q+1}) \in \mathbb{F}_q.
\]

Observe that \( x^{q^{-1}+1} - x^{q+1} \not\equiv 0 \) as \( x \notin \mathbb{F}_q \). We distinguish several cases, which are treated in order of increasing difficulty.

Let \( r \) be odd and \( q \) a power of 2. As \( g = 1 \) in this case (see Lemma 1) we have that \( y^{q^{-1}+1} \) varies over \( F \) when \( y \) does. We can choose \( y \) such that \( \lambda_3 \in \mathbb{F}_q \). It follows that no extension cap is obtained.

Let \( r \) and \( q \) both be odd. We have \( g = 2 \). This means that \( y^{q^{-1}+1} \) varies over the squares in \( F \). Observe that the elements of \( \mathbb{F}_q \) are squares in \( F \). We have to show that when \( x \in Z((q^r + 1)(q - 1)) \setminus \mathbb{F}_q \), among the values \( x^{q^{-1}+1} - x^{q+1} \) there are squares as well as nonsquares.

Let \( \lambda = N(x) \in \mathbb{F}_q \) and \( y = x^{q^{-1}+1} \). Then \( y^q = x^{q^r+q} = \lambda x^{q-1} \), hence \( y = y^{q^2} = \lambda(x^{q-1})y^{q^{r-1}} \). It follows that

\[
f(x) = y - \lambda = \lambda(x^{q^{-1} - 1})y^{q^{r-1}}.
\]

Let \( \chi \) be the quadratic character of \( F \). Then \( \chi(f(x)) = \chi(x^{q^{-1}} - 1) \chi(y^{q^{r-1}}) = \chi(x^{q-1} - 1) \). Here \( x^{q^{-1}} \) varies over \( Z(q^r + 1) \setminus \{1\} \). This yields an equivalent formulation for our claim that no extension caps are obtained in the case under consideration. We have to show that \( v - 1 \) represents both squares and nonsquares, where \( v \) varies over \( Z(q^r + 1) \setminus \{1\} \). As it is clear that squares are represented (choose \( v = -1 \)), it suffices to show that there is some \( v \in Z(q^r + 1) \setminus \{1\} \) such that \( v - 1 \) is a nonsquare in \( F \).

Let \( w = v - 1 \not\equiv 0 \). The statement to be proved is equivalent to the following: there is some nonsquare \( w \in F \) such that \( N(w + 1) = 1 \). As \( N(w + 1) = N(w) + T(w) + 1 \) we can write equivalently \( N(w) = -T(w) \) or \( T(w/N(w)) = -1 \). As \( N(w) \) is a square in \( F \), our statement is equivalent to the following:
• There is a nonsquare \( w \in F \) such that \( T(w) = -1 \).

The elements \( w \) of trace \( T(w) = -1 \) are those of the form \( w = -1/2 + y \), where \( y = 0 \) or \( y^2 = -1 \). We have \( N(w) = 1/4 - y^2 = 1/4 - z \), where either \( z = 0 \) or \( z \) a nonsquare in \( L \). Observe that \( w \) is a square in \( F \) if and only if \( N(w) \) is a square in \( L \). Assume the statement we wish to prove is not true and fix a nonsquare \( c \in L \). Then the equation \( 1/4 - cz^2 = b^2 \) has a solution \( b \) for every \( a \in L \). Clearly these are way too many solutions for this quadratic equation, which, as we know, has \( Q + 1 \) projective solutions. This concludes the proof in the case that \( r \) is odd.

Let \( r \) be even. As \( g = q + 1 \) we have that \( y^q - 1 \) varies over the subgroup \( U \). Observe that \( \mathbb{F}_q^* \subseteq U \). We have to prove that \( x^q - 1 \) contains elements of each coset of \( U \) as \( x \) varies over \( Z(q + 1)(q - 1) \setminus \mathbb{F}_q \). The same arguments as in the case when \( r \) and \( q \) are odd show that we can reformulate our claim as follows.

• Let \( r \) be even and either \( r > 2 \) or \( q \) odd. For every coset \( yU \) there is some \( z \in Z(q^r + 1) \setminus [1] \) such that \( z - 1 \in yU \).

Consider first the case that \( q \) is odd. The choice \( z = -1 \) shows that \( U \) itself is represented. Observe that \( Z \) consists of the elements of norm \( N(z) = 1 \). Let \( v \in Z \) and \( w = v - 1 \). Our claim is that every coset \( yU \) contains an element \( w \) such that \( N(w + 1) = 1 \). As before this is equivalent with \( -1 = T(w/N(w)) = T(1/w) \). In other words, we have to show that every coset \( yU \) contains an element of trace \( -1 \).

The elements \( x \neq 0 \) of trace \( T(x) = 0 \) are those satisfying \( x^{q - 1} = -1 \). As \( T(-1/2) = -1 \) the element \( x \in F \) with \( T(x) = -1 \) are precisely those of the form \( x = -\frac{1}{2} + y \), where \( y \neq 0 \) or \( y^2 = -1 \). We want to show that every coset of \( U \) contains such an element. The subgroup \( U \) consists precisely of the elements \( u \in F \) such that \( N(u) \) is a \( (q + 1) \)th power (this is clear: as \( Z(q + 1) \) is the kernel of \( N \), the image \( N(U) \) has order \( |U|/|Z(q + 1)| = (q - 1)/(q + 1) \)). We have \( N(-\frac{1}{2} + y) = \frac{1}{4} - y^2 \) with \( y \) as above. Our claim is that every coset of the group \( N(U) \) of index \( q + 1 \) in \( L \) contains one of our elements \( -\frac{1}{2} - y^2 \). Here \( y \) varies over \( y \neq 0 \) and the elements satisfying \( y^q - 1 = -1 \). It follows that \( z = y^2 \) varies precisely over \( z = 0 \) and the elements in \( L \) satisfying \( y(q - 1)/2 = -1 \), in other words the nonsquares in \( L = \mathbb{F}_Q \).

Assume our claim is not true. Then there exists an element \( c \in L \) such that \( cx^q = \frac{1}{4} - z \); we have that \( z \) is never a nonsquare or \( 0 \), in other words

\[
y^2 = \frac{1}{4} - cx^q + 1
\]

has solutions \( y \in L \). If \( y \neq 0 \) for every \( x \in L^* = \mathbb{F}_Q^* \). This is a hyperelliptic curve of genus \( (q - 1)/2 \) (see [17, p. 197]). We observe that \( c \) cannot be a \( (q + 1) \)th power for it if we were able to choose \( x \neq 0 \) such that \( y = 0 \) is the only solution of the equation, which we assume not to be the case.

What can we say about the number \( N \) of rational points if our assumption is satisfied? There is one point \((0:1:0)\) at infinity (and the curve has a singularity there). If \( y = 0 \), then by assumption we have no solution. It follows that every \( x \neq 0 \) yields precisely two values for \( y \). Together with two solutions when \( x = 0 \) this yields a number of rational places \( N \geq 1 + 2 + 2(Q - 1) = 2Q + 1 \), contradicting the Hasse–Weil bound.

Our last case is: \( r \) even, \( q \) a power of 2. Recall that we have to show the following when \( r > 2 \): for every \( 0 \neq y \in F \) there is some \( z \neq 1 \) such that \( z - 1 \in \gamma U \) and \( N(z) = 1 \). Using \( w = z - 1 \) instead, an equivalent expression is \( N(w + 1) = 1 \). By now
familiar argument shows that this is equivalent to $T(w/N(w)) = 1$. This yields the following equivalent condition:

- For every $0 \neq \gamma \in F$ there is a $w \in \gamma U$ such that $T(w) = 1$.

Fix $w_0$ such that $T(w_0) = 1$. The general element of trace $T = 1$ has the form $w = w_0 + a$, where $a \in L$. Write $c = N(\gamma)$. We have to show that there is some $a \in L$ such that $N(w_0 + a) = cx^{q+1}$, where $x \in L$. We have $N(w_0 + a) = (w_0 + a)(w_0^q + a) = N(w_0) + aT(w_0) + a^2 = N(w_0) + a + a^2$. Let $\text{tr} : L \rightarrow F_2$ be the absolute trace. As $a$ varies over $L$, the element $a + a^2$ varies over the elements of trace $\text{tr} = 0$. We have reached the following equivalent reformulation:

- Fix $w_0 \in F$ such that $T(w_0) = 1$. For every $0 \neq c \in L$ there is an $x \in L$ such that $\text{tr}(cx^{q+1} + N(w_0)) = 0$.

As $T(w_0) = 1$ we have $w_0^q = w_0 + 1$, hence $N(w_0) = w_0(w_0 + 1) = w_0 + w_0^2$. Apply the definition of the trace. This yields $\text{tr}(N(w_0)) = 1$. Our claim simplifies as follows:

- For every $0 \neq c \in L$ there is an $x \in L$ such that $\text{tr}(cx^{q+1}) = 1$.

Assume this is not the case for some $c \in L$. Consider the trace-form defined on $L$ by $\text{tr}$, where we view $L$ as a vector space over $F_2$. With respect to this nondegenerate bilinear form we have $L^{q+1} \subset L$. It follows that $L^{q+1}$ is contained in a proper subgroup of the additive group of $L$. As the linear combinations of $(q + 1)$th powers are closed under addition and multiplication, this means that $L^{q+1}$ is contained in a proper subfield of $L$. Clearly, this cannot happen unless $Q = q^2$, in which case $L^{q+1} = F_q$. We see that for $r > 2$ such extension caps cannot exist, whereas in the case $r = 2$ they positively exist.

**Remark 1.** Theorem 3 is also confirmed by a result in [3, Proposition 9], where it is proved that if $q$ is even, a cap $O(a : b)$ in $PG(5, q)$ can always be extended by the points of an elliptic ovoid in $PG(F)$, where $F$ is now a three-dimensional projective space.

**Remark 2.** We have not been able to decide the completeness of our caps. Computer experiments suggest the conjecture that $O(a : b)$ can never be extended by a point $(c : d)$, where $c \neq 0, d \neq 0$.

## 7. Some Geometric Links

**Proposition 1.** Each cap constructed above is a projection of an EMS cap.

**Proof.** We give the proof in the case $r = 3$. It is easy to see that the proof generalizes to arbitrary $r$.

The collineation group $\langle \phi \rangle$ fixes two five-dimensional subspaces $K$ and $F$ and a plane $L$, inducing collineations whose matrix representations are $S^{q+1}, S^{q+1}$ and a Singer cycle $T$, respectively. Take anEMS cap $E$ inside the Grassmannian $G_{1,5}$ in $PG(14, q)$. We note that $E$ spans $PG(14, q)$. Consider the cone $C$ with vertex $K$ (hence its generators are six-dimensional subspaces of $PG(14, q)$ generated by $K$ and a point of $E$), and project $E$ on the space $\Sigma = (F, L)$. Since $K$ is $\phi$-invariant as well as $E$, the cone $C$ is $\phi$-invariant. The Grassmann dimensional formula shows that each generator of $C$ meets $\Sigma$ in exactly one point. Call $X$ the set of all such points. Clearly $X$ is $\phi$-invariant, and in particular it must be a $\langle \phi \rangle$-orbit. We have three possibilities. The set $X$ cannot be the plane $L$ as $E$ would have to be contained in an eight-dimensional subspace, contradicting the fact that $E$ spans $PG(14, q)$. Likewise, $X$ is not contained in $L$ as $X$ is not contained in an 11-dimensional subspace. This shows that $X$ must be one of our caps. \qed
Let $\mathcal{O}$ be one of the caps constructed in Theorem 1. Consider the subgroup $\langle C \rangle$ of $\langle A \rangle$ of order $q^2 + q + 1$. Its canonical form in $GL(9, q^3)$ is a diagonal matrix whose entries are $\eta^{q^2+1}$ and all its conjugates over $F_q$, again $\eta^{q^2+1}$ and all its conjugates over $F_q$, and $\eta^2$ and all its conjugates over $F_q$, where $\eta = \alpha q^{\frac{1}{3}} \in F_{q^3}$. In geometrical terms, $\langle C \rangle$ fixes the 5-space $F$ inducing a regular 2-spread $S$ and the plane $L$ permuting its points in a single orbit (indeed $\gcd(2, q^2 + q + 1) = 1$). Also $\langle C \rangle$ fixes each 5-subspace generated by $\pi$ and a plane of $S$. The collineation induced by $C$ on each of these 5-subspaces is exactly the lifting of a Singer cycle of $PGL(3, q)$ to a collineation of $PG(5, q)$ fixing a Veronese surface [1]. Each of these 5-subspaces is either disjoint from $\mathcal{O}$ or meets $\mathcal{O}$ in at least a Veronese surface. We have proved the following proposition.

**Proposition 2.** Each cap constructed in Theorem 1 is a union of $q^3 + 1$ Veronese surfaces.

**Remark 3.** Note that the previous proposition extends to higher dimensions. In the general case we have Veronese varieties instead of Veronese surfaces.

The canonical form of $C$ in $GL(9, q^3)$ coincides with the canonical form of the Kronecker product of a Singer cycle of $GL(3, q^3)$ by itself. We conclude with the following corollary.

**Corollary 1.** Each of the Veronese surfaces partitioning $\mathcal{O}$ is contained in a Segre variety $S_{2,2}$ of $\Sigma$.

8. The Link to Cyclic Codes

Consider the cap $\mathcal{O}(1 : 1)$. Write the points of this cap as columns of a matrix $G$ with $3r$ rows. There are $n = \frac{q^{2r}-1}{q-1}$ columns. The presence of the Singer cycle (regular on the columns) shows that this generates the dual of a cyclic $q$-ary code, more precisely: the cyclic code is the dual of the trace code of the $F$-ary code generated by the rows of $G$. This cyclic code has parameters

$$\left[\frac{q^{2r} - 1}{q - 1}, \frac{q^{2r} - 1}{q - 1} - 3r, 4\right].$$

In the language of the theory of cyclic codes it has as defining set the cyclotomic cosets containing $q^{r-1} + 1$ (of length $2r$) and $q^r + 1$ (of length $r$). Apparently the standard bounds for cyclic codes do not suffice to show that the minimum distance is indeed 4.

9. Cap Partitions

Denote by $\kappa(PG(n, q))$ the minimum number of caps into which $PG(n, q)$ can be partitioned. Theorem 1 shows that the points of $PG(3r - 1, q)$ can be partitioned into

- the points of a subspace $PG(2r - 1, q)$,
- the points of a subspace $PG(r - 1, q)$, and
- $q^r - 1$ caps of size $(q^{2r} - 1)/(q - 1)$ each.

This yields the following recursive bound:

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

Recent results on the ternary case are in [11]. Cap partitions will be studied in a subsequent paper.
REFERENCES


Received 2 December 1999 and accepted 28 September 2000

Jürgen Bierbrauer
Department of Mathematical Sciences,
Michigan Technological University,
Houghton,
MI 49931, U.S.A.

Antonio Cossidente
Dipartimento di Matematica,
Università della Basilicata,
via N. Sauro, 85,
85100 Potenza,
Italy
E-mail: cossidente@unibas.it

Yves Edel
Mathematisches Institut der Universität,
Im Neuenheimer Feld 288,
69120 Heidelberg,
Germany