CLASSICAL VARIETIES AND CAPS

A. COSSIDENTE   V. NAPOLITANO

Dipartimento di Matematica - Università degli Studi della Basilicata, via Nazario Sauro, 85 -I- 85100 POTENZA
E-mail address: cossidente@unibas.it, vnapolitano@unibas.it

Abstract. Let $PG(n,q)$ be the projective n–space over the Galois field $GF(q)$. A k–cap in $PG(n,q)$ is a set of k points such that no three of them are collinear. A k-cap is said to be *complete* if it is maximal with respect to set–theoretic inclusion. In this paper, using classical algebraic varieties, such as Segre varieties and Veronese varieties, some new infinite classes of caps are constructed.

1. Introduction

The aim of this paper is to give some cap constructions in Galois projective spaces using classical varieties such as Segre varieties and Veronese varieties.
Let $PG(n,q)$ be the n-dimensional projective space over the Galois field $GF(q)$.
A k cap in $PG(n,q)$ is a set of k points such that no three of them are collinear. A k-cap is said to be *complete* if it is maximal with respect set-theoretic inclusion.
The cardinality of the largest cap in $PG(n,q)$ is denoted by $m_2(n,q)$. This number $m_2(n,q)$ is known for only a few values of n and q, namely

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

$$m_2(3,q) = q^2+1, \quad \text{if } q > 2$$

$$m_2(r,2) = 2^r, \forall r \geq 2$$

$$m_2(4,3) = 20$$

$$m_2(5,3) = 56$$

$$m_2(4,4) = 41.$$

Finding the exact value of $m_2(n,q)$ and constructing an $m_2(n,q)$-cap in $PG(n,q)$, in general, appears to be a very difficult problem.

Hence much work has been devoted to the construction of caps embedded in various varieties (quadrics, hermitian varieties and so on) or caps admitting a particularly interesting automorphism group.
Here we do not construct caps which are particularly large, but they are interesting from a geometric point of view.

2. Segre varieties and caps

In this section we generalize the main results of [BBCE], showing that the caps constructed in the cited paper belong to an infinite family.

Let $PG(m,q)$ and $PG(k,q)$ be projective spaces over $GF(q)$ with $m,k \geq 1$. Set $N=(m+1)(k+1)-1$. For each $\mathbf{u}=(u_0,u_1,\dots,u_m) \in GF(q^{m+1})$ and $\mathbf{w}=(w_0,w_1,\dots,w_m) \in GF(q^{k+1})$ define:

$$(\mathbf{u} \otimes \mathbf{w}) = (u_0v_0, u_0w_1, \dots, u_0w_k,$$

$$u_1w_0, u_1w_1,, \dots, u_1w_k, \dots, u_mw_0, u_mw_1, \dots, u_mw_k).$$

The *Segre variety* of the two projective spaces, is the variety $\mathcal{S}=\mathcal{S}_{m,k}$ of $PG(N,q)$ consisting of all points represented by the vectors $(u \otimes w)$ as u and w vary over all non-zero vectors of $GF(q)^{m+1}$ and $GF(q)^{k+1}$, respectively.

The Segre variety has two families of maximal subspaces with dimensions m and k respectively, say $\mathcal{M}$ and $\mathcal{K}$, each of which form a cover of $\mathcal{S}$. Two maximal subspaces from one and the same family are skew; two maximal subspaces from distinct families meet in exactly one point. We have [HT]

$$\mathcal{M}=\{PG(m,q)\otimes w | w \in PG(k,q)\},$$

$$\mathcal{K}=\{u \otimes PG(k,q) | u \in PG(m,q)\}.$$

Let S and T be Singer cycles in $GL(m+1,q)$ and $GL(n+1,q)$, respectively. Then the Kronecker product $S \otimes T$ yields a linear collineation of $PG(n,q)$ fixing $\mathcal{S}$ setwise.

Lemma 2.1. [[BBCE], Lemma 2] *Each point orbit of $S \otimes T$ contained in $\mathcal{S}$ meets each member of $\mathcal{M} \cup \mathcal{K}$ in at least one point.*

Assume from now on that n is an even integer.
Let T be a Singer cycle in $GL(2n,q)$. The matrix T is conjugate in $GL(2n,q^{2n})$ to the diagonal matrix $D_2 = diag(\omega, \omega^q, \dots, \omega^{q^{2n-1}})$ for some

primitive element ω in $GF(q^{2n})$. The element ω^{q^n+1} is a primitive element of $GF(q^n)$ and so there exists a Singer cycle S in $GL(n,q)$ which is conjugate in $GL(n,q^n)$ to the diagonal matrix

$$D_1 = diag(w^{q^n+1}, w^{q^{n+1}+q}, \dots, w^{q^{2n-1}+q^{n-1}}).$$

The Kronecker product $S \otimes T$ is conjugate in $GL(2n^2, q)$ to the Kronecker product

$$D_1 \otimes D_2 = diag(\omega^{q^n+2}, \omega^{q^n+q+1}, \omega^{q^n+q^2+1}, \dots, \omega^{q^n+q^{n-1}+1}, \dots).$$

It follows that the rational canonical form of $S \otimes T$ over $GF(q)$ is a block diagonal matrix

$$R = diag(C_1, C_2, \dots, C_n),$$

being each C_i the companion matrix of an irreducible polynomial of degree $2n$.

Let g be the collineation induced by R on $PG(2n^2-1, q)$, it fixes n projective $(2n-1)$-dimensional subspaces, say $\Sigma_1, \Sigma_2, \dots, \Sigma_n$, and all subspaces generated by them.

Lemma 2.2. (i) *The order of g is $\dfrac{q^{2n}-1}{q-1}$;*

(ii) *The collineation group G generated by g acts semiregularly on $PG(2n^2-1, q) \setminus (\cup_{i=1,\dots,n}\Sigma_i)$.*

PROOF. (i) Let $\alpha = q^{2n-1} + q^{2n-2} + \dots + q + 1$, then since ω is a primitive element of $GF(q^{2n})$, it follows that

$$\omega^{(q^n+2)\alpha} = \omega^{(q^n+q+1)\alpha} = \dots = \omega^{(q^n+q^{n-1}+1)\alpha} = \beta^3,$$

whit $\beta \in GF(q)^*$, and so the order of g is at most α. Assume that the order of g is $k < \alpha$. Then

$$\omega^{(q^n+2)k} = \omega^{(q^n+q+1)k} = \dots = \omega^{(q^n+q^{n-1}+1)k},$$

and so we get for instance, $\omega^{(q-1)k} = 1$. It follows that $q^{2n}-1|(q-1)k$ and so α divides k, a contradiction.

(ii) Let P be a point of $PG(2n^2, q)$ not belonging to $\cup_{i=1,\dots,n}\Sigma_i$ and subspaces generated by part of $\Sigma_i's$.

Let $P = (\underline{x}_1, \dots, \underline{x}_n)$, where $\underline{x}_i$ is a non- zero vector in $GF(q^{2n})$. Assume that P is proportional to $P \cdot R^i$ for some $i, 0 \le i < \dfrac{q^{2n}-1}{q-1}$. Then there exists a non-zero element $\lambda \in GF(Q)$ such that, for example, $\lambda\underline{x}_1 = \underline{x}_1 C_1^i$ and $\lambda\underline{x}_2 = \underline{x}_2 C_2^i$. This means that C_1^i and C_2^i have a common eigenvalue in $GF(q) \setminus \{0\}$.

We have $\lambda = \lambda^{(q^n+2)i} = \omega^{(q^n+q+1)iq^j}$ for some $j \in \{0, 1, 2, \ldots, 2n-1\}$. Since $\lambda \in GF(q)$, hence $\lambda = \lambda^{(q^{2n}-j)} = \omega^{(q^n+q+1)i}$. Then $\omega^{(q^n+2)}i = \omega^{(q^n+q+1)i}$ and so $\omega^{(q-1)i=1}$. It follows that $q^{2n}-1|(q-1)i$, and so $\alpha|i$, a contradiction. □

Let $\mathcal{S} = \mathcal{S}_{n-1,2n-1}$ be the Segre variety of $PG(2n^2-1, q)$ fixed by G.

Theorem 2.3. *Each point orbit of G on $\mathcal{S}$ is a cap of size $q^{2n-1}+\ldots+q+1$.*

PROOF. Let $\mathcal{O}$ be an orbit of G on $\mathcal{S}$. Of course G leaves $\mathcal{M}$ and $\mathcal{K}$ invariant, and each G-orbit on $\mathcal{S}$ meets each subspace in $\mathcal{M}$ in at least one point (Lemma 2.1).

Since $|\mathcal{M}| = |\mathcal{O}| = q^{2n-1} + q^{2n-2} + \ldots + q + 1$ and since two elements in $\mathcal{M}$ are skew, it follows that each element of $\mathcal{M}$ meets $\mathcal{O}$ in exactly one point.

In the same way, $\mathcal{O}$ meets each element of $\mathcal{K}$ meets $\mathcal{O}$ in at least one point and so G acts transitively on $\mathcal{K}$.

Since $|\mathcal{K}| = q^n + q^{n-1} + \ldots + q + 1$, the stabilizer of a subspace in $\mathcal{K}$ is the subgroup $H = [g^{q^{n-1}+\ldots+q+1}]$ of order q^n+1 of G, and so H fixes $\mathcal{K}$ elementwise.

We conclude that H induces a cyclic linear collineation of order q^n+1 on each subspace π of $\mathcal{K}$.

In particular, from [[BBCE], Lemma 1] it follows that each H-orbit is a power of a Singer cycle and so from [E] it is a q^n+1 cap.

Suppose that there exists a line ℓ of $PG(2n^2-1, q)$ meeting $\mathcal{O}$ in three points. Then since $\mathcal{S}$ is intersection of quadrics, $\ell \subset \mathcal{S}$ and so ℓ is contained in some maximal subspace of either $\mathcal{M}$ or $\mathcal{K}$. Since each element of $\mathcal{M}$ meets $\mathcal{O}$ in exactly one point, it follows that ℓ lies inside a subspace of $\mathcal{K}$. This means that ℓ is a trisecant of a Ebert's cap of size q^n+1, a contradiction. □

As an immediate consequence we have the following corollary.

Corollary 2.4. *The projective space $PG(2n^2-1, q)$ can be partitioned into n-projective subspaces of dimension $2n$ and caps of type $\mathcal{O}$.*
Moreover the Segre variety $\mathcal{S}$ can be partitioned into caps of type $\mathcal{O}$.

Remark 2.5. The size of the caps constructed as above is small with respect to the number of points of the space.

It should be remarked, however, that such caps can be projected onto a subspace S. The projected caps turn out to be fairly big with respect to the dimension of S.

Example 2.6. Assume $n = 4$. Consider the group H induced by G on the projective subspace Σ of $PG(31, q)$ generated by Σ_1, and Σ_2. Then

$H = \langle h \rangle$, where

$$h = \begin{pmatrix} C_1 & 0 \\ 0 & C_2 \end{pmatrix}.$$

Using the software package MAGMA [MAGMA] we showed that for low values of q, the non-linear H-orbits are caps of size $q^7 + \ldots + q + 1$, and each of them can be obtained by projecting the caps of type $\mathcal{O} \subset PG(31, q)$ from the subspace generated by Σ_3, and Σ_4.

Proposition 2.7. *Let $\mathcal{O}$ be a cap of the type described above. Then $\mathcal{O}$ is complete in $\mathcal{S}$ if and only if $X \cap \mathcal{O}$ is complete, for all $X \in \mathcal{K}$.*

PROOF. Suppose that $X \cap \mathcal{O}$ is complete for each $X \in \mathcal{K}$. If $\mathcal{O}$ is not complete, then there exists a point $p \in \mathcal{S}$ such that $\mathcal{O} \cup \{p\}$ is a cap. But the elements of $\mathcal{K}$ partition $\mathcal{O}$, hence there exists $X \in \mathcal{K}$ such that $p \in X$. So we can add the point p to the complete cap $X \cap \mathcal{O}$.

Let $\mathcal{O}$ be complete. Assume that there exists $X \in \mathcal{K}$ such that $X \cap \mathcal{O}$ is not complete. Put $\Omega = X \cap \mathcal{O}$. Since Ω is not complete, there exists a point $p \in X \setminus \Omega$ such that $\{p\} \cup \Omega$ is a cap. But $\mathcal{O}$ is complete, then there exists a line ℓ passing through p meeting $\mathcal{O}$ in two points. This line is not contained in X, because $\{p\} \cup \Omega$ is a cap. So $\ell \cap X = \{p\}$. Since elements of $\mathcal{K}$ are pairwise skew, then ℓ is contained in no one $Y \in \mathcal{K}$. Let p_1, p_2 be the two points of $\mathcal{O} \cap \ell \setminus \{p\}$. Since $\ell \subset \mathcal{S}$, there exists a maximal subspace Z of $\mathcal{S}$ containing ℓ. Hence, from the previous argumentation, $Z \in \mathcal{M}$, contradicting the fact that $|X \cap \mathcal{O}| = 1$, for all $X \in \mathcal{M}$. □

In the proof of Theorem 2.3 we have seen that if $X \in \mathcal{K}$ then $X \cap \mathcal{O}$ is a $(q^n + 1)$-Ebert cap. Since for $n = 2$ an Ebert cap is an elliptic quadric, then from the previous proposition it follows the following result.

Proposition 2.8. *Let $\mathcal{O}$ be a cap of the type described above. If $n = 2$ then $\mathcal{O}$ is complete in $\mathcal{S}$.*

Remark 2.9. Since in general, for $n \geq 4$ and n even, an Ebert cap is not complete, then in general caps of type $\mathcal{O}$ are not complete.

3. Veronese varieties and generalized inscribed bundles

In this section we consider the following problem. It is known that the quadric Veronesean of $PG(n, q)$ [HT] is a cap of size $q^n + \ldots + q + 1$. Can two or more Veronese varieties be glued to obtain a larger cap?

We begin with the following definition.

Definition 3.1. A generalized inscribed bundle of $PG(n,q)$ consists of all quadrics of $PG(n,q)$ that are simultaneously tangent to the fundamental lines of a $(n+1)$-simplex of $PG(n,q)$.

The generic quadric Q of $PG(n,q)$, q odd, has equation

$$\sum_{i<j} a_{ij}x_ix_j = 0, \text{ with } a_{ij} \in GF(q).$$

Denote by $A = (a_{ij})$ the symmetric matrix associated to the quadric Q. By imposing the condition that the $\binom{n+1}{2}$ lines joining the points U_i and U_j of the standard $(n+1)$ simplex, to be tangent to the quadric Q gives the following $\binom{n+1}{2}$ conditions

$$a_{ii}ajj - a_{ij}^2 = 0, \text{ with } i<j,\ i = 0,1,\dots,n.$$

Consider the projective space $PG(\frac{n(n+3)}{2},q)$, where $X_{00}, X_{11}\dots,$ $X_{n-1n-1}, X_{01}, X_{02},\dots, X_{n-1n}$ are homogeneous coordinates and map the quadric of $PG(n,q)$, represented by the matrix A, to the point $(a_{00}, a_{11},\dots, a_{n-1n}$ of $PG(\frac{n(n+3)}{2},q)$.
For $i,j \in \{0,1,\dots,n\}, i \neq j$ define

$$Q_{ij} = X_{ij}^2 - X_{ii}X_{jj}.$$

An immediate generalization of [[BC], Proposition 1] gives the following proposition.

Proposition 3.2. *The quadrics of a generalized inscribed bundle of $PG(n,q)$ in the quadric-point correspondence, are points of a variety $\mathcal{O}_n$ obtained by intersecting the $\binom{n+1}{2}$ quadrics Q_{ij}*

Proposition 3.3. *The variety $\mathcal{O}_n$ is a cap.*

PROOF. We will prove the result by induction on n.
For $n=1$, $\mathcal{O}$ is a conic of $PG(2,q)$ and so is a cap.
Assume the result is true for $n-1, n>2$.
Suppose that $\mathcal{O} \subset PG(\frac{n(n+3)}{2},q)$ has three collinear points on the line ℓ.
Let M be a monomial matrix of $PG(n+1,q)$, say $M = diag(\alpha_0,\alpha_1,\dots,$ $\alpha_n)$. Using [[CLS], Th 3.1] we can lift M to a matrix $\overline{M}$ of $PGL(\frac{n(n+3)}{2}+1,q)$ leaving the quadric Veronesean $\mathcal{V}_n$ invariant.

Of course, $\langle\overline{M}\rangle$ leaves $\mathcal{O}$ invariant. Now, we can choose M in the stabilizer S in $PGL(n+1,q)$ of a hyperplane H of $(PG(n,q)$.
From[[HT], Theorem 25.1.7], under the quadratic-point correspondence, the image of H is a quadric Veronesean $\mathcal{V}_{n-1}$, which is the complete intersection of $\mathcal{V}_n$ and the projective space $PG(\frac{(n-1)(n+2)}{2},q)$ containing $\mathcal{V}_{n-1}$.
Suitably choosing H we can assume that the lifting of $M \in S$ is

$$\overline{M} = diag(1,\alpha_1^2,\alpha_2^2,\dots,\alpha_{n-1}^2,1,\dots,1\dots,\alpha_{n-1}\alpha_n).$$

Such a collineation sends the line ℓ into a line of $PG(\frac{(n-1)(n+2)}{2},q)$ which is trisecant to a variety $\mathcal{O}_{n-1}$. The inductive hypothesis gives the result.

Remark 3.4. The variety $\mathcal{O}_2$ has been studied in [BC]. It turns out that $\mathcal{O}_2$ is the union of two Veronese surfaces, say $\mathcal{V}_1, \mathcal{V}_2$, of $PG(5,q)$. The intersection of $\mathcal{V}_1$ and $\mathcal{V}_2$ is the union of three conics intersecting pairwise in one point.
For further results on gluings of Veronese surfaces in $PG(5,q)$ see [CHS].

Remark 3.5. The variety $\mathcal{O}_n$ is the union of Veronese variety $\mathcal{V}_n$ of $PG(\frac{n(n+3)}{2},q)$.
The proof is completely similar to [BC].

Example 3.6. The cap $\mathcal{O}_3 \subset PG(9,q)$ is union of 8 Veronese varieties.

Actually it contains the following 8 Veronese varieties.

$$(u_1^2, u_1u_2, u_1u_3, u_1u_4, u_2^2, u_2u_3, u_2u_4, u_3^2, u_3u_4, u_4^2)$$

$$(u_1^2, -u_1u_2, u_1u_3, u_1u_4, u_2^2, u_2u_3, u_2u_4, u_3^2, u_3u_4, u_4^2)$$

$$(u_1^2, u_1u_2, -u_1u_3, u_1u_4, u_2^2, u_2u_3, u_2u_4, u_3^2, u_3u_4, u_4^2)$$

$$(u_1^2, u_1u_2, u_1u_3, -u_1u_4, u_2^2, u_2u_3, u_2u_4, u_3^2, u_3u_4, u_4^2)$$

$$(u_1^2, u_1u_2, u_1u_3, u_1u_4, u_2^2, -u_2u_3, u_2u_4, u_3^2, u_3u_4, u_4^2)$$

$$(u_1^2, u_1u_2, u_1u_3, u_1u_4, u_2^2, u_2u_3, -u_2u_4, u_3^2, u_3u_4, u_4^2)$$

$$(u_1^2, u_1u_2, u_1u_3, u_1u_4, u_2^2, u_2u_3, u_2u_4, u_3^2, -u_3u_4, u_4^2)$$

$$(u_1^2, -u_1u_2, -u_1u_3, -u_1u_4, u_2^2, -u_2u_3, -u_2u_4, u_3^2, -u_3u_4, u_4^2).$$

4. A cap embedded in the Klein quadric $\mathcal{H}^5$

In [CHS] a new $(2q^2+q+1)$-cap embedded in the Klein quadric $\mathcal{H}^5$ was constructed. This cap is the image, via the Plücker map, of the chords of a twisted cubic Γ of $PG(3,q)$ and of the axes of its osculating developable Γ^*.

A *chord* of Γ is a line of $PG(3,q)$ joining either a pair of real points of Γ, possibly coincident, or a pair of complex conjugate points of Γ. Let Γ^* be the set of osculating planes of Γ. If $p \neq 3$, dual to the chords of Γ are the *axes* of Γ^*. An *axis* of Γ^* is a line of $PG(3,q)$, which is the intersection of a pair of real planes of Γ^*, possibly coincident, or of a pair of complex conjugate planes of Γ^*. The total number of chords of Γ is q^2+q+1. Dually, the total number of axes of Γ^* is q^2+q+1.

From now on assume q even.

Let

$$\mathcal{V}^0 = \{(u^2, uv, v^2, uw, vw, w^2) : u, v, w \in GF(q)\}$$

be a Veronese surface of $PG(5,q)$. And let $N(\mathcal{V}) : \{(0,a,0,b,c,0) : a,b,c \in GF(q)\}$ be the nucleus of $\mathcal{V}$, (i.e. the plane of $PG(5,q)$ with contains all the nuclei of conics of $\mathcal{V}$).

Denote by

$$(X_{01}, X_{02}, X_{03}, X_{12}, X_{13}, X_{23})$$

the homogeneous coordinates of points of $PG(5,q)$.

The linear map

$$\Phi : (X_{01}, X_{02}, X_{03}, X_{12}, X_{13}, X_{23}) \mapsto (X_{01} X_{02}, X_{03} + X_{12}, X_{12}, X_{13}, X_{23})$$

embeds $\mathcal{V}$ in the Klein quadric $\mathcal{H}^5 : X_{01}X_{23} + X_{02}X_{13} + X_{03}X_{12} = 0$. The Veronese surface embedded in $\mathcal{H}^5$ is:

$$\mathcal{V} = \{(u^2, uv, v^2 - uw, uw, vw, w^2) : u, v, w \in GF(q) \cup \{\infty\}\}.$$

Also, the map Φ sends the nucleus of $\mathcal{V}$ to the plane

$$N(\mathcal{V}) : \{(0,a,b,b,c,0) : a,b,c \in GF(q)\}.$$

The axes of a twisted cubic of $PG(3,q)$ give a Veronese variety $\overline{\mathcal{V}}$ embedded in $\mathcal{H}^5$, (see[CHS]) and it is:

$$\overline{\mathcal{V}} = \{(u^2, uv, uw, v^2 - uw, vw, w^2) : u, v, w \in GF(q) \cup \{\infty\}\}.$$

Its nucleus is

$$N(\overline{\mathcal{V}}) : \{(0,a,b,b,c,0) : a,b,c \in GF(q)\}.$$

Hence, we have the following result.

Proposition 4.1. $N(\mathcal{V}) = N(\overline{\mathcal{V}})$.

Remark 4.2. The two Veronese varieties embedded on $\mathcal{H}^5$ are distinct, (see [CHS]).

The equations of the conic C, obtained by sectioning $\mathcal{H}^5$ with the nucleus $N(\mathcal{V})$ are

$$C : \begin{cases} X_{02}X_{13} + X_{03}^2 = 0 \\ X_{03} = X_{12} \\ X_{01} = X_{13} = 0 \end{cases} .$$

The two surfaces $\mathcal{V}$ and $\overline{\mathcal{V}}$ meet in the following conic:

$$C' : \begin{cases} X_{01}X_{23} + X_{03}^2 = 0 \\ X_{02} = X_{13} = 0 \\ X_{03} = X_{12} \end{cases} .$$

Since q is even the conics C and C' represent reguli of lines of $PG(3,q)$. The regulus corresponding to C is $R_C = (M_1, M_2, M_3)$, where

$$M_1 = (0,0,0,0,1,0),\ M_2 = (0,1,1,1,1,0),\ M_3 = (0,1,0,0,0,0).$$

The regulus of tangents to Γ (i.e. the regulus represented by C') is:

$$R_{C'} = (L_1, L_2, L_3)$$

where:

$$L_1 = (1,0,1,1,0,1),\ L_2 = (0,0,0,0,0,1)\ L_3 = (1,0,0,0,0,0).$$

By using the mutual invariant [HT] we see that the second regulus is the opposite of the first.

Proposition 4.3. *The set* $\mathcal{V} \cup \overline{\mathcal{V}} \cup C$ *is a cap.*

PROOF. Assume by way of contradiction that there are three collinear points P_1, P_2, P_3 on $\mathcal{V} \cup \overline{\mathcal{V}} \cup C$, and let L be the line containing these three points. The line L is contained in $\mathcal{H}^5$, since it contains three points of $\mathcal{H}^5$. Since $\mathcal{V} \cup \overline{\mathcal{V}}$ is a cap (see [CHS]) and since $\mathcal{V}$ (respectively $\overline{\mathcal{V}}$) and $N(\mathcal{V})$ are skew we have only to consider the following cases.

(i) $P_i, P_j \in \mathcal{V}$ and $P_k \in C$, $i \neq j \neq k \neq i$, $i,j,k \in \{1,2,3\}$.
(ii) $P_i, P_j \in \overline{\mathcal{V}}$ and $P_k \in C$, $i \neq j \neq k \neq i$, $i,j,k \in \{1,2,3\}$.
(iii) $P_i, P_j \in C'$ and $P_k \in C$, $i \neq j \neq k \neq i$, $i,j,k \in \{1,2,3\}$.
(iv) $P_i \in \mathcal{V} \setminus C'$, $P_j \in \mathcal{V} \setminus C'$ and $P_k \in C$, $i \neq j \neq k \neq i$, $i,j,k \in \{1,2,3\}$.

Let ℓ, ℓ' and ℓ'' be the three lines in $PG(3,q)$ corresponding to the points P_1, P_2 and P_3. Since L is a line of $\mathcal{H}^5$ the lines ℓ, ℓ' and ℓ'' belong to the pencil of center p.

CASE (i). Let Ω be a conic of $\mathcal{V}$ passing through P_2 and P_3. Then

the conic plane π_Ω, (that is the plane meeting $\mathcal{V}$ in Ω), contains the line L. Since π_Ω meets the nucleus $N(\mathcal{V})$ in exactly one point, we have $\pi_\Omega \cap N(\mathcal{V}) = P_1$. Hence P_1 is the nucleus of Ω in π_Ω, contradicting the fact that through P_1 there passes the line L that is a secant of Ω.

CASE (ii). It follows from the previous CASE (i) by duality (see [HT]).

CASE (iii). In this case the contradiction follows from the fact that the lines ℓ, ℓ' and ℓ'' are in a pencil and one on them is in the opposite regulus in which the other two lie.

CASE (iv). Let $P_2 = (u^2, uv, v^2 - uw, uw, vw, w^2)$ be the point of $\mathcal{V}$ and $P_3 = (\overline{u}^2, \overline{uv}, \overline{uw}, \overline{v}^2 - \overline{uw}, \overline{vw}, \overline{w}^2)$ that of $\overline{\mathcal{V}}$. If the line P_2P_3 meets $N(\mathcal{V})$ then $\lambda u^2 = \mu\overline{u}^2, \lambda v^2 = \mu\overline{v}^2, \lambda w^2 = \mu\overline{w}^2$. It follows that such line meets the plane $N(\mathcal{V})$ outside $\mathcal{C}$. Hence also this case is not possible.

This completes the proof. □

Remark 4.4. Using the software package MAGMA [MAGMA] we found that for the first values of q (q even) the cap constructed in Proposition 4.3 is complete. In a recent paper A.Blokhuis and P.Sziklai [BS] proved that any complete cap on the Klein quadric has size at least cons$\cdot q^{\frac{12}{7}}$. Hence our cap reach the above lower bound.

References

[BBCE] R.D. Baker, A.Bonisoli, A.Cossidente , G.L.Ebert, Cap partitions of Segre variety $\mathcal{S}_{1,3}$, (submitted).

[BC] A.Bonisoli, A.Cossidente, Inscribed bundles, Veronese surfaces and caps, in: Geometry, Combinatorial Designs and related structures, Proocedings of the First Pythagorean Conference, Spetses 1-7 June 1996, Eds. J.W.P.Hirschfeld, s.S. Magliveras, M.J. de Resmini, 27-32, cambridge University Press, Cambridge 1997.

[BS] A.Blokhuis, P.Sziklai A note on small complete caps in the Klein quadric, Bull. Belg. Math. Soc. 5(1998), 159-161.

[CHS] A.Cossidente, J.W.P.Hirschfeld, L.Storme, Application of line geometry. III. The quadric Veronesean and the chords of a twisted cubic, Australas. J. Combin. 16 (1997), 99-111.

[CLS] A.Cossidente, D.Labbate, A. Siciliano, Veronese varieties over finite fields and their projections, Designs, Codes and Cryptography, (to appear).

[E] G.L.Ebert, Partitioning projective geometries into caps. Canad. J. Math. 37 (1985), no.6, 1163-1175.

[HT] J.W.P.Hirschfeld, J.A.Thas, *General Galois Geometry*, Oxford University Press, Oxford, 1991.

[H] B.Huppert, *Endliche Gruppen I*, Springer, Berlin, 1967.

[MAGMA] J. Cannon, C. Playoust, An Introduction to MAGMA, University of Sidney, Sidney Australia, 1993.

On Groups with Redundancy in Multiplication[1]

M.M. Parmenter

Following the terminology in [2], we define a B_k-group to be a group G which satisfies the following condition:

If $\{a_1, \ldots, a_k\}$ is a k-subset of G, then $|\{a_i a_j | 1 \leq i, j \leq k\}| \leq \frac{k(k+1)}{2}$.

As in [2] and [3], we will use the notation $\{a_1, a_2, \ldots, a_k\}^2$ to denote $\{a_i a_j | 1 \leq i, j \leq k\}$.

Clearly all abelian groups are B_k-groups, as are all nonabelian groups of order $\leq \frac{k(k+1)}{2}$. The interesting problem is to determine which other nonabelian groups are B_k-groups. When $k = 2$, Freiman [4] showed that a nonabelian group is a B_2-group if and only if it is a Hamiltonian 2-group. It appears that this is the only value of k for which a complete characterization has been given, but Brailovsky [3] proved that when $k > 2$ a nonabelian B_k-group must be finite of order $\leq 2(k^3 - k)$. The corresponding notion of B_k-rings has been investigated by Bell and Klein in [2], and the same authors studied a related redundancy condition on rings in [1]. We would like to thank Howard Bell for several helpful conversations on this topic, and for providing us with a copy of [2].

In this note, we give a complete characterization of B_k-groups in the cases $k = 3, k = 4$. Specifically, we show that the only nonabelian B_k-groups in these cases are those of order $\leq \frac{k(k+1)}{2}$. We then give an example showing that this behaviour does not extend to $k = 5$.

The first half of the proof of the $k = 3$ case is essentially the same as the proof of Lemma 4.3 in [2].

[1] This research was supported in part by NSERC grant A-8775.

Theorem 1 *A nonabelian group G is a B_3-group if and only if G is isomorphic to S_3.*

Proof.
Assume that G is a nonabelian B_3-group. We will show first that if x, y are two noncommuting elements of G, then $< x, y > \cong S_3$.

To see this suppose first that $x^2 = 1$ and $y^2 \neq 1$. Note that $\{x, y, xy\}^2$ contains the 6 distinct elements $1, xy, y, yx, y^2, yxy$, so any other element in $\{x, y, xy\}^2$ must equal one of these. The only possibility for xy^2 is $xy^2 = yx$, while the possibilities for $xyxy$ are $xyxy = 1, yx$, or y^2. The latter two cases are incompatible with $xy^2 = yx$, so we are left with $xyxy = 1$ and $xy^2 = yx$. But this means that $y^3 = x^2y^3 = xyxy = 1$, and so $< x, y > \cong S_3$ as desired.

Next note that if $x^2 = 1$ and $y^2 = 1$, then $(xy)^2 \neq 1$ (since $xy \neq yx$). Since $< x, y >=< x, xy >$, we are in the case covered by the previous paragraph.

Finally assume $x^2 \neq 1$ and $y^2 \neq 1$. Since $\{1, x, y\}^2$ contains the 6 distinct elements $1, x, y, x^2, xy, yx$, we conclude that $y^2 = x^2$ in this case. But then consider $\{x, y, xy\}^2$. It contains the 6 distinct elements $x^2, xy, x^2y, yx, yxy, xy^2$. Hence xyx equals one of these elements, and the only possibility is $xyx = yxy$. Similarily we must have $xyxy = x^2$ or yx, but these are both incompatible with $xyx = yxy$. We conclude that this case is impossible.

Now let x, y be any two noncommuting elements of G. We have shown that $< x, y > \cong S_3$, and may assume that $x^2 = 1, y^3 = 1$ and $yx = xy^2$.

We wish to prove that $< x, y >= G$. Assume to the contrary that $z \notin < x, y >$. We may assume that x and z don't commute (otherwise replace z by yz). It follows from our earlier argument that $< x, z > \cong S_3$. Since $x^2 = 1$, either $z^3 = 1$ or $(xz)^3 = 1$. Replacing z by xz if necessary, we may assume that $z^3 = 1$. But then $\{x, y, z\}^2$ contains the 7 distinct elements $1, xy, xz, yx, y^2, yz, z^2$, and we have a contradiction. □

The proof for the $k = 4$ case follows along similar lines but is somewhat longer, primarily because of the proof of the following lemma (let D_n denote the dihedral group of order n and K_8 the quaternion group).

Lemma 2 *If x, y are noncommuting elements of a B_4-group, then $< x, y >$ is isomorphic to one of S_3, D_8, K_8, D_{10}.*

The main result follows reasonably directly from Lemma 2. Because of this, we will give the proof of Theorem 3 first and later outline the argument for Lemma 2.

Theorem 3 *A nonabelian group G is a B_4-group if and only if G is isomorphic to one of S_3, D_8, K_8, D_{10}.*

Proof of Theorem 3.
Let x, y be noncommuting elements from a nonabelian B_4-group G. Then $< x, y >$ is isomorphic to one of S_3, D_8, K_8, D_{10}. We will prove that $G =< x, y >$ in all cases.

First assume $< x, y >\cong D_8$ or D_{10}. We may also assume $x^2 = 1, y^4 = 1$ or $y^5 = 1$, and $yx = xy^{-1}$. Note that $\{x, y, xy\}^2$ contains the 8 distinct elements $1, xy, y, yx, y^2, yxy, xyx, xy^2$. Hence, if $z \notin< x, y >$ we would have 11 distinct elements in $\{x, y, xy, z\}$, giving a contradiction. So $< x, y >= G$ in this case.

Next assume $< x, y >\cong K_8$ and $x^4 = 1, y^2 = x^2, yx = xy^3$. Say $z \notin< x, y >$. We can assume that z does not commute with x (otherwise use yz). By Lemma 2, since $< x, z >$ contains an element of order 4 we know that $< x, z >\cong D_8$ or $< x, z >\cong K_8$. But if $< x, z >\cong D_8$, then $< x, z >= G$ by the previous paragraph. So we may assume $< x, z >\cong K_8$. It follows that $z^2 = x^2(= y^2)$ and $zx = xz^3$. Now $\{x, y, xy\}^2$ contains the 7 distinct elements $x^2, xy, x^2y, yx, yxy, xyx, xy^2$. Also the elements xz, yz, xyz, zx are distinct, so $\{x, y, xy, z\}^2$ has 11 distinct elements and we have a contradiction. Again $G =< x, y >$.

Finally assume that $< x, y > \cong S_3$ and $x^2 = 1, y^3 = 1, yx = xy^2$. Say $z \not\in < x, y >$. We may assume that z does not commute with x, and the only case not settled is where $< x, z > \cong S_3$. We may assume z is of order 3 (using xz if necessary), and so $zx = xz^2$. But now $\{x, y, xy, z\}^2$ contains all 6 elements of $< x, y >$ plus the 5 additional distinct elements xz, yz, xyz, z^2, zx. We again have a contradiction and conclude that $G = < x, y >$. □

Now we return to the lemma.

Proof of Lemma 2.
This argument is divided into a number of cases, depending on the orders of x and y. Initially we will consider the situation where one of the generators (say x) is of order 2.

First assume that $x^2 = 1$ and that y is of order 8. Then $\{x, y, y^2, y^3\}^2$ contains the 9 distinct elements $1, xy, xy^2, xy^3, y^2$, y^3, y^4, y^5, y^6. Hence either yx or y^3x must be equal to one of the 9 elements listed. The only possibility for yx is $yx = xy^3$ (note $yx = xy^2$ implies $y^4x = xy^8 = x$), while the only possibility for y^3x is $y^3x = xy$ (note $y^3x = xy^3$ implies $yx = xy$) and this would then give $yx = xy^3$. So yx must equal xy^3 in either case. But then $\{x, y, xy, y^2\}^2$ contains the 11 distinct elements $1, xy, y, xy^2, yx, y^2, yxy, y^3, xyxy, y^2x, y^2xy$. We have a contradiction, so this case doesn't occur.

Next assume that $x^2 = 1$ and that the order of y is greater than 6 but not equal to 8. In this case $\{x, y, y^2, y^3\}^2$ contains the 10 distinct elements $1, xy, xy^2, xy^3, yx, y^2, y^3, y^4, y^5, y^6$ (note $yx = xy^2$ implies $y = yx^2 = y^4$ while $yx = xy^3$ implies $y = y^9$). It follows that y^2x must equal one of these ten elements and the only possibilities are $y^2x = xy^2$ or $y^2x = xy^3$ (note $y^2x = xy$ implies $y = x^2y = y^4$). Similarly we must have $y^3x = xy^2$ or $y^3x = xy^3$. But $y^2x = xy^2$ and $y^3x = xy^3$ together imply $yx = xy$, while $y^2x = xy^3$ and $y^3x = xy^2$ give $y^6x = xy^9$ and $y^6x = xy^4$. Hence we obtain a contradiction and this case also cannot occur.

Now assume that $x^2 = 1$ and that y is of order 6. Hence $\{x, y, y^2, y^3\}^2$ contains the 9 distinct elements $1, xy, xy^2, xy^3, yx$, y^2, y^3, y^4, y^5. So either y^2x or y^3x must equal one of these nine elements. The only possibilities are $y^2x = xy^2$ or $y^3x = xy^3$ (for example $y^2x = xy^3$ would imply $y^4x = xy^6 = x$). But if $y^2x = xy^2$, then $\{x, y, xy, y^3\}^2$ contains the 11 distinct elements $1, xy, y, xy^3, yx, y^2$, $yxy, y^4, xy^2, y^3x, y^3xy$. Also, if $y^3x = xy^3$ then $\{x, y, xy, y^2\}^2$ contains the 11 distinct elements $1, xy, y, xy^2$, $yx, y^2, yxy, y^3, xy^3, y^2x, y^4$. Again we have a contradiction.

The next case is where $x^2 = 1$ and $y^5 = 1$. Observe that $\{x, y, xy, y^2\}^2$ contains the 10 distinct elements $1, xy, y, xy^2, yx$, y^2, yxy, y^3, xy^3, y^4 (note $yx = xy^2$ implies $y = yx^2 = y^4, xy^3 = yx$ implies $y = y^9$). Now y^2x must equal one of these elements, and the only possibility is $y^2x = xy^3$ (note $y^2x = xy$ implies $y = y^4, y^2x = xy^2$ implies $yx = xy$). But then $yx = y^6x = xy^4$, and so in this case we have $< x, y > \cong D_{10}$ which was one of the possibilities.

Next assume $x^2 = 1$ and y is of order 4. If $yx = xy^3$, then we have $< x, y > \cong D_8$, so assume this is not the case. But then similar reasoning to that seen before tells us that $\{x, y, xy, y^3\}^2$ contains the 11 distinct elements $1, xy, y, xy^3, yx, y^2, yxy, xy^2, x, y^3x$, y^3xy, and we have a contradiction.

We now assume $x^2 = 1$ and $y^3 = 1$. If $yx = xy^2$ then $< x, y > \cong S_3$, so assume that this is not the case. Then $\{x, y, xy, y^2\}^2$ contains the 10 distinct elements $1, xy, y, xy^2, yx$, y^2, yxy, x, y^2x, y^2xy. In this case, xyx and $xyxy$ must both equal elements which are already listed. But the only possibilities for xyx are $xyx = yxy$ or $xyx = y^2xy$, while the possibilities for $xyxy$ are $xyxy = yx$ or $xyxy = y^2x$. Checking case by case, we see that each combination of these possibilities leads to a contradiction.

If $x^2 = 1$ and $y^2 = 1$ then $(xy)^2 \neq 1$ (since $xy \neq yx$), so we can assume we are in one of the cases already considered.

To finish the argument, we need to handle cases where neither x nor y is of order 2.

First assume that $x^2 \neq 1, y^2 \neq 1$ and $x^2 = y^2$. If $yx = xy^3$, it will then follow that $y^3 = yx^2 = xy^3x = y^7$, so $y^4 = 1$ and $G \cong K_8$. Hence we may assume $yx \neq xy^3$. Then $\{x, x^3, y, xy\}^2$ contains the 10 distinct elements $x^2, x^4, xy, x^2y, x^3y, x^4y, yx, yx^3, yxy, xy^2$ (note $x^3 \neq 1$ since $x^2 = y^2$, also $yx^3 = xy$ implies $xyx = yx^4 = x^4y$). Hence xyx must be equal to some element in this list, and the only possiblity is $xyx = yxy$. But then xyx^3 is distinct from all elements in the list, and we have a contradiction.

Next assume that $x^2 \neq 1, y^2 \neq 1, x^2 \neq y^2$, and also that $xyx \neq y$ and $yxy \neq x$. We may also assume $(xy)^2 \neq 1$ or we would be in an earlier case. Consider the 12 elements $1, x, y, xy, x^2, x^2y, yx, y^2, yxy, xyx, xy^2, xyxy$ in $\{1, x, y, xy\}^2$. At least <u>two</u> of these must be equal to other elements in the list. However, given the conditions, the only possibilities are $yx = x^2y, yxy = x^2, xyx = yxy, xyx = y^2, xy^2 = yx, xyxy = yx$. The condition $yx = x^2y$ contradicts each of the other 5, and the same remark holds for $yx = xy^2$ and $xyxy = yx$. So we assume these do not hold. Next observe that $yxy = x^2$ and $xyx = yxy$ cannot be true at the same time, nor can $xyx = yxy$ and $xyx = y^2$. We are left with the possibility that $yxy = x^2$ and $xyx = y^2$. But in this case $\{x, y, xy, x^2\}^2$ contains the 11 distinct elements $x^2, xy, x^2y, x^3, yx, y^2, yx^2, xy^2, xyx^2, x^3y, x^4$, and so this case cannot occur.

The last set of cases all assume $x^2 \neq 1, y^2 \neq 1, x^2 \neq y^2$ and $xyx = y$. Once these possibilities have been settled, we will be finished because similar situations with $yxy = x$ are symmetrical. Note that $yx = x^{-1}y$ means that $y^nx = x^{-1}y^n$ whenever n is odd, and so forces the order of y to be even.

To begin, assume $x^2 \neq 1, y^2 \neq 1, x^2 \neq y^2, xyx = y$ and the order of y is greater than 4 but not equal to 8. Then $\{1, x, y, y^3\}^2$ contains the 11 distinct elements $1, x, y, y^3, x^2, xy, xy^3, yx, y^2, y^4, y^3x$ (note $x^2 = y^3$ implies $xy^3 = y^3x = x^{-1}y^3$, also either of $yx = xy^3, xy = y^3x$ implies that $x^2 = y^2$, also $y^4 = x^2$ implies $y^5 = yx^2 = x^{-2}y = y^{-3}$), and so this case can't occur.

Next consider the case where $x^2 \neq 1, y^2 \neq 1, x^2 \neq y^2, xyx = y$ and the order of y is 8. Now $\{1, x, y, y^3\}^2$ contains the 10 distinct elements $1, x, y, y^3, x^2, xy, xy^3, yx, y^2, y^3x$. So y^4 must be in this list, and the only possibility is $y^4 = x^2$. But then y^6 is distinct from all elements in the list, and we have a contradiction.

Finally, we assume $x^2 \neq 1, y^2 \neq 1, x^2 \neq y^2, xyx = y$ and the order of y equals 4. Then $\{x, y, xy, y^2\}^2$ contains the 9 distinct elements $x^2, xy, x^2y, xy^2, y^2, y^3, xyx, xy^3, 1$. It follows that either yx or yxy must be equal to one of the elements listed, and the only possibilities are $yx = x^2y$ or $yxy = x^2$. If $yx = x^2y$, then $x^3 = 1$ and $\{xy^2, y, x^2, x^2y\}^2$ contains the 11 distinct elements $xy^2xy^2, xy^3, xy^2x^2, xy^2x^2y, yxy^2, yx^2, yx^2y, x^2y, x, x^2y^2, x^2yx^2$ $(= x^2, xy^3, y^2, y^3, x^2y^3, xy, xy^2, x^2y, x, x^2y^2, y)$. On the other hand, if $yxy = x^2$, then $y^2 = x^3$ and $\{x, y, x^2, x^2y\}^2$ contains the 11 distinct elements $x^2, xy, x^3, x^3y, yx, yx^2, yx^2y, x^2y, x^4, x^2y^2$, x^2yx^2. So this case can't occur either.

The proof is complete. □

We will close with an example showing that Theorems 1 and 3 do not extend to the case $k = 5$. Specifically, we present a nonabelian B_5-group of order $16 > \frac{5(6)}{2}$.

Example 4.
Let $G = K_8 \times C_2$. We will show that G is a B_5-group. To do this, it will be useful to note that the center $Z(G)$ is an elementary abelian 2-group of order 4, and that one particular element of $Z(G)$, which we will denote h, has the property that $x^2 = h$ for all noncentral elements x of G. In addition, if a product xy of noncentral elements x, y is noncentral in G then $xy = yxh$.

Assume to the contrary that G is not a B_5-group. This means that we can choose distinct elements a, b, c, d, e in G such that $\{a, b, c, d, e\}^2 = G$.

Observe that each of a^2, b^2, c^2, d^2, e^2 must equal 1 or h. In particular, this means that there are at least 3 repeated products among these squares. If $a^2 = 1$ and $b^2 = 1$, then a and b would have to be central, and this would lead to 7 more repeated products in $\{a, b, c, d, e\}^2$. We now have a contradiction to $\{a, b, c, d, e\}^2 = G$ (since there are 25 products), so we can assume from now on that at most one of a, b, c, d, e is central in G.

First assume that one of these elements is central, i.e. $a^2 = 1$ and $b^2 = c^2 = d^2 = e^2 = h$. We now have 7 repeated products in $\{a, b, c, d, e\}^2$ (namely $c^2, d^2, e^2, ba, ca, da, ea$). Since $\{a, b, c, d, e\}^2 = G$ and $|Z(G)| = 4$, some product of different noncentral elements must be in $Z(G)$ and not equal to 1 or h - by relabelling if necessary we can assume bc is this product. But then $bc = cb$, so we have an eighth repeated product. In addition, some other such product must equal the fourth element of $Z(G)$, and this gives a ninth repeated product. If this product involves b or c, we would be able to construct yet another central product and would have a tenth repeated product and a contradiction (e.g.if bd is central, then so is $cd = (cb)b^2(bd)$). So the only possibility is that $de \in Z(G)$. But now $(ce)(db) = c(ed)b = (cb)(ed) = h$, since it is the product of the two elements of $Z(G)$ which are different from 1 and h. But for this to happen in G, it must be the case that either ce and db are central or $ce = db$. In either case, we have a tenth repeated product, and hence a contradiction.

We are left with the case where $a^2 = b^2 = c^2 = d^2 = e^2 = h$. So now we have 4 repeated products in $\{a, b, c, d, e\}^2$. In this situation, the three central elements other than h must all be obtainable in $\{a, b, c, d, e\}^2$. Some element in $\{a, b, c, d, e\}$ must be used twice in these products - by relabelling, we can assume ab and ac are central. But then, as seen earlier, $bc (= ba(a^2)ac)$ is also central. So now we have 7 repeated products. Since ab, ac and bc are all different, we may assume that $ab = 1$ and it follows that $b = ah$. Next observe that if ad or ae were central, then we would be able to find additional central elements as above, getting more repeated products and a contradiction. So we can assume that none of these products is central. But then $ad = dah = db, da = adh = bd, ae = eah = eb$, and again we have 10 repeated products.

This completes the proof. □

The argument in Example 4 shows that $|\{a, b, c, d, e\}^2| \leq 14$ when $G = K_8 \times C_2$. It is easy to see that the bound of 14 is best possible.

References

1. Howard E. Bell and Abraham A. Klein, On rings with redundancy in multiplication, Arch. Math. 51(1988), 500-504.

2. Howard E. Bell and Abraham A. Klein, Combinatorial commutativity and finiteness conditions for rings, preprint.

3. L. Brailovsky, A characterizatiion of abelian groups, Proc. Amer. Math Soc. 117(1993), 627-629.

4. G.A. Freiman, On two- and three-element subsets of groups, Aequationes Math. 22 (1981), 140-152.

Department of Mathematics & Statistics
Memorial University of Newfoundland
St. John's, Newfoundland, Canada
A1C 5S7