Can. J. Math., Vol. XXXII, No. 6, 1980, pp. 1299–1305

PROJECTIVE GEOMETRIES THAT ARE DISJOINT UNIONS OF CAPS

BARBU C. KESTENBAND

We show that any $PG(2n, q^2)$ is a disjoint union of $(q^{2n+1} - 1)/(q - 1)$ caps, each cap consisting of $(q^{2n+1} + 1)/(q + 1)$ points. Furthermore, these caps constitute the "large points" of a $PG(2n, q)$, with the incidence relation defined in a natural way.

A square matrix $H = (h_{ij})$ over the finite field $GF(q^2)$, q a prime power, is said to be *Hermitian* if $h_{ij}^q = h_{ji}$ for all i, j [**1**, p. 1161]. In particular, $h_{ii} \in GF(q)$. If H is Hermitian, so is $p(H)$, where $p(x)$ is any polynomial with coefficients in $GF(q)$.

Given a Desarguesian Projective Geometry $PG(2n, q^2)$, $n > 0$, we denote its points by column vectors:

$$\mathbf{x} = \begin{pmatrix} x_1 \\ x_2 \\ \cdot \\ \cdot \\ \cdot \\ x_{2n+1} \end{pmatrix}$$

All Hermitian matrices in this paper will be $2n + 1$ by $2n + 1$, $n > 0$.

Further, $A = (a_{ij})$ being any matrix, we denote $A^{(q)} = (a_{ij}^q)$.

In $PG(2n, q^2)$, the set of points $\mathbf{x}$ satisfying $\mathbf{x}^T H \mathbf{x}^{(q)} = 0$, where H is a Hermitian matrix, will be called a *Hermitian Variety* (abbreviated HV) and denoted by $\{H\}$. If H is nondegenerate, $\{H\}$ is a nondegenerate HV [**1**, p.1168].

The points $\mathbf{u}$ and $\mathbf{v}$ are said to be *conjugate* with respect to the HV $\{H\}$ if $\mathbf{u}^T H \mathbf{v}^{(q)} = 0$, or, equivalently, $\mathbf{v}^T H \mathbf{u}^{(q)} = 0$ [**1**, p. 1169].

It is convenient to denote the number of points of $PG(2n, q^2)$ and of a nondegenerate HV by m_0 and m_1, respectively:

$$m_0 = (q^{2n+1} + 1)(q^{2n+1} - 1)/(q^2 - 1)$$

By [**1**, p. 1175],

$$(1) \quad m_1 = (q^{2n+1} + 1)(q^{2n} - 1)/(q^2 - 1).$$

For convenience's sake again, we will say that the intersection of zero HV's is the whole geometry and the intersection of one HV is, of course, the HV itself.

Received November 7, 1978 and in revised form October 29, 1979.

A collection of HV's will be called *dependent* or *independent* (over $GF(q)$) according as the corresponding collection of Hermitian matrices is one or the other. By a linear combination of HV's we shall mean the obvious thing.

Let now H' be a Hermitian matrix with characteristic polynomial $p_{2n+1}'(x)$, irreducible over $GF(q)$. Since H' satisfies $p_{2n+1}'(H') = \mathbf{0}$, the polynomials $p(H')$ over $GF(q)$ form a field $GF(q^{2n+1})$. Let H be a primitive root of this field. H satisfies an irreducible equation $p_{2n+1}(H) = \mathbf{0}$ and thus $p_{2n+1}(x)$ is a fortiori its characteristic and minimal polynomial.

Let μ be a characteristic root of H. Then μ^r is a characteristic root of H^r. The smallest power of μ belonging to $GF(q)$ is the $(q^{2n+1} - 1)/(q - 1)$th. Hence the characteristic polynomials of the Hermitian matrices H^i, $i = 1, 2, \ldots, (q^{2n+1} - q)/(q - 1)$, have no roots in $GF(q)$.

Thus, if we consider the family $\chi = \{H^i: i = 0, 1, \ldots, (q^{2n+1} - q)/(q - 1)\}$, the polynomial $|H^i - \lambda H^j|$ has no roots in $GF(q)$ for any $H^i, H^j \in \chi$, $i \neq j$.

We denote by $\{\chi\}$ the collection of HV's $\{H^i\}$, $H^i \in \chi$.

LEMMA 1. *Given the independent* HV's $\{H_1\}, \ldots, \{H_m\}$, *consider the collection* Γ *of all their linear combinations with ceofficients in* $GF(q)$. *Then for any* $n \geqq m$, *the common intersection of any* n HV's *from* Γ, m *of which are independent, is the same set of points.*

Proof. The system of equations

$$\sum_{j=1}^{m} c_{ij}\mathbf{x}^T H_j \mathbf{x}^{(q)} = 0, \quad i = 1, 2, \ldots, n,$$

reduces to the system $\mathbf{x}^T H_j \mathbf{x}^{(q)} = 0$, $j = 1, 2, \ldots, m$, proving the lemma.

LEMMA 2. *Any* j *independent* HV'*s from* $\{\chi\}$, $j \leqq 2n + 1$, *intersect on* $m_j = (q^{2n+1} + 1)(q^{2n-j+1} - 1)/(q^2 - 1)$ *points.*

Proof. The lemma holds for $j = 1$, by (1). Next we prove it for $j = 2$, namely we show that in general, given any two nondegenerate Hermitian matrices H_1, H_2, such that the polynomial $|H_1 - \lambda H_2|$ has no roots in $GF(q)$, the HV's $\{H_1\}$ and $\{H_2\}$ have

$$m_2 = (q^{2n+1} + 1)(q^{2n-1} - 1)/(q^2 - 1)$$

points in common.

The $q + 1$ HV's $\{H_2\}$, $\{H_1 - \lambda H_2\}$, λ ranging through $GF(q)$, are nondegenerate by assumption. Any two of them intersect on the same set (by Lemma 1), the cardinality of which we denote m_2. Moreover, these HV's span the geometry: if $\mathbf{x}^T H_1 \mathbf{x}^{(q)} = m \neq 0$ and $\mathbf{x}^T H_2 \mathbf{x}^{(q)} = n \neq 0$, the HV $\{H_1 - (m/n)H_2\}$ contains the point $\mathbf{x}$.

These considerations lead to the equation

$$(q+1)(m_1 - m_2) + m_2 = m_0,$$

whence the desired expression for m_2.

Now we proceed by induction: We assume the lemma to be true for $j-1$ and j and show that it also holds true for $j+1$.

Let $H^{k_1}, H^{k_2}, \ldots, H^{k_{j+1}} \in \chi$ be independent, $2 \leqq j \leqq 2n$. Also let

$$A_{j-1} = \bigcap_{i=1}^{j-1} \{H^{k_i}\}, \quad A_{j+1} = \bigcap_{i=1}^{j+1} \{H^{k_i}\}.$$

By the inductive hypothesis, we have

$$|A_{j-1}| = m_{j-1} = (q^{2n+1}+1)(q^{2n-j+2}-1)/(q^2-1) \text{ and}$$
$$|A_{j-1} \cap \{H^{k_j}\}| = |A_{j-i} \cap \{H^{k_{j+1}} - \lambda H^{k_j}\}| = m_j$$
$$= (q^{2n+1}+1)(q^{2n-j+1}-1)/(q^2-1) \text{ for any } \lambda \in GF(q).$$

Any two or more of the $q+1$ HV's $\{H^{k_j}\}, \{H^{k_{j+1}} - \lambda H^{k_j}\}$, $\lambda \in GF(q)$, meet on the same set, by Lemma 1. Therefore the common intersection of A_{j-1} and any two of the above is the same set, viz. A_{j+1} defined before.

On the other hand, the $q+1$ HV's in question span the geometry and as such, their intersections with A_{j-1} span A_{j-1}. Consequently:

$$(q+1)(m_j - |A_{j+1}|) + |A_{j+1}| = m_{j-1}.$$

Denote $|A_{j+1}| = m_{j+1}$ and obtain $m_{j+1} = [(q+1)m_j - m_{j-1}]/q$. Upon substituting the values for m_{j-1} and m_j, we get:

$$m_{j+1} = (q^{2n+1}+1)(q^{2n-j}+1)/(q^2-1).$$

This completes the induction, and the proof.

LEMMA 3. *A polynomial of odd degree with coefficients in $GF(q)$ is irreducible over $GF(q)$ if and only if it is irreducible over $GF(q^2)$.*

Proof. Let $p(x)$, of odd degree, have coefficients in $GF(q)$ and be reducible over $GF(q^2)$. We will show that $p(x)$ is reducible over $GF(q)$ as well.

Let $p(x) = r(x)s(x)$, where $r(x)$ is irreducible over $GF(q^2)$. If z is a primitive root of $GF(q^2)$, one can write

$$r(x) = \sum_{i=0}^{m} z^{n_i} x^i, \quad s(x) = \sum_{i=0}^{n} z^{r_i} x^i.$$

Denote

$$r^{(q)}(x) = \sum_{i=0}^{m} z^{qn_i} x^i \quad \text{and} \quad s^{(q)}(x) = \sum_{i=0}^{n} z^{qr_i} x^i.$$

It is straightforward that $r^{(q)}(x)s^{(q)}(x) = r(x)s(x) = p(x)$. Thus

$$r^{(q)}(x) | r(x)s(x).$$

But $(r^{(q)}(x), r(x)) = 1$ (unless they are identical, in which case $r(x)$ has coefficients in $GF(q)$ and the proof is finished). Hence $r^{(q)}(x)|s(x)$, so that in fact

$$p(x) = r(x)r^{(q)}(x)t(x).$$

The polynomial $r(x)r^{(2)}(x)$ has coefficients in $GF(q)$ and even degree, hence $t(x)$ is not a constant and therefore $p(x)$ is reducible over $GF(q)$.

A *t-cap* in a geometry is a set of t points no three of which are collinear.

THEOREM. *Any* $2n$ *independent* HV'*s from* $\{\chi\}$ *intersect on a* $(q^{2n+1} + 1)/(q + 1)$-*cap and any two such caps are disjoint.*

Proof. Use Lemma 2 with $j = 2n$ to obtain the required number of points.

We turn now to proving that they constitute a cap.

First note that a line can intersect a HV in $q + 1$ points, in one point, or lies entirely in it [**1**, p. 1171].

Let $\{H^{k_1}\}, \ldots, \{H^{k_{2n+1}}\} \in \{\chi\}$ be independent (over $GF(q)$). By Lemma 2, their intersection is empty. Thus the intersection of any $2n$ of them cannot contain a complete line or that line would be disjoint from the remaining HV. We infer that the intersection of any $2n$ independent HV's from $\{\chi\}$ contains at most $q + 1$ collinear points. We will now prove a stronger statement, namely that no intersection of $2n - 1$ independent HV's from $\{\chi\}$ can contain a complete line.

Let $A = \bigcap_{i=1}^{2n-1} \{H^{k_i}\}$ contain a full line L.

A is a disjoint union of the following $q + 1$ sets:

$$A \cap \{H^{k_{2n}}\}, A \cap \{H^{k_{2n+1}} - \lambda H^{k_{2n}}\}, \lambda \text{ ranging through } GF(q).$$

L cannot intersect any of these sets at more than $q + 1$ points. Hence it must intersect $q - 1$ of them at $q + 1$ points each and the remaining two, say $A \cap \{H^{k_{2n}}\}$ and $A \cap \{H^{k_{2n+1}}\}$, at one point each. Let those two points be $\mathbf{u}$ and $\mathbf{v}$, respectively.

It is known that the line joining two points on a HV lies entirely in the HV if and only if the two points are conjugate with respect to the HV [**1**, p. 1176]. Thus $\mathbf{u}$ and $\mathbf{v}$ are conjugate with respect to $\{H^{k_i}\}$, $i = 1, 2, \ldots, 2n - 1$.

We shall now prove by contradiction that $\mathbf{u}$ and $\mathbf{v}$ are also conjugate with respect to $\{H^{k_{2n}}\}$ and $\{H^{k_{2n+1}}\}$: If they are not, we can find elements $a \in GF(q^2)$ such that the points $a\mathbf{u} + \mathbf{v} \in \{H^{k_{2n}}\}$. To achieve this, we have to solve

$$(a\mathbf{u} + \mathbf{v})^T H^{k_{2n}} (a\mathbf{u} + \mathbf{v})^{(q)} = 0.$$

Because $\mathbf{u} \in \{H^{k_{2n}}\}$, this equation reduces to

$$x + x^q = -\mathbf{v}^T H^{k_{2n}} \mathbf{v}^{(q)} \neq 0,$$

where x stands for $a\mathbf{u}^T H^{k_{2n}} \mathbf{v}^{(q)}$. The latter equation has q distinct solutions, all nonzero, so that unless $\mathbf{u}^T H^{k_{2n}} \mathbf{v}^{(q)} = 0$, L intersects $\{H^{k_{2n}}\}$ at $q + 1$ points, the sought contradiction.

Likewise we obtain $\mathbf{u}^T H^{k_{2n+1}} \mathbf{v}^{(q)} = 0$ and therefore $\mathbf{u}$ and $\mathbf{v}$ are conjugate with respect to all $\{H^{k_i}\}$, $i = 1, 2, \ldots, 2n + 1$.

It follows that the $2n + 1$ vectors $H^{k_i} \mathbf{v}^{(q)}$ cannot form a basis of the $(2n + 1)$-dimensional vector space, for if they did, we would have $\mathbf{u}^T \mathbf{w}^{(q)} = 0$ for any point $\mathbf{w}$ of the geometry, so that $\mathbf{u}$ would be the zero vector. Hence there exist $2n + 1$ elements $c_i \in GF(q^2)$, not all zero, such that the matrix

$$M = \sum_{i=1}^{2n+1} c_i H^{k_i}$$

is singular. However, M cannot be the zero matrix: If $M = \mathbf{0}$ and since the main diagonal entries of all Hermitian matrices are in $GF(q)$, we obtain a homogeneous system of equations with coefficients in $GF(q)$ and unknowns $c_1, \ldots, c_{2n+1}$. This system will have solutions in $GF(q)$, which contradicts the independence of $H^{k_1}, \ldots, H^{k_{2n+1}}$ over $GF(q)$. On the other hand, H satisfies an irreducible equation of degree $2n + 1$ over $GF(q)$, which is, by Lemma 3, irreducible over $GF(q^2)$ also, thereby generating a $GF(q^{2(2n+1)})$. Where N is a primitive root of the latter field, we have $M = N^b$ for some integer b. But N is non-singular, thus M cannot be singular and this final contradiction proves that the intersection of $2n - 1$ independent HV's from $\{\chi\}$ does not contain a whole line, but at most $q + 1$ collinear points.

It may be worth mentioning parenthetically that the present author has constructed examples where a line has exactly $q + 1$ points in common with $2n - 1$ such HV's, and still other examples with fewer common points.

Let now a line L have $y \geqq 2$ points in common with $2n$ independent HV's from $\{\chi\}$. It is an easy exercise, based on the above, to show that there are at least two HV's among the $2n$ given ones, say $\{H^{k_1}\}$ and $\{H^{k_2}\}$, none of whose linear combinations contains L.

L must have $z \geqq y$ points in common with $\{H^{k_1}\} \cap \{H^{k_2}\}$ and exactly $q + 1$ common points with each of $\{H^{k_1}\}$, $\{H^{k_2} - \lambda H^{k_1}\}$, $\lambda \in GF(q)$. These $q + 1$ HV's span the geometry on the other hand, as in the proof of Lemma 2. Thus we obtain

$$(q + 1)(q + 1 - z) + z = q^2 + 1,$$

yielding $z = 2$, hence $y = 2$ and the configuration is a cap as claimed.

It remains to be shown that no two caps meet. Each one of the two caps is the intersection of $2n$ independent HV's from $\{\chi\}$. By Lemma 1, each family of HV's contains a HV that is independent of the $2n$ HV's in the other family. But the intersection of $2n+1$ independent HV's from $\{\chi\}$ is empty, which completes the proof.

COROLLARY. *The point-set of any Desarguesian* $PG(2n, q^2)$ *is a disjoint union of* $(q^{2n+1}+1)/(q+1)$*-caps.*

Proof. Each Hermitian matrix in χ is a linear combination of the independent Hermitian matrices $I, H, H^2, \ldots, H^{2n}$. This $(2n+1)$-dimensional vector space has $(q^{2n+1}-1)/(q-1)$ distinct $2n$-dimensional subspaces.

It follows from the theorem that the $PG(2n, q^2)$ contains $(q^{2n+1}-1)/(q-1)$ pairwise disjoint caps and because of their cardinality, they exhaust the geometry.

At this point we need to introduce the following terminology: the HV's $\{H^i\} \in \{\chi\}$ will be called *large hyperplanes*, the caps obtained in the theorem we will call *large points*, the intersections of $2n-1$ independent HV's from $\{\chi\}$, *large lines* and, in general, the intersection of $2n-m$ independent HV's from $\{\chi\}$ will be an m-dimensional *large subspace*.

We show that the large points and the large lines form a $PG(2n, q)$, by checking the axioms for Projective Geometry [**2**, p. 167]:

*PG*1. We have to verify that any two large points A_1 and A_2 are contained in one and only one large line.

Among the $2n$ Hermitian Varieties whose intersection is A_1, there must be one which is independent of the $2n$ HV's whose intersection is A_2. Now the dimension theorem for vector spaces shows that one can find exactly $2n-1$ independent HV's the intersection of which contains both A_1 and A_2.

*PG*2. Let $A, B, C,$ be distinct noncollinear large points and let $D \not\equiv A$ be collinear with A, B and $E \not\equiv A$ be collinear with A, C. We have to find a large point collinear with B, C and D, E.

Let, without loss of generality:

$$A = \{H^{k_1}\} \cap \ldots \cap \{H^{k_{2n}}\};\ B = \{H^{k_1}\} \cap \ldots \cap \{H^{k_{2n-1}}\} \cap \{H^{k_{2n+1}}\};$$

$$C = \{H^{k_2}\} \cap \ldots \cap \{H^{k_{2n}}\} \cap \{H^{k_{2n+1}} + bH^{k_1}\};$$

$$\text{Line } AB = \{H^{k_1}\} \cap \ldots \cap \{H^{k_{2n-1}}\};\ \text{Line } AC = \{H^{k_2}\} \cap \ldots \cap \{H^{k_{2n}}\};$$

$$D = \{H^{k_1}\} \cap \ldots \cap \{H^{k_{2n-1}}\} \cap \{H^{k_{2n+1}} + aH^{k_{2n}}\};$$

$$E = \{H^{k_2}\} \cap \ldots \cap \{H^{k_{2n}}\} \cap \{H^{k_{2n+1}} + cH^{k_1}\},\ a, b, c \in GF(q).$$

Consequently:

$$\text{Line } BC = \{H^{k_2}\} \cap \ldots \cap \{H^{k_{2n-1}}\} \cap \{H^{k_{2n+1}} + bH^{k_1}\} \quad \text{and}$$

$$\text{Line } DE = \{H^{k_2}\} \cap \ldots \cap \{H^{k_{2n-1}}\} \cap \{H^{k_{2n+1}} + aH^{k_{2n}} + cH^{k_1}\}.$$

We see now that these two large lines intersect on the large point:

$$\{H^{k_2}\} \cap \ldots \cap \{H^{k_{2n-1}}\} \cap \{H^{k_{2n+1}} + bH^{k_1}\} \cap \{H^{k_{2n+1}} + aH^{k_{2n}} + cH^{k_1}\}.$$

*PG*3. Every large line contains at least three large points: By Lemma 2,

$$m_{2n} = (q^{2n-1} + 1)/(q + 1) \text{ and } m_{2n-1} = q^{2n+1} + 1,$$

so that

$$m_{2n-1}/m_{2n} = q + 1 \geqq 3.$$

Next we observe the following:

H is a primitive root of $GF(q^{2n+1})$, hence the matrix $H^{(q^{2n+1}-1)/(q-1)}$ is a member of the $GF(q)$ subfield consisting of scalar matrices. It follows that

$$H^{2i} = cH, c \in GF(q),$$

where

$$i = \tfrac{1}{2}(q^{2n+1} - 1)/(q - 1) + \tfrac{1}{2}.$$

The collineation $\mathscr{C}$ of $PG(2n, q^2)$ that maps each point $\mathbf{x}$ onto $H^{i^T}\mathbf{x}$, will map each HV $\{H^j\}$ onto the HV $\{H^{j-1}\}$, as can be readily checked.

Furthermore, $\mathscr{C}$ maps all large subspaces of $PG(2n, q)$ onto large subspaces; an m-dimensional large subspace, $0 \leqq m \leqq 2n$, is the intersection of the independent HV's $\{H^{k_1}\}, \ldots, \{H^{k_{2n-m}}\}$ (and of their linear combinations, by Lemma 1).

Let $\mathbf{x} \in \{H^{k_1}\} \cap \ldots \cap \{H^{k_{2n-m}}\}$. Then

$$H^{i^T}\mathbf{x} \in \{H^{k_1-1}\} \cap \ldots \cap \{H^{k_{2n-m}-1}\}.$$

But multiplication of $H^{k_1}, \ldots, H^{k_{2n-m}}$, by H^{-1}, does not affect their linear independence and hence the latter intersection is also an m-dimensional large subspace.

Thus we conclude that $\mathscr{C}$ is a collineation of the $PG(2n, q)$, too.

Remark. The exponents of H in the $(q^{2n} - 1)/(q - 1)$ linear combinations of any $2n$ independent Hermitian matrices from χ (two Hermitian matrices are considered identical, of course, if they differ by a factor in $GF(q)$) form a perfect difference set, as in the theorem of James Singer [**3**].

REFERENCES

1. R. C. Bose and I. M. Chakravarti, *Hermitian varieties in a finite projective space* $PG(N, q^2)$, Can. J. Math. *17* (1966), 1161–1182.

2. M. Hall, Jr., *Combinatorial theory* (Blaisdell, 1967).

3. J. Singer, *A theorem in finite projective geometry and some applications to number theory*, Trans. Amer. Math. Soc. *43* (1938), 377–385.

New York Institute of Technology,
Old Westbury, New York