Can. J. Math., Vol. XXXIII, No. 2, 1981, pp. 500–512

# HERMITIAN CONFIGURATIONS IN ODD-DIMENSIONAL PROJECTIVE GEOMETRIES

BARBU C. KESTENBAND

A *t-cap* in a geometry is a set of $t$ points no three of which are collinear. A $(t, k)$-cap is a set of $t$ points, no $k + 1$ of which are collinear.

It has been shown in [**3**] that any Desarguesian $PG(2n, q^2)$ is a disjoint union of $(q^{2n+1} - 1)/(q - 1)$ $(q^{2n+1} + 1)/(q + 1)$-caps. These caps were obtained as intersections of $2n$ Hermitian Varieties of a certain kind; the intersection of $2n + 1$ such varieties was empty. Furthermore, the caps in question constituted the "large points" of a $PG(2n, q)$, with the incidence relation defined in a natural way.

It seemed at the time that nothing similar could be said about odd-dimensional projective geometries, if only because $|PG(2n - 1, q)| \nmid |PG(2n - 1, q^2)|$.

Closer investigation shows, however, that in $PG(2n - 1, q^2)$, the intersection of $2n$ Hermitian Varieties of a suitable kind has cardinality $2|PG(n - 1, q^2)|$; besides, $|PG(2n - 1, q)|$ does divide $|PG(2n - 1, q^2)| - 2|PG(n - 1, q^2)|$.

Thus it turns out that by removing two disjoint subspaces $PG(n - 1, q^2)$ from a $PG(2n - 1, q^2)$, what is left behaves more or less as a $PG(2n, q^2)$ does, in the sense that it can be partitioned into caps (see the statement of the Theorem below) and it can be also viewed as a $PG(2n - 1, q)$ the "large points" of which, however, are not the caps that appear in the theorem (except in the case $q = 2$), but $((q^{2n} - 1)/(q + 1), q - 1)$-caps obtained as unions of $q - 1$ $(q^{2n} - 1)/(q^2 - 1)$-caps.

The main purpose of the present paper is therefore to prove the following:

THEOREM. *Given any two disjoint subspaces $PG(n - 1, q^2)$ of a $PG(2n - 1, q^2)$, the point-set of the latter is a disjoint union of the former and of $q^{2n} - 1$ $(q^{2n} - 1)/(q^2 - 1)$-caps.*

Many terms and symbols in the present paper are the same as in [**3**]. We have avoided repetitions whenever we could, with a view, however, to making the present paper as self-contained as possible.

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 $i, j$ [**2**, p. 1161]. In

Received January 15, 1980.

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 projective geometry $PG(2n - 1, q^2)$, $n \geqq 2$, we denote its points by column vectors:

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

We shall use "point" and "vector" interchangeably.

All matrices in this paper will be $2n$ by $2n$, $n \geqq 2$.

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

In $PG(2n - 1, q^2)$, 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 $\{H\}$. The HV $\{cH\}$ is the same as $\{H\}$, as long as $c \neq 0$. If $H$ is nondegenerate, $\{H\}$ is a nondegenerate HV [**2**, 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, $\mathbf{v}^T H \mathbf{u}^{(q)} = 0$ [**2**, p. 1169]. We will say that $\mathbf{u}$ is conjugate with a set of points with respect to $\{H\}$, if $\mathbf{u}$ is conjugate with all points in that set, with respect to $\{H\}$.

It is convenient to denote the number of points of $PG(2n - 1, q^2)$ and of a nondegenerate HV by $m_0$ and $m_1$, respectively:

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

By [**2**, p. 1175],

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

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.

A collection of HV's will be called dependent or independent 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 $p_{2n}'(x)$, irreducible over $GF(q)$. Since $H'$ satisfies $p_{2n}'(H') = \mathbf{0}$, the polynomials $p(H')$ over $GF(q)$ form a shield $GF(q^{2n})$. Let $H$ be a primitive root of this field. $H$ satisfies an irreducible equation $p_{2n}(H) = \mathbf{0}$ and thus $p_{2n}(x)$ is a fortiori its characteristic and minimal polynomial.

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

Thus, if we consider the family $\chi = \{H^i : i = 1, 2, \ldots, (q^{2n} - 1)/(q - 1)\}$, 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. *Any polynomial of degree divisible by $m$, with coefficients in $GF(q)$, is reducible over $GF(q^m)$.*

*Proof.* Let $f(x)$, of degree $mn$, with coefficients in $GF(q)$, be irreducible over $GF(q)$. Then $f(x)$ generates a $GF(q^{mn})$ in which it has $mn$ distinct roots $a^{q^i}$, $i = 0, 1, \ldots, mn - 1$. All the $m$ polynomials of degree $n$,

$$p_j(x) = (x - a^{q^j})(x - a^{q^{j+m}}) \ldots (x - a^{q^{j+(n-1)m}}),$$
$$j = 0, 1, \ldots, m - 1,$$

have coefficients in the subfield $GF(q^m)$. On the other hand, given two fields $GF(q^m)$, there is always an isomorphism between them which fixes each element of $GF(q)$ and this completes the proof.

If $p(x) = \sum_{i=0}^{n} a_i x^i$, we denote $p^{(q)}(x) = \sum_{i=0}^{n} a_i^q x^i$.

COROLLARY 1. *Let $f(x)$ be a polynomial of degree $2n$ with coefficients in, and irreducible over, $GF(q)$. Then $f(x) = r_n(x) r_n^{(q)}(x)$, where $r_n$, $r_n^{(q)}$ have degree $n$, coefficients in $GF(q^2)$, and are irreducible over $GF(q^2)$.*

*Proof.* $f(x)$ is reducible over $GF(q^2)$ by Lemma 1. If $r_n(x)$ is reducible over $GF(q^2)$, then $r_n(x) = s(x)t(x)$ and it follows that

$$r_n^{(q)}(x) = s^{(q)}(x) t^{(q)}(x).$$

But $s(x)s^{(q)}(x)$ will have coefficients in $GF(q)$ and thus $f(x)$ will be reducible over $GF(q)$, a contradiction.

The following lemma is actually Lemma 1 in [**3**].

LEMMA 2. *Given the independent* HV'*s* $\{H_1\}, \ldots, \{H_m\}$, *consider the collection $\Gamma$ of all their linear combinations with coefficients in $GF(q)$. Then for any $n \geqq m$, the common intersection of any $n$* HV'*s from $\Gamma$, $m$ of which are independent, is the same set of points.*

The proof of the next lemma is quite similar to that of Lemma 2 in [**3**], so we omit it.

LEMMA 3. *Any $j$ independent* HV'*s from $\{\chi\}$, $j \leqq 2n$, intersect on $m_j = (q^{2n} - 1)(q^{2n-j} + 1)/(q^2 - 1)$ points.*

LEMMA 4. *For any number $N \geqq 2n$, the intersection of $N$* HV'*s from $\{\chi\}$, exactly $2n$ of which are independent, consists of two disjoint projective subgeometries $PG(n - 1, q^2)$.*

*Proof.* Since $\chi$, as a vector space, has dimension $2n$, what this lemma actually says is that the common intersection of all HV's in $\{\chi\}$ is a disjoint union of two $PG(n-1, q^2)$. Proceeding to the proof, we first remark that the intersection in question contains

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

points, which is the required number of points.

Let $\mathbf{u}$ be a point in the intersection. Then

$$\mathbf{u}^T\mathbf{u}^{(q)} = \mathbf{u}^T H\mathbf{u}^{(q)} = \ldots = \mathbf{u}^T H^{2n-1}\mathbf{u}^{(q)} = 0.$$

This shows that the vectors $\mathbf{u}^{(q)}, H\mathbf{u}^{(q)}, \ldots, H^{2n-1}\mathbf{u}^{(q)}$, cannot form a basis for the $2n$-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 and thus $\mathbf{u}$ would be the zero vector.

Therefore there exist elements $c_0, c_1, \ldots, c_{2n-1} \in GF(q^2)$ such that

$$(c_0 I + c_1 H + \ldots + c_{2n-1}H^{2n-1})\mathbf{u}^{(q)} = \mathbf{0},$$

i.e., the matrix

$$p_{2n-1}(H) = c_0 I + c_1 H + \ldots + c_{2n-1}H^{2n-1}$$

is singular and so is

$$p_{2n-1}^{(q)}(H) = c_0{}^q I + c_1{}^q H + \ldots + c_{2n-1}^q H^{2n-1}.$$

It follows that the singular matrix $p(H) = p_{2n-1}(H)p_{2n-1}^{(q)}(H)$, of even degree (at most $4n-2$), must be the zero matrix: if it is not, it must be (up to a multiplicative constant) a member of $\chi$, because $p(x)$ has coefficients in $GF(q)$. But no matrix in $\chi$ is singular.

Hence $p(H) = p_{2n}(H)s(H)$, where $p_{2n}$ is the minimal and characteristic polynomial of $H$. By Corollary 1, $p_{2n}(H) = r_n(H)r_n{}^{(q)}(H)$, $r_n$, $r_n{}^{(q)}$ irreducible over $GF(q^2)$; then $s(H)$ has even degree (at most $2n-2$) and coefficients in $GF(q)$. By Lemma 1,

$$s(H) = s_{n-1}(H)s_{n-1}{}^{(q)}(H).$$

Therefore:

$$(1) \quad p(H) = [r_n(H)r_n{}^{(q)}(H)][s_{n-1}(H)s_{n-1}{}^{(q)}(H)].$$

This implies that $p_{2n-1}(H)$ is a product of two factors, one from each square bracket of (1). On the other hand, $s_{n-1}(H)$ (and $s_{n-1}{}^{(q)}(H)$ as well) are not singular: $s(x)$ being of degree less than $2n$, $s(H)$ cannot be the zero matrix, thus $s(H) \in \chi$ (up to a multiplicative constant) and it is not singular.

This enables us to conclude that $p_{2n-1}(H)\mathbf{u}^{(q)} = \mathbf{0}$ implies

$$r_n(H)\mathbf{u}^{(q)} = \mathbf{0} \quad \text{or} \quad r_n{}^{(q)}(H)\mathbf{u}^{(q)} = \mathbf{0}.$$

We have thus far shown that the intersection of $2n$ independent HV's from $\{\chi\}$ must belong to the union of the null spaces of $r_n(H)$ and $r_n{}^{(q)}(H)$.

To complete the proof, we will now show that the null space of each of $r_n(H)$ and $r_n^{(q)}(H)$ is a $PG(n-1, q^2)$. To this end it suffices to prove that $r_n(H)$ and $r_n^{(q)}(H)$ have nullity $n$.

We will denote the rank and nullity of a matrix $A$ by $\rho(A)$ and $\nu(A)$.

We have $\rho(r_n(H)) = \rho(r_n^{(q)}(H))$ and $\nu(r_n(H)) = \nu(r_n^{(q)}(H))$.

In the sequel, $\theta$ will always stand for the number $(q^{2n} - 1)/(q^2 - 1)$.

Consider the subfield $GF(q^2)$ of our $GF(q^{2n})$, consisting of the zero matrix and $H^{i\theta}$, $i = 1, 2, \ldots, q^2 - 1$ (we remind the reader that $H$ is a primitive root of $GF(q^{2n})$). $H^\theta$ is a primitive root of this $GF(q^2)$. As such, $H^\theta$ satisfies $g(H^\theta) = \mathbf{0}$, where $g$, of degree two in $H^\theta$, is the irreducible (over $GF(q)$) minimal polynomial of $H^\theta$.

Let $g(H^\theta) = (H^\theta - aI)(H^\theta - a^qI)$, $a, a^q \in GF(q^2) - GF(q)$.

$H^\theta$ is a linear combination of $I, H, \ldots, H^{2n-1}$. Thus

$$g(H^\theta) = t_{2n-1}(H)t_{2n-1}^{(q)}(H) = \mathbf{0},$$

where $t_{2n-1}(H) = H^\theta - aI$, $t_{2n-1}^{(q)}(H) = H^\theta - a^qI$.

Therefore

$$r_n(H)r_n^{(q)}(H)|t_{2n-1}(H)t_{2n-1}^{(q)}(H).$$

But $r_n(H)$ and $r_n^{(q)}(H)$ are irreducible over $GF(q^2)$, hence $r_n(H)|t_{2n-1}(H)$, say, and $r_n^{(q)}(H)|t_{2n-1}^{(q)}(H)$.

Thus $r_n(H)\mathbf{u}^{(q)} = \mathbf{0}$ implies $t_{2n-1}(H)\mathbf{u}^{(q)} = \mathbf{0}$, i.e., $H^\theta\mathbf{u}^{(q)} = a\mathbf{u}^{(q)}$. Likewise, $r_n^{(q)}(H)\mathbf{v}^{(q)} = \mathbf{0}$ implies $H^\theta\mathbf{v}^{(q)} = a^q\mathbf{v}^{(q)}$ and this shows that $\mathbf{u} \neq c\mathbf{v}$. Thus the null spaces of $r_n(H)$ and $r_n^{(q)}(H)$ share no common vectors, which implies

$$\nu(r_n(H)) = \nu(r_n^{(q)}(H)) \leqq n.$$

On the other hand, by Sylvester's law of nullity [**1**, p. 221], we have

$$\nu(r_n(H)) + \nu(r_n^{(q)}(H)) \geqq 2n$$

and we conclude that

$$\nu(r_n(H)) = \nu(r_n^{(q)}(H)) = \rho(r_n(H)) = \rho(r_n^{(q)}(H)) = n$$

and the proof is finished.

We shall henceforth denote by $\Pi_1$ and $\Pi_2$ the two disjoint $PG(n-1, q^2)$ that appear in the above lemma.

$$\mathbf{u} \in \Pi_1 \Leftrightarrow r_n(H)\mathbf{u}^{(q)} = \mathbf{0} \quad \text{and} \quad \mathbf{v} \in \Pi_2 \Leftrightarrow r_n^{(q)}(H)\mathbf{v}^{(q)} = \mathbf{0}.$$

Let $\mathbf{u} \in \Pi_1$. Then

$$r_n(H)(H^T\mathbf{u})^{(q)} = r_n(H)H\mathbf{u}^{(q)} = Hr_n(H)\mathbf{u}^{(q)} = \mathbf{0},$$

i.e., $H^T\mathbf{u} \in \Pi_1$ and therefore $H^{T^i}\mathbf{u} \in \Pi_1$ for any integer $i$. But we have seen before that:

$$(2) \quad H^\theta\mathbf{u}^{(q)} = a\mathbf{u}^{(q)}, \quad \text{i.e.,} \quad H^{T^\theta}\mathbf{u} = a^q\mathbf{u}$$

https://doi.org/10.4153/CJM-1981-043-7 Published online by Cambridge University Press

and this shows that $\Pi_1$ consists of the $\theta$ distinct points $H^{T^i}\mathbf{u}$, $i = 0, 1, \ldots, \theta - 1$.

Likewise, if $\mathbf{v} \in \Pi_2$, we have:

$$(3) \quad H^\theta \mathbf{v}^{(q)} = a^q \mathbf{v}^{(q)} \quad \text{and} \quad H^{T^\theta}\mathbf{v} = a\mathbf{v}$$

hence $\Pi_2$ consists of the $\theta$ distinct points $H^{T^i}\mathbf{v}$, $i = 0, 1, \ldots, \theta - 1$.

At this point we need the following fact which becomes crucial in the sequel: the line joining two points on a HV $\{H\}$ is completely contained in $\{H\}$ if and only if the two points are conjugate with respect to $\{H\}$ [**2**, p. 1176].

LEMMA 5. *Given a Hermitian matrix $H^j \in \chi$, there is a one to one correspondence between the points of $\Pi_1$ (or $\Pi_2$) and the $(n - 2)$-dimensional subspaces of $\Pi_2$ (or $\Pi_1$), in which each such subspace is conjugate with the corresponding point, with respect to all* HV'*s* $\{H^{j+k\theta}\}$, $k = 1, 2, \ldots, q^2 - 1$.

*Proof*. First, if $\mathbf{u} \in \Pi_1$ and $\mathbf{v} \in \Pi_2$ are conjugate with respect to $\{H^j\}$, they are also conjugate with respect to $\{H^{j+k\theta}\}$ for any $k$, because of (2) and (3).

Second, all points in $\Pi_2$ that are conjugate with $\mathbf{u} \in \Pi_1$ with respect to $\{H^j\}$ form a subspace, call it $\Sigma$, of $\Pi_2$. Furthermore, $\Sigma \not\equiv \Pi_2$: if $\mathbf{u}^T H^j \mathbf{v}^{(q)} = 0$ for any $\mathbf{v} \in \Pi_2$, then the $PG(n, q^2)$ containing $\mathbf{u}$ and $\Pi_2$ is completely included in $\{H^j\}$. But [**2**, p. 1176] a nondegenerate HV in a $PG(2n - 1, q^2)$ cannot contain subspaces of higher dimension than $n - 1$.

On the other hand, any line in $\Pi_2$ contains at least one point that is conjugate with $\mathbf{u}$: if $\mathbf{v}, \mathbf{w} \in \Pi_2$ with $\mathbf{u}^T H^j \mathbf{v}^{(q)} = r \neq 0, \mathbf{u}^T H^j \mathbf{w}^{(q)} = s \neq 0$, then $\mathbf{u}^T H^j \mathbf{x}^{(q)} = 0$, where $\mathbf{x} = \mathbf{v} - (r/s)^q \mathbf{w}$.

Now, since the only proper subspaces of $\Pi_2$ that intersect all its lines are the subgeometries $PG(n - 2, q^2)$, we conclude that $\Sigma$ is such a subgeometry. The point $\mathbf{u}$ cannot be conjugate with any other subgeometry of $\Pi_2$, or it would be conjugate with the whole of $\Pi_2$, a contradiction.

Assume now that $\mathbf{y} \in \Pi_1$ is also conjugate with $\Sigma$, with respect to $\{H^j\}$; $\mathbf{y}$ and $\Sigma$ determine a $PG(n - 1, q^2)$, denote it $\Sigma'$. The $n$-dimensional geometry determined by $\mathbf{u}$ and $\Sigma'$ is contained in $\{H^j\}$, a contradiction, and this completes the proof.

Given $\mathbf{u} \in \Pi_1$ and $H^j \in \chi$, the conjugate subspace of $\mathbf{u}$ consists precisely of those points $\mathbf{v} \in \Pi_2$ that satisfy $\mathbf{v}^T H^j \mathbf{u}^{(q)} = 0$. Thus, if $\mathbf{u}$ is conjugate with $\mathbf{v}$ with respect to $\{H^j\}$, then $H^{T^i}\mathbf{u}$ is conjugate with $H^{T^{\theta-i}}\mathbf{v}$, with respect to the same $\{H^j\}$. Therefore, given any $(n - 2)$-dimensional subspace of $\Pi_2$, say $\Sigma$, the subspaces $H^{T^i}\Sigma$, $i = 0, 1, \ldots, \theta - 1$, are all the $(n - 2)$-dimensional subspaces of $\Pi_2$. Here $H^{T^i}\Sigma$ means multiplication of each point of $\Sigma$ by $H^{T^i}$.

https://doi.org/10.4153/CJM-1981-043-7 Published online by Cambridge University Press

We next note that given any point $\mathbf{u} \in \Pi_1$ and any $(n-2)$-dimensional subspace $\Sigma$ of $\Pi_2$, there is a unique number $j$ modulo $\theta$ such that $\mathbf{u}$ is conjugate with $\Sigma$, with respect to all HV's $\{H^{j+k\theta}\}$, $k = 1, 2, \ldots, q^2 - 1$: $\mathbf{u}$ is conjugate with respect to $\{I\}$, with an $(n-2)$-dimensional subspace $\hat{\Sigma}$. But $\Sigma = H^{T^i}\hat{\Sigma}$ for some fixed $i \in \{0, 1, \ldots, \theta - 1\}$, hence the sought $j$ is simply $-i \pmod{\theta}$.

At this point, in order to establish Lemma 6, we need James Singer's Theorem [**4**]. Let $x$ be a primitive root of a $GF(q^n)$. Then $x^i = a_0 + a_1 x + \ldots + a_{n-1}x^{n-1}$, $a_i \in GF(q)$. There are $q^n - 1$ different powers $x^i$, or, if we do not distinguish between $x^i$ and $cx^i$, $c \in GF(q)$, there are $(q^n - 1)/(q-1)$ different powers $x^i$.

Consider the $GF(q^n)$ as an $n$-dimensional vector space $V$, the vectors being $\mathbf{v} = (a_0, a_1, \ldots, a_{n-1})$; again, we do not distinguish between $\mathbf{v}$ and $c\mathbf{v}$, $c \in GF(q)$. We now set up a one to one correspondence between the set of numbers $\{1, 2, \ldots, (q^n - 1)/(q - 1)\}$ and the vectors $\mathbf{v}$, as follows: $i \leftrightarrow \mathbf{v}$ if the coefficients of $1, x, \ldots, x^{n-1}$ in the expression of $x^i$ are the components of $\mathbf{v}$.

What Singer's Theorem essentially says is the following: consider any $(n-1)$-dimensional subspace of $V$, consisting, of course, of $(q^{n-1} - 1)/(q-1)$ vectors. The $(q^{n-1} - 1)/(q - 1)$ numbers $i$ that correspond to these vectors form a $(v, k, \lambda)$-difference set, where

$$v = (q^n - 1)/(q-1), \quad k = (q^{n-1} - 1)/(q-1),$$
$$\lambda = (q^{n-2} - 1)/(q-1).$$

Now we are prepared for the next lemma, which together with Lemma 2 shows that the intersection of any $2n - 1$ independent HV's from $\{\chi\}$ is the same as the intersection of a special family of $2n - 1$ independent HV's, and this simplifies the problem, as will be seen later (Lemma 8 and Corollary 2).

LEMMA 6. *Given any $2n - 1$ independent Hermitian matrices in $\chi$, the vector space they span has a basis*

$$\{H^{i_0}, H^{i_1}, H^{i_1+\theta}, \ldots, H^{i_{n-1}}, H^{i_{n-1}+\theta}\}, \ i_r \not\equiv i_s \bmod \theta \textit{ for } r \neq s.$$

*Proof.* By Singer's Theorem, the exponents of $H$ in the $(q^{2n-1} - 1)/(q - 1)$ linear combinations over $GF(q)$, of any $2n - 1$ independent Hermitian matrices in $\chi$, form a $(v, k, \lambda)$-difference set $D$, where

$$v = (q^{2n} - 1)/(q-1), \quad k = (q^{2n-1} - 1)/(q-1),$$
$$\lambda = (q^{2n-2} - 1)/(q-1).$$

In the difference set $D$, the difference $\theta$ appears $\lambda$ times, just like any other. Let $i, i + \theta \in D$. This implies that $i + j\theta \in D$ for all $j = 0, 1, \ldots, q$, because given $H^i, H^{i+\theta} \in \chi$, the exponents of all their linear combinations must be in $D$, but all their linear combinations are of form $cH^{i+j\theta}$, $c \in GF(q)$, this last fact being so because $H^\theta$ is a primitive root of the subfield $GF(q^2)$. These $q+1$ numbers $i+j\theta$ account for $q+1$ differences $\theta$. Therefore there must be in $D$, $\lambda/(q+1) = (q^{2n-2}-1)/(q^2-1)$ such cycles of length $q+1$.

The number $(q^{2n-2}-1)/(q^2-1)$ will be denoted $\tau$ in the sequel.

We have thus shown that all the $\lambda$ differences $\theta$ appear within the following subsets of $D$:

$$D_r = \{i_r, i_r+\theta, \ldots, i_r+q\theta\}, \quad r = 1, 2, \ldots, \tau.$$

Let $H_1 = H^{i_s+j\theta}$, $H_2 = H^{i_t+k\theta}$. The exponents of $H$ in $aH_1 + bH_2$ and in $aH^\theta H_1 + bH^\theta H_2$ differ by $\theta$ and this shows that the subset $\chi' \subset \chi$ defined as

$$\chi' = \left\{H^j : j \in \bigcup_{r=1}^{\tau} D_r\right\}$$

is a subspace of $\chi$; since its cardinality is $(q^{2n-2}-1)/(q-1)$, $\chi'$ must have dimension $2n-2$.

We now want to prove that after a possible renumbering of the $D_r$'s, the matrices $H^{i_1}, H^{i_1+\theta}, \ldots, H^{i_{n-1}}, H^{i_{n-1}+\theta}$ constitute a basis for $\chi'$. To this end, if we regard the $GF(q^{2n})$ as a $GF((q^2)^n)$, we can express any $H^j \in \chi'$ as a linear combination of $I, H, \ldots, H^{n-1}$, with coefficients in $GF(q^2)$, these coefficients being matrices of form $aI + bH^\theta$, $a, b \in GF(q)$. In this setting no distinction is being made between $H^{i_r}$ and $H^{i_r+j\theta}$. Thus $\chi'$ reduces to the vector space (over $GF(q^2)$) $\chi'' = \{H^{i_1}, H^{i_2}, \ldots, H^{i_\tau}\}$. Because $\tau = (q^{2n-2}-1)/(q^2-1)$, $\chi''$ has dimension $n-1$ (over $GF(q^2)$). Let, without loss of generality, a basis of $\chi''$ be $\{H^{i_1}, \ldots, H^{i_{n-1}}\}$. Now $\{H^{i_1}, H^{i_1+\theta}, \ldots, H^{i_{n-1}}, H^{i_{n-1}+\theta}\}$ is a basis of $\chi'$, for if not, one could find $n-1$ matrices of the form

$$C_s = a_sI + b_sH^\theta, \quad s = 1, 2, \ldots, n-1, a_s, b_s \in GF(q), C_s \in GF(q^2),$$

such that

$$\sum_{s=1}^{n-1} C_s H^{i_s} = \mathbf{0}$$

and this is not possible.

Extend now this basis of $\chi'$ to a basis of $\chi$ to complete the proof.

LEMMA 7. *Given two disjoint subgeometries $PG(n-1, q^2)$ of a $PG(2n-1, q^2)$, the lines that intersect both subgeometries contain among themselves all the points of the geometry and no two such lines meet outside the two subgeometries.*

*Proof.* Let the two subgeometries be $x_1 = \ldots = x_n = 0$ and $x_{n+1} =$

https://doi.org/10.4153/CJM-1981-043-7 Published online by Cambridge University Press

$\ldots = x_{2n} = 0$. Any point of $PG(2n-1, q^2)$ is evidently contained in a line that intersects both subgeometries.

There are $(q^{2n}-1)^2/(q^2-1)^2$ such lines, hence containing $(q^{2n}-1)^2/(q^2-1)$ points outside the two subgeometries. But this is the total number of points outside said subgeometries and as such no two lines intersect outside them.

We shall denote by $\Lambda$ the collection of lines that intersect $\Pi_1$ and $\Pi_2$:

$$\Lambda = \{L: |L \cap \Pi_1| = |L \cap \Pi_2| = 1\}.$$

LEMMA 8. *Let* $P_k = \{H^{i_1}\} \cap \{H^{i_1+\theta}\} \cap \ldots \cap \{H^{i_k}\} \cap \{H^{i_k+\theta}\}$, *the* $2k$ HV'*s being independent*, $1 \leqq k \leqq n-1$. *Then* $P_k$ *is a union of* $\theta$ $(n-k)$-*dimensional subspaces that are mutually disjoint outside* $\Pi_1 \cup \Pi_2$.

*Proof.* By Lemma 3, $P_k$ contains $|P_k| = m_{2k} = (q^{2n}-1)(q^{2n-2k}+1)/(q^2-1)$ points.

Let $\mathbf{u} \in \Pi_1$. By Lemma 5, one finds $k$ $(n-2)$-dimensional subspaces of $\Pi_2$, namely $\Sigma_1, \ldots, \Sigma_k$, such that $\mathbf{u}$ is conjugate with $\Sigma_r$, with respect to $\{H^{i_r}\}$ and $\{H^{i_r+\theta}\}$, $r = 1, \ldots, k$.

$\Sigma_r$ consists precisely of those points $\mathbf{v} \in \Pi_2$ that satisfy

$$\mathbf{v}^T H^{i_r} \mathbf{u}^{(q)} = 0.$$

Then $\bigcap_{r=1}^k \Sigma_r$ has dimension at least $n-k-1$, because a homogeneous system of $n+k$ equations with $2n$ unknowns has at least $n-k$ nontrivial solutions.

Let $\tilde{\Sigma} \subseteq \bigcap_{r=1}^k \Sigma_r$ have dimension $n-k-1$. For any $\mathbf{v} \in \tilde{\Sigma}$, the line $[\mathbf{u}, \mathbf{v}]$ is contained in all HV's $\{H^{i_r}\}$, $\{H^{i_r+\theta}\}$, $r = 1, \ldots, k$, and hence so are all lines $[H^{T^i}\mathbf{u}, H^{T^{\theta-i}}\mathbf{v}]$, $i = 0, 1, \ldots, \theta-1$. Thus $P_k$ contains $\theta$ $(n-k)$-dimensional subspaces, which are also mutually disjoint outside $\Pi_1 \cup \Pi_2$, by Lemma 7. A straightforward counting argument shows that these $\theta$ subspaces contain $m_{2k}$ points among themselves, i.e., $P_k$ consists precisely of these subspaces and $\tilde{\Sigma} = \bigcap_{r=1}^k \Sigma_r$.

COROLLARY 2. *Let* $\{H^{i_1}\}, \{H^{i_1+\theta}\}, \ldots, \{H^{i_{n-1}}\}, \{H^{i_{n-1}+\theta}\}$ *be independent* HV'*s from* $\{\chi\}$. *Their intersection consists of* $\theta$ *mutually disjoint lines*

$$[H^{T^i}\mathbf{u}, H^{T^{\theta-i}}\mathbf{v}] \in \Lambda, H^{T^i}\mathbf{u} \in \Pi_1, H^{T^{\theta-i}}\mathbf{v} \in \Pi_2, i = 0, 1, \ldots, \theta-1.$$

LEMMA 9. *The intersection of any* $2n-1$ *independent* HV'*s from* $\{\chi\}$ *consists of* $\theta$ *mutually disjoint sets of* $q+1$ *collinear points.*

*Proof.* By Lemmas 2 and 6 and Corollary 2, the intersection in question is actually the intersection of $\{H^{i_0}\}$ and $\theta$ mutually disjoint lines $[H^{T^i}\mathbf{u}, H^{T^{\theta-i}}\mathbf{v}]$, $i = 0, 1, \ldots, \theta-1$.

We will show that each of these lines intersects $\{H^{i_0}\}$ at $q-1$ points outside $\Pi_1 \cup \Pi_2$: the equation

$$(4) \quad (\mathbf{u} + cH^{T^\theta}\mathbf{v})^T H^{i_0} (\mathbf{u} + cH^{T^\theta}\mathbf{v})^{(q)} = 0$$

reduces, by (2) and (3), to

$$c(a\mathbf{v}^T H^{i_0}\mathbf{u}^{(q)}) + c^q(a\mathbf{v}^T H^{i_0}\mathbf{u}^{(q)})^q = 0,$$

which yields $q - 1$ distinct nonzero values for $c$. Furthermore, (4) is equivalent to

$$(H^{T^i}\mathbf{u} + cH^{T^{\theta-i}}\mathbf{v})^T H^{i_0}(H^{T^i}\mathbf{u} + cH^{T^{\theta-i}}\mathbf{v})^{(q)} = 0, \quad \text{for any } i.$$

Thus the intersection of any $2n - 1$ independent HV's from $\{\chi\}$ is made up of $\theta$ sets of $q + 1$ collinear points:

$$\{H^{T^i}\mathbf{u}, H^{T^{\theta-i}}\mathbf{v}, H^{T^i}\mathbf{u} + c_1H^{T^{\theta-i}}\mathbf{v}, \dots, H^{T^i}\mathbf{u} + c_{q-1}H^{T^{\theta-i}}\mathbf{v}\},$$
$$i = 0, 1, \dots, \theta - 1.$$

Our next goal is to demonstrate that the intersection of $2n - 1$ independent HV's from $\{\chi\}$ does not possess, outside $\Pi_1 \cup \Pi_2$, any three collinear points, except those that appear in Lemma 9. To this end we need several more lemmas.

LEMMA 10. *A line $L$ such that $|L \cap (\Pi_1 \cup \Pi_2)| = 1$ cannot have more than two points in common with the set*

$$P_{n-1} = \{H^{i_1}\} \cap \{H^{i_1+\theta}\} \cap \dots \cap \{H^{i_{n-1}}\} \cap \{H^{i_{n-1}+\theta}\},$$

*where the $2n - 2$ HV's are independent.*

*Proof.* Let $L \cap (\Pi_1 \cup \Pi_2) = \{\mathbf{u}\}, \mathbf{u} \in \Pi_1$, and let $\mathbf{w} \in L \cap P_{n-1}$, $\mathbf{w} \not\equiv \mathbf{u}$. By Corollary 2 one can find two points $\mathbf{x} \in \Pi_1$, $\mathbf{y} \in \Pi_2$, $\mathbf{x} \not\equiv \mathbf{u}$, such that $\mathbf{w}$, $\mathbf{x}$, $\mathbf{y}$, are collinear. Let $\mathbf{x}_1, \mathbf{x}_2, \dots, \mathbf{x}_{q^2-1}$ be the remaining points on the line $[\mathbf{u}, \mathbf{x}]$. Then

$$L \cap [\mathbf{y}, \mathbf{x}_j] = \{\mathbf{t}_j\}, \quad \mathbf{t}_j \not\equiv \mathbf{t}_k \quad \text{for } j \neq k.$$

The points $\mathbf{t}_j \notin P_{n-1}$ for any $j$, by Corollary 2 and Lemma 7.

LEMMA 11. *If a line $L \notin \Lambda$, $L \not\subset \Pi_1, \Pi_2$, is completely contained in $2n - 2$ independent HV's from $\{\chi\}$, then $L$ intersects $\Pi_1$ or $\Pi_2$.*

*Proof.* Let $\{H^{k_1}\}, \dots, \{H^{k_{2n}}\} \in \{\chi\}$ be independent (over $GF(q)$).

Let $A = \bigcap_{i=1}^{2n-2} \{H^{k_i}\}$ contain a full line $L$, $L \cap \Pi_1 = L \cap \Pi_2 = \emptyset$. We will show that this assumption leads to a contradiction.

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

$$A_{-1} = A \cap \{H^{k_{2n-1}}\}, A_\lambda = A \cap \{H^{k_{2n}} - \lambda H^{k_{2n-1}}\},$$

$\lambda$ ranging through $GF(q)$. We have $A_i \cap A_j = \Pi_1 \cup \Pi_2$ for any $i \neq j$.

By [**2**, p. 1171], a line intersects a HV in $q + 1$ points, in one point, or lies entirely in it. Thus $L$ cannot be contained in any one $A_i$. Hence $L$ must intersect $q - 1$ of the $A_i$'s at $q + 1$ points each and the remaining two, say $A_{-1}$ and $A_0$, at one point each. Let those two points be $\mathbf{y}$ and $\mathbf{z}$,

https://doi.org/10.4153/CJM-1981-043-7 Published online by Cambridge University Press

respectively; they are, of course, conjugate with respect to $\{H^{k_i}\}, i = 1, 2, \ldots, 2n - 2$.

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

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

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

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

where $x$ stands for $a\mathbf{z}^T H^{k_{2n}} \mathbf{y}^{(q)}$. The latter equation has $q$ distinct solutions, all nonzero, so that unless

$$\mathbf{z}^T H^{k_{2n}} \mathbf{y}^{(q)} = 0,$$

$L$ will intersect $\{H^{k_{2n}}\}$ at $q + 1$ points, the sought contradiction.

Likewise we obtain

$$\mathbf{z}^T H^{k_{2n-1}} \mathbf{y}^{(q)} = 0$$

and therefore $\mathbf{y}$ and $\mathbf{z}$ are conjugate with respect to all $\{H^{k_i}\}$, $i = 1, 2, \ldots, 2n$.

It follows that the $2n$ vectors $H^{k_i}\mathbf{y}^{(q)}$ cannot form a basis of the $2n$-dimensional vector space, for if they did, we would have $\mathbf{z}^T\mathbf{w}^{(q)} = 0$ for any point $\mathbf{w}$ of the geometry, so that $\mathbf{z}$ would be the zero vector.

Hence there exist $2n$ elements $c_i \in GF(q^2)$, not all zero, such that

$$\sum_{i=1}^{2n} c_i H^{k_i} \mathbf{y}^{(q)} = \mathbf{0},$$

i.e., the matrix

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

is singular and so is $M^{(q)}(H)$. Also, $M \neq \mathbf{0}$. As a polynomial in $H$, $M(H)$ has degree at most $2n - 1$. The matrix $M(H)M^{(q)}(H)$ is singular and has coefficients in $GF(q)$, thus

$$M(H)M^{(q)}(H) = \mathbf{0}$$

and this enables us to write

$$M(H)M^{(q)}(H) = r_n(H) r_n^{(q)}(H),$$

which implies, say:

$$(5) \quad M(H) = r_n(H)\alpha(H).$$

https://doi.org/10.4153/CJM-1981-043-7 Published online by Cambridge University Press

$\alpha(H)$ has degree at most $n-1$, therefore $\alpha(H)\alpha^{(q)}(H)$, with coefficients in $GF(q)$, has degree at most $2n-2$ and thus $\alpha(H)$ is not singular. Now (5) shows that $M(H)\mathbf{y}^{(q)} = \mathbf{0}$ implies $r_n(H)\mathbf{y}^{(q)} = \mathbf{0}$, i.e., $\mathbf{y} \in \Pi_1$ and this final contradiction concludes the proof.

LEMMA 12. *A line $L \notin \Lambda$, $L \not\subset \Pi_1, \Pi_2$, cannot have more than two points in common with the intersection $P$ of $2n-1$ independent* HV'*s from* $\{\chi\}$.

*Proof.* By Lemmas 6 and 10, we need consider only those lines that do not intersect $\Pi_1 \cup \Pi_2$. Let $L$ be such a line and let $|L \cap P| = y \geqq 2$.

By Lemma 11, no intersection of $2n-2$ independent HV's from $\{\chi\}$ can contain $L$. As a consequence, there must be at least two HV's among the $2n-1$ given ones, say $\{H^{i_1}\}$ and $\{H^{i_2}\}$, none of whose linear combinations contains $L$.

$L$ must have $z \geqq y$ points in common with $\{H^{i_1}\} \cap \{H^{i_2}\}$ and exactly $q+1$ common points with each of $\{H^{i_1}\}$, $\{H^{i_2} - \lambda H^{i_1}\}$, $\lambda \in GF(q)$. These $q+1$ HV's span the geometry on the other hand. Thus we obtain

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

yielding $z = 2$, hence $y = 2$.

*Proof of the theorem.* By Lemma 9, the intersection $P$ of any $2n-1$ independent HV's from $\{\chi\}$ can be written as a disjoint union:

$$P = \Pi_1 \cup \Pi_2 \bigcup_{k=1}^{q-1} \Omega_k,$$

where

$$\Omega_k = \{H^{T^i}\mathbf{u} + c_k H^{T^{\theta-i}}\mathbf{v} \colon i = 0, 1, \ldots, \theta - 1\}.$$

The $\Omega_k$'s are $\theta$-caps, by Lemma 12, completing the proof.

On the other hand, $\bigcup_{k=1}^{q-1}\Omega_k$, for $q \neq 2$, is a $((q^{2n}-1)/(q+1), q-1)$-cap, so that we also have

COROLLARY 3. *Given any two disjoint subspaces $PG(n-1, q^2)$ of a $PG(2n-1, q^2)$, $q \neq 2$, the point-set of the latter is a disjoint union of the former and of $(q^{2n}-1)/(q-1)$ $((q^{2n}-1)/(q+1), q-1)$-caps.*

As in [**3**], we introduce the following terminology: the HV's $\{H^i\} \in \{\chi\}$ will be called *large hyperplanes* and in general, the intersection of $2n-m-1$ independent HV's from $\{\chi\}$, $0 \leqq m \leqq 2n-1$, will be an $m$-dimensional *large subspace*. The large points and the large lines form a $PG(2n-1, q)$, exactly as in [**3**].

The collineation $\mathscr{C}$ of $PG(2n-1, q^2)$ that maps each point $\mathbf{x}$ onto $H^{T^i}\mathbf{x}$ will map each HV $\{H^j\}$ onto the HV $\{H^{j-2i}\}$, as can be readily checked. $\mathscr{C}$ maps $\Pi_1$ and $\Pi_2$ onto themselves, of course.

Again as in [**3**], one shows that $\mathscr{C}$ maps all large subspaces of $PG(2n - 1, q)$ onto large subspaces and thus we conclude that $\mathscr{C}$ is a collineation of the $PG(2n - 1, q)$ as well.

Furthermore, it is a straightforward verification that $\mathscr{C}$ maps the caps $\Omega_k$ that appear in the proof of the theorem, onto caps of the same type.

## References

**1.** G. Birkhoff and S. MacLane, *A survey of modern algebra* (MacMillan, Third Ed., 1966).

**2.** R. C. Bose and I. M. Chakravarti, *Hermitian varieties in a finite projective space* $PG(N, q^2)$, Can. J. Math. *18* (1966), 1161–1182.

**3.** B. C. Kestenband, *Projective geometries that are disjoint unions of caps*, Can. J. Math. (to appear).

**4.** James 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*