HERMITIAN VARIETIES IN A FINITE PROJECTIVE SPACE PG(N, q^2)

R. C. BOSE AND I. M. CHAKRAVARTI

1. Introduction. The geometry of quadric varieties (hypersurfaces) in finite projective spaces of N dimensions has been studied by Primrose **(12)** and Ray-Chaudhuri **(13)**. In this paper we study the geometry of another class of varieties, which we call Hermitian varieties and which have many properties analogous to quadrics. Hermitian varieties are defined only for finite projective spaces for which the ground (Galois field) GF(q^2) has order q^2, where q is the power of a prime. If h is any element of GF(q^2), then $\bar{h} = h^q$ is defined to be conjugate to h. Since $h^{q^2} = h$, h is conjugate to $\bar{h}$. A square matrix $H = ((h_{ij}))$, $i, j = 0, 1, \ldots, N$, with elements from GF(q^2) is called Hermitian if $h_{ij} = \bar{h}_{ji}$ for all i, j. The set of all points in PG(N, q^2) whose row vectors $\mathbf{x}^T = (x_0, x_1, \ldots, x_N)$ satisfy the equation $\mathbf{x}^T H \mathbf{x}^{(q)} = 0$ are said to form a Hermitian variety V_{N-1}, if H is Hermitian and $\mathbf{x}^{(q)}$ is the column vector whose transpose is $(x_0^q, x_1^q, \ldots, x_N^q)$. The properties of the curve $x_0^{q+1} + x_1^{q+1} + x_2^{q+1} = 0$ in PG$(2, q^2)$, which is a Hermitian variety, have been studied in some detail by one of the authors **(3)**. The present paper generalizes these results to N dimensions. The theory of tangent and polar hyperplanes of Hermitian varieties has been developed, and the sections of these varieties by hyperplanes have been studied and the number of points on a Hermitian variety obtained.

It has been shown that if $N = 2t + 1$ or $2t + 2$, a non-degenerate Hermitian variety V_{N-1} contains flat spaces of t dimensions and no higher. The number of such subspaces contained in V_{N-1} has been derived. Finally the geometry of the surface

$$x_0^{q+1} + x_1^{q+1} + x_2^{q+1} + x_3^{q+1} = 0$$

has been studied in some detail, leading to a geometric interpretation of some designs. For example if $q = 2$, the surface contains 45 points and is ruled by 27 lines, three of which pass through each point. Corresponding to any point P on the surface we get a set of 12 points that are joined to P by a line on the surface. The 45 sets so obtained form the blocks of a balanced incomplete block design with parameters $v = b = 45$, $r = k = 12$, $\lambda = 3$. There are many other interesting designs and configurations connected with Hermitian varieties which will be discussed in a separate communication.

Received June 30, 1965. This research was supported by the National Science Foundation Grant No. GP-3792 and the Air Force Office of Scientific Research Grant No. AF-AFOSR-760-65.

2. Correspondence between the elements of GF(q) and GF(q^2). Let $q = p^m$, where p is a prime number and m is a positive integer. Let GF(q) be a Galois field with q elements, and GF(q^2) an extension of GF(q). If θ is a primitive element of GF(q^2), then the elements of GF(q^2) are

(2.1) $$0, \theta, \theta^2, \ldots, \theta^{q^2-1} = 1.$$

Any non-zero element x of GF(q^2) satisfies the fundamental equation

(2.2) $$x^{q^2-1} = 1.$$

Writing

(2.3) $$\phi = \theta^{q+1},$$

it follows that

(2.4) $$0, \phi, \phi^2, \ldots, \phi^{q-1} = 1,$$

are all different and are elements of GF(q). Hence ϕ is a primitive element of GF(q), and all of the elements of GF(q) are given by (2.4).

Corresponding to a given element x of GF(q^2), *there is a unique element y belonging to* GF(q), *given by*

(2.5) $$y = x^{q+1}.$$

But for a given non-zero y belonging to GF(q), *there are precisely $q + 1$ distinct elements x of* GF(q^2) *which satisfy* (2.5).

Thus if

(2.6) $$y = \phi^i = \theta^{i(q+1)}, \qquad 1 \leqslant i \leqslant q - 1,$$

then

(2.7) $$x = \theta^{i+j(q-1)}, \qquad j = 1, 2, \ldots, q + 1.$$

If, however, y is zero, then the corresponding element x of GF(q^2) is zero.

3. Conjugate elements of GF(q^2). The primitive element θ of GF(q^2) satisfies a quadratic equation

(3.1) $$x^2 - sx + t = 0,$$

where s and t belong to GF(q), and the left-hand side of (3.1) is irreducible over GF(q).

Using the relation $\theta^2 - s\theta + t = 0$, every element x of GF(q^2) can be expressed as

(3.2) $$x = a + b\theta$$

where a and b belong to GF(q). We then define

(3.3) $$\bar{x} = x^q,$$

as the *conjugate* of x. Since

$$x^{q^2} = x, \tag{3.4}$$

the conjugate of $\bar{x}$ is x. If x is given by (3.3), then

$$\bar{x} = (a + b\theta)^q = a + b\theta^q = a + b\bar{\theta}. \tag{3.5}$$

Since $x \to x^q$ is an automorphism of $\mathrm{GF}(q^2)$, the second root of (3.1) is θ^q or $\bar{\theta}$. Hence

$$\theta + \bar{\theta} = s, \qquad \theta\bar{\theta} = t, \tag{3.6}$$

$$x + \bar{x} = 2a + bs, \tag{3.7}$$

$$x\bar{x} = a^2 + abs + b^2t. \tag{3.8}$$

Hence *the sum as well as the product of two conjugate elements of* $\mathrm{GF}(q^2)$ belongs to $\mathrm{GF}(q)$.

It should be noted that *the necessary and sufficient condition for any element of* $\mathrm{GF}(q^2)$ *to be self-conjugate is that it belong to* $\mathrm{GF}(q)$.

The elements s and t of $\mathrm{GF}(q)$ *appearing in the equation* (3.1) *are non-zero.* From (3.6), $t = \theta^{q+1} \neq 0$ since θ is a primitive element of $\mathrm{GF}(q^2)$. Again if $s = 0$, it would follow from (3.6) that $\theta + \theta^q = 0$, i.e. either $\theta = 0$ or $\theta^{q-1} = -1$. Obviously $\theta \neq 0$. Also $\theta^{q-1} \neq -1$, otherwise $\theta^{2q-2} = 1$, which is contradicted by the fact that θ is a primitive element of $\mathrm{GF}(q^2)$.

LEMMA 3.1. *If h is a non-zero element of* $\mathrm{GF}(q^2)$, *we can find a non-zero element λ of* $\mathrm{GF}(q^2)$ *such that* $h\bar{\lambda} + \bar{h}\lambda \neq 0$.

Let $h = a + b\theta$ and $\lambda = u + v\theta$, where a, b, u, v belong to $\mathrm{GF}(q)$. Then using (3.6)

$$h\bar{\lambda} + \bar{h}\lambda = (2a + bs)u + (2bt + as)v.$$

Case I. If $2a + bs \neq 0$, we can choose $u = 1$, $v = 0$, i.e. $\lambda = 1$.

Case II. If $2a + bs = 0$, then $a \neq 0$, since $a = 0$ would make $b = 0$, contradicting $h \neq 0$. Now $(2bt + as) = a(s^2 - 4t)/s \neq 0$, since $s^2 - 4t = 0$ is the condition for the roots of (3.1) to coincide, i.e. for θ to be equal to θ^q, which is obviously false since θ is a primitive element of $\mathrm{GF}(q^2)$. Hence in this case we can choose $u = 0$, $v = 1$, i.e. $\lambda = \theta$.

4. Hermitian matrices and Hermitian forms.

A square matrix

$$H = ((h_{ij})), \qquad i, j = 0, 1, \ldots, N, \tag{4.1}$$

with elements from $\mathrm{GF}(q^2)$, will be defined to be *Hermitian* if

$$h_{ij} = \bar{h}_{ji}, \tag{4.2}$$

for all i, j. Hence *the diagonal elements of a Hermitian matrix belong to* $\mathrm{GF}(q)$, *and symmetrically situated off-diagonal elements are conjugate to each other.*

Given a matrix $A = ((a_{ij}))$ with elements from $\mathrm{GF}(q^2)$ we define the *conjugate* of A by

$$A^{(q)} = ((a_{ij}^{\,q})) = ((\bar{a}_{ij})). \tag{4.3}$$

Clearly, the conjugate of $A^{(q)}$ is A itself. Thus the *relation of conjugacy is symmetric.* So far as this definition is concerned, A may or may not be a square matrix. In particular A may be a row vector or a column vector. Clearly, the necessary and sufficient condition for A to be self-conjugate is that all of its elements belong to $\mathrm{GF}(q)$.

The transpose of A will be denoted by A^T. Clearly *the transpose of the conjugate is the conjugate of the transpose*, i.e.

$$A^{T(q)} = A^{(q)T}. \tag{4.4}$$

LEMMA 4.1. *A square matrix $G = ((g_{ij}))$ with elements from* $\mathrm{GF}(q^2)$ *is Hermitian if and only if*

$$G^{(q)} = G^T. \tag{4.5}$$

The proof is obvious.

LEMMA 4.2. *Suppose A and B are two matrices of order $m \times n$ and $n \times h$ with elements from* $\mathrm{GF}(q^2)$, *and $C = AB$; then*

$$C^{(q)} = A^{(q)} B^{(q)}. \tag{4.6}$$

Proof. Now $C = ((c_{ik}))$, where $c_{ik} = \sum_j a_{ij} b_{jk}$. Hence

$$\bar{c}_{ik} = c_{ik}^{\,q} = \left(\sum_{j=1}^{n} a_{ij} b_{jk}\right)^q = \sum_{j=1}^{n} a_{ij}^{\,q} b_{jk}^{\,q} = \sum_{j=1}^{n} \bar{a}_{ij} \bar{b}_{jk}.$$

Hence by definition $C^{(q)} = A^{(q)} B^{(q)}$.

LEMMA 4.3. *If H is a Hermitian matrix of order $N + 1$, and A is any matrix of order $(N + 1) \times m$ with elements from* $\mathrm{GF}(q^2)$, *then*

$$G = A^T H A^{(q)},$$

is a Hermitian matrix of order m.

From Lemmas 4.1 and 4.2, and the equation (4.4),

$$G^T = A^{(q)T} H^T A = A^{T(q)} H^{(q)} A = G^{(q)}.$$

The required result follows from Lemma 4.1.

COROLLARY. *If $\mathbf{x}$ is a $(N + 1) \times 1$ column vector, and H is a Hermitian matrix of order $N + 1$, then $\mathbf{x}^T H \mathbf{x}^{(q)}$ is an element of* $\mathrm{GF}(q)$.

Proof. $\mathbf{x}^T H \mathbf{x}^{(q)}$ is a 1×1 Hermitian matrix. Hence it is a self-conjugate element of $\mathrm{GF}(q^2)$.

The elements of all of the vectors and matrices which we shall consider belong to $\mathrm{GF}(q^2)$. When we speak of the dependence or independence of a set

https://doi.org/10.4153/CJM-1966-116-0 Published online by Cambridge University Press

of vectors, we shall mean dependence and independence over $GF(q^2)$. The rank of a vector space or the rank of a matrix will mean rank over $GF(q^2)$.

Two Hermitian matrices H and G of the same order $N + 1$ with elements from $GF(q^2)$ will be called equivalent if we can find a non-singular square matrix A, with elements from $GF(q^2)$, such that

$$A^T H A^{(q)} = G.$$

If H and G are equivalent, we may write $H \sim G$. It is readily seen that this relation satisfies the three axioms of equivalence, i.e. (i) $H \sim H$, (ii) if $H \sim G$, then $G \sim H$, (iii) if $H \sim G$ and $G \sim K$, then $H \sim K$.

The above follows by noting that

(i) $I^T = I^{(q)} = I$ where I is the unit matrix of order $N + 1$,
(ii) $(A^T)^{-1} = (A^{-1})^T$, $(A^{(q)})^{-1} = (A^{-1})^{(q)}$,
(iii) $B^T A^T = (AB)^T$, $A^{(q)} B^{(q)} = (AB)^{(q)}$ from Lemma 4.2.

THEOREM 4.1. *A Hermitian matrix H of order $N + 1$ and rank $r > 0$, with elements from $GF(q^2)$, is equivalent to a diagonal matrix of order $N + 1$, the first r diagonal elements of which are unity and the rest zero.*

(a) We can permute the columns of H in any desired manner and permute its rows in the corresponding manner by postmultiplying H with a suitable permutation matrix $P = P^{(q)}$, and premultiplying H with P^T. Hence, by such operations, we can rearrange the rows and columns of H so that all null rows and columns are at the end. The transformed matrix is equivalent to H.

(b) We shall denote by $E_{uv}(\lambda)$, a matrix of order $N + 1$, for which each diagonal element is unity, the element in the uth row and vth column is λ, $u \neq v$, and all other elements are zero. Such a matrix will be called an *elementary matrix of order $N + 1$*. Clearly

$$E_{uv}^T(\lambda) = E_{vu}(\lambda).$$

The effect of premultiplying H with $E_{uv}^T(\lambda)$ is to replace the vth row of H by the sum of the vth row and the uth row multiplied by λ. The effect of postmultiplying the matrix so obtained with $E_{uv}^{(q)}(\lambda)$ is to replace its vth column by the sum of the vth column and the uth column multiplied with $\bar{\lambda}$. Thus if H is given by (4.1),

$$E_{uv}^T(\lambda) \mathrm{H} E_{uv}^{(q)}(\lambda) = G = ((g_{ij}))$$

where

$$g_{v-1,v-1} = h_{v-1,v-1} + \lambda h_{u-1,v-1} + \bar{\lambda} h_{v-1,u-1} + \lambda\bar{\lambda} h_{u-1,u-1}$$
$$g_{v-1,j} = h_{v-1,j} + \lambda h_{u-1,j}, \qquad g_{j,v-1} = h_{j,v-1} + \bar{\lambda} h_{j,u-1} \qquad (j \neq v - 1),$$
$$g_{ij} = h_{ij} \qquad (i \neq v - 1, j \neq v - 1).$$

If the vth row and column of H are non-null but all diagonal elements are zero, then we can find non-zero conjugate elements $h_{u-1,v-1}$ and $h_{v-1,u-1}$

belonging to the $(u-1)$st row and column respectively. By Lemma 3.1 there exists an element λ of $GF(q^2)$ such that $\lambda h_{u-1,v-1} + \bar{\lambda} h_{v-1,u-1} \neq 0$. Then the matrix $E_{uv}^T(\lambda) H E_{uv}^{(q)}(\lambda)$ is equivalent to G and the element $g_{v-1,v-1}$ in the vth row and column is non-zero.

(c) By using (a) and (b) suppose H has already been transformed to an equivalent form such that the first row and column are non-null and $h_{00} \neq 0$. We now reduce the non-diagonal elements of the first row and column to zero, in N steps, the $(v-1)$st step consisting of premultiplying the matrix obtained in the previous step by $E_{1v}^T(-h_{v-1,0}/h_{00})$ and postmultiplying it by $E_{1v}^{(q)}(-h_{v-1,0}/h_{00})$, $v = 2, 3, \ldots, N+1$.

If any null rows and columns appear, they are transferred to the end by using (a). If now all the diagonal elements other than h_{00} are zero and there is a non-null row, by using (a) and (b) we can bring a non-zero element at the diagonal position of the second row. Then as in (c), we can reduce the non-diagonal elements of the second row and column to zero. Proceeding in this manner, we reduce H to an equivalent diagonal matrix D, in which the first r_0 diagonal elements are non-null, and the remaining diagonal elements are null. Since all our transformations have been rank preserving, $r_0 = r$.

(d) Since D is Hermitian, the diagonal elements belong to $GF(q)$. Let the ith diagonal element be d_i. From the correspondence described in § 2, we can find an element α_i of $GF(q^2)$ such that

$$d_i = \alpha_i^{q+1} = \alpha_i \bar{\alpha}_i \qquad (i = 0, 1, \ldots, r-1).$$

We denote by $\Delta(\alpha_i)$ the diagonal matrix whose ith diagonal element is α_i and the other diagonal elements are zero. We can finally reduce D to the form desired in the theorem in r steps, the $(i+1)$st step consisting of premultiplying the matrix obtained in the previous step by $D^T(\alpha_i)^{-1}$ and postmultiplying it by $D^{(q)}(\alpha_i)^{-1}$ $(i = 0, 1, \ldots, r-1)$. This completes the proof of the theorem.

Let $\mathbf{x}^T$ be the row vector $(x_0, x_1, \ldots, x_N)$, and $\mathbf{x}$ the corresponding column vector, where $x_0, x_1, \ldots, x_N$ are indefinites. Then the form $\mathbf{x}^T H \mathbf{x}^{(q)}$ is called a *Hermitian form* if H is a Hermitian matrix. H is called the matrix of the form. The order and rank of the form are defined to be the order and rank of H. Note that $\mathbf{x}^T H \mathbf{x}^{(q)}$ is a homogeneous polynomial of the $(q+1)$st degree in the indefinites $x_0, x_1, \ldots, x_N$.

The Hermitian form $\mathbf{x}^T H \mathbf{x}^{(q)}$ is transformed into $\mathbf{y}^T A^T H A^{(q)} \mathbf{y}^{(q)}$ by the linear transformation $\mathbf{x} = A\mathbf{y}$. Two Hermitian forms are defined to be equivalent if one can be transformed to the other by a non-singular linear transformation. Clearly the necessary and sufficient condition for two Hermitian forms to be equivalent is that their matrices be equivalent.

COROLLARY. *The Hermitian form $\mathbf{x}^T H \mathbf{x}^{(q)}$ of order $N+1$ and rank r can be reduced to the canonical form $y_1 \bar{y}_1 + y_2 \bar{y}_2 + \ldots + y_r \bar{y}_r$ by a suitable non-singular linear transformation $\mathbf{x} = A\mathbf{y}$.*

https://doi.org/10.4153/CJM-1966-116-0 Published online by Cambridge University Press

5. Hermitian varieties in $PG(N, q^2)$**.** We denote by $PG(N, s)$ the finite projective space of N dimensions over the Galois field $GF(s)$ where s is a prime power. The points of the space can be made to correspond to ordered $(N + 1)$-tuplets

$$(x_0, x_1, \dots, x_N), \tag{5.1}$$

where the x_i's belong to $GF(s)$, and are not all zero. The ordered n-tuplets $(x_0, x_1, \dots, x_N)$ and $(x_0^*, x_1^*, \dots, x_N^*)$ correspond to the same point if and only if there exists a non-zero element ρ of $GF(s)$ such that

$$\rho x_i^* = x_i, \qquad i = 0, 1, \dots, N.$$

If P is the point corresponding to (5.1), then the row vector $\mathbf{x}^T = (x_0, x_1, \dots, x_N)$ is called the row vector of P, and its transpose $\mathbf{x}$ is called the column vector of P. The elements $x_0, x_1, \dots, x_N$ are called the coordinates of P.

If C is a matrix with $N + 1$ rows and of rank $N - m$ with elements from $GF(s)$, then the set of points whose row vectors satisfy

$$\mathbf{x}^T C = 0 \tag{5.2}$$

is called an *m-flat* or a *linear subspace of m dimensions*, and (5.2) is called the equation of the m-flat. Points are linear subspaces of zero dimensions. Linear subspaces of 1, 2, and $N - 1$ dimensions are respectively called lines, planes, and hyperplanes.

A set of points will be said to be dependent or independent according as the corresponding row (column) vectors are dependent or independent. Any $m + 1$ independent points determine a unique m-flat containing them.

Let E_i be the point for which the $(i + 1)$st coordinate is unity, and other coordinates are zero $(i = 0, 1, \dots, N)$. Also let E be the point all of whose coordinates are unity. Then $E_0, E_1, \dots, E_N$ are called the *fundamental points* and E is called the *unit point*. Clearly any N of the $N + 1$ points $E_0, E_1, \dots, E_N, E$ are independent. Together they are said to constitute the *reference system*.

Let A be an $(N + 1) \times (N + 1)$ non-singular matrix with elements from $GF(s)$. Then the homogeneous linear transformation

$$\mathbf{y} = A\mathbf{x} \tag{5.3}$$

defines a transformation of coordinates. If $\mathbf{x}$ is the original column vector of P, the transformed column vector is $\mathbf{y}$. This transformation defines new fundamental points $F_0, F_1, \dots, F_N$ and a new unit point F. Their transformed coordinates are $(1, 0, \dots, 0)$, $(0, 1, \dots, 0), \dots, (0, 0, \dots, 1)$, and $(1, 1, \dots, 1)$ and the original coordinates can be calculated from (5.3). An important theorem states that given any $N + 2$ points $P_0, P_1, \dots, P_N$, and and P, no $N + 1$ of which are dependent, there exists a unique linear transformation, which would make $P_0, P_1, \dots, P_N$ the fundamental points and P the unit point. Thus in $PG(N, s)$ any $N + 2$ points, no $N + 1$ of which are

https://doi.org/10.4153/CJM-1966-116-0 Published online by Cambridge University Press

dependent, may be chosen as the fundamental points and the unit point. This choice uniquely determines the coordinates of all other points (up to a non-zero multiple of GF(s)). Projective geometry studies those properties that are invariant under linear homogeneous transformations and are thus independent of the choice of a reference system. An excellent account of finite projective spaces will be found in (**1**; **10**; **15**).

In particular, let us choose $s = q^2$, where q is a prime power, and consider the finite projective space PG(N, q^2). If H is a Hermitian matrix of order $N + 1$ and rank r with elements from GF(q^2), then the set of points whose coordinates satisfy the $(q + 1)$st degree equation

$$\mathbf{x}^T H \mathbf{x}^{(q)} = 0 \tag{5.4}$$

are said to be the points of a Hermitian variety V_{N-1} of $N - 1$ dimensions and rank r. The equation (5.4) is said to be the equation of V_{N-1}. If we apply the linear transformation (5.3) the new equation of V_{N-1} becomes

$$\mathbf{y}^T A^T H A^{(q)} \mathbf{y} = 0. \tag{5.5}$$

Now $A^T H A^{(q)}$ is a Hermitian matrix of rank r equivalent to H. Hence the rank of a Hermitian variety is invariant under a non-singular linear transformation. It follows from Theorem 4.1 and its corollary that by a suitable choice of the frame of reference, the equation of a Hermitian variety of $N - 1$ dimensions and rank r can be reduced to the canonical form

$$x_0\bar{x}_0 + x_1\bar{x}_1 + \ldots + x_{r-1}\,\bar{x}_{r-1} = 0. \tag{5.6}$$

A Hermitian variety V_{N-1} of $N - 1$ dimensions is said to be *non-degenerate* if its rank is $N + 1$. Now PG(N, q^2) contains linear subspaces of dimensions $r < N$. Let Σ_r be such a subspace. Then each point of Σ_r can be characterized by a set of $r + 1$ coordinates $(y_0, y_1, \ldots, y_r)$. For example, if we choose the frame of reference so that the equations of Σ_r are $y_{r+1} = y_{r+2} = \ldots = y_N = 0$, then if the point P, when regarded as a point of PG(N, q^2), has the row vector $\mathbf{y}^T = (y_0, y_1, \ldots, y_r, 0, 0, \ldots, 0)$, regarded as a point of Σ_r it has row vector $\mathbf{y}^{*T} = (y_0, y_1, \ldots, y_r)$. Then if H^* is a Hermitian matrix of order $r + 1$, the points of Σ_r which satisfy the equation $\mathbf{y}^{*T} H^* \mathbf{y}^{*(q)} = 0$ will be said to form the Hermitian variety V_{r-1} of dimensions $r - 1$ and rank equal to the rank of H^*. We shall in what follows always denote a Hermitian variety by the letter V and choose our notation so that the subscript of V denotes the number of dimensions of V.

Let us consider the special case $N = 1$. Our space is now the projective line PG$(1, q^2)$. Let V_0 be a non-degenerate Hermitian variety in this space. Then the equation of V_0 can be taken as

$$x_0\,\bar{x}_0 + x_1\,\bar{x}_1 = 0 \quad \text{or} \quad x_0^{q+1} + x_1^{q+1} = 0. \tag{5.7}$$

The point $(0, 1)$ obviously does not lie on V_1. Hence for points satisfying (5.7), $x_0 \neq 0$. Now (5.7) gives $(x_1/x_0)^{q+1} = -1$. The correspondence described

https://doi.org/10.4153/CJM-1966-116-0 Published online by Cambridge University Press

in § 2 shows that there are precisely $q + 1$ values of x_1/x_0 which satisfy (5.7). Hence *a non-degenerate Hermitian variety* V_0 *on a projective line* (*over a field of order* q^2) *contains exactly* $q + 1$ *distinct points*. Again suppose the rank of V_0 is one. Then by a suitable choice of the frame of reference its equation can be reduced to $x_0{}^{q+1} = 0$. The only point satisfying this equation is (0, 1). Hence in this case V_0 *consists of a single point*.

The properties of the curve

$$x_0{}^{q+1} + x_1{}^{q+1} + x_2{}^{q+1} = 0 \tag{5.8}$$

were studied in some detail in **(3)**. In particular, it was shown that *a non-degenerate Hermitian variety* V_1 *in* PG$(2, q^2)$ *has exactly* $q^3 + 1$ *points*.

6. Conjugate points, polar spaces, and tangent spaces. Consider a Hermitian variety V_{N-1} with equation (5.4). A point C with row vector $\mathbf{c}^T = (c_0, c_1, \ldots, c_N)$ will be called a *singular point* of V_{N-1} if $\mathbf{c}^T H = 0$ or equivalently $H\mathbf{c}^{(q)} = 0$.

Of course a singular point must lie on V_{N-1}. A point of V_{N-1} which is not singular is called a *regular point* of V_{N-1}. A point C will be called a non-singular point if it is not a singular point of V_{N-1}. Thus a non-singular point may be a regular point of V_{N-1} or a point not lying on V_{N-1}.

A non-degenerate Hermitian variety cannot possess a singular point, since in this case there cannot exist a non-null $\mathbf{c}^T$ satisfying $\mathbf{c}^T H = 0$ as H is non-singular. If V_{N-1} is degenerate, let $r < N + 1$ be the rank of H. Then $\mathbf{c}^T H = 0$ has $N + 1 - r$ independent solutions

$$\mathbf{c}_1{}^T, \mathbf{c}_2{}^T, \ldots, \mathbf{c}_{N+1-r}{}^T. \tag{6.1}$$

Thus the singular points of V_{N-1} are the points of the $(N - r)$-flat determined by the points with row vectors (6.1). This will be said to constitute the singular space of V_{N-1}.

All points whose row vectors satisfy the equation

$$\mathbf{x}^T H\mathbf{c}^{(q)} = 0 \tag{6.2}$$

constitute the polar space of the point C with row vector $\mathbf{c}^T$. When C is a singular point of V_{N-1}, the polar space of C is identical with the whole space PG(N, q^2). When however C is non-singular, the rank of $H\mathbf{c}^{(q)}$ is one and (6.2) is the equation of a hyperplane, which may be called the *polar hyperplane* of C. If $\mathbf{d}^T$ is the row vector of a point D, then the necessary and sufficient condition for the polar space of C to pass through D is $\mathbf{d}^T H\mathbf{c}^{(q)} = 0$, which is equivalent to $\mathbf{c}^T H\mathbf{d}^{(q)} = 0$. This shows that if the polar space of C passes through D, then the polar space of D passes through C. Two such points whose polar spaces mutually pass through each other are said to be conjugate to each other with respect to V_{N-1}. In case V_{N-1} is degenerate, the polar space of C passes through every singular point of V_{N-1} and thus contains the

https://doi.org/10.4153/CJM-1966-116-0 Published online by Cambridge University Press

singular space of V_{N-1}. Hence any two points at least one of which is singular are always conjugate to one another.

The condition for the point C to be self-conjugate, i.e. to lie on its own polar space, is that $\mathbf{c}^T H \mathbf{c}^{(q)} = 0$. Hence a point C is conjugate to itself with respect to V_{N-1} if and only if C lies on V_{N-1}.

The polar hyperplane of a regular point C of V_{N-1} is defined to be the tangent hyperplane to V_{N-1} at C. The tangent hyperplane is defined only for regular points of V_{N-1} and when V_{N-1} is degenerate it contains the singular space of V_{N-1}.

When V_{N-1} is non-degenerate, there is no singular point. To every point there corresponds a unique polar hyperplane, and at every point of V_{N-1} there is a unique tangent hyperplane.

7. Sections of Hermitian varieties with flat spaces. Let V_{N-1} be a Hermitian variety of rank r in $\mathrm{PG}(N, q^2)$ with equation (5.4). The set of points common to V_{N-1} and the m-flat Σ_m with equation (5.2) is defined to be the section of V_{N-1} by Σ_m. If $m = N$, then Σ_m is the whole space and the section is V_{N-1} itself. Let $m < N$. Let Σ_m be defined by $m + 1$ independent points $F_0, F_1, \ldots, F_m$. We can find a non-singular linear transformation $\mathbf{y} = A\mathbf{x}$ such that $F_0, F_1, \ldots, F_m$ become the fundamental points of the reference system. Then the points of Σ_m will satisfy the equations

$$(7.1) \qquad y_{m+1} = y_{m+2} = \ldots = y_{N-1} = 0,$$

while the equation of V_{N-1} will become

$$(7.2) \qquad \mathbf{y}^T G \mathbf{y}^{(q)} = 0$$

where G is a Hermitian matrix equivalent to H. Writing (7.2) in full we have

$$(7.3) \qquad \sum_{j=0}^{N} \sum_{i=0}^{N} g_{ij} y_i y_j^{(q)} = 0.$$

Hence the points common to Σ_m and V_{N-1} satisfy (7.1) and

$$(7.4) \qquad \sum_{j=0}^{m} \sum_{i=0}^{m} g_{ij} y_i y_j^{(q)} = 0.$$

Let G^* be the matrix obtained from G by retaining only the first $m + 1$ rows and columns of G. Evidently G^* is Hermitian and the points on the section of V_{N-1} by Σ_m satisfy (7.1) and

$$(7.5) \qquad \mathbf{y}^{*T} G^* \mathbf{y}^{*(q)} = 0,$$

where $\mathbf{y}^* = (y_0, y_1, \ldots, y_m)$. Regarding Σ_m as a projective space of m dimensions, it is clear that the section of a Hermitian variety V_{N-1} in $\mathrm{PG}(N, q^2)$ by a flat space Σ_m of m dimensions is a Hermitian variety V_{m-1} contained in Σ_m. Clearly the rank of V_{m-1} cannot exceed $m + 1$. However, this rank could be less and, in particular, it may happen that G^* is null so that every point of

Σ_m belongs to the section, which therefore coincides with the section. In this case, the flat space Σ_m is contained in V_{N-1}. We shall therefore adopt the convention that a flat-space Σ_m of dimensions m can be regarded as a Hermitian variety V_{m-1} of dimensions $m - 1$ and rank zero.

As a particular case, let $m = 1$. Then Σ_m is a line. Since the intersection of a line with V_{N-1} must be a Hermitian variety V_0 of rank 2, 1, or 0, we see that a *line intersects* V_{N-1} *in* (i) $q + 1$ *points*, (ii) *a single point*, or (iii) *lies completely in* V_{N-1}. We shall now prove the following theorem:

THEOREM 7.1. *If the Hermitian variety* V_{N-1} *with equation* $\mathbf{x}^T H \mathbf{x}^{(q)} = 0$ *is degenerate with rank* $r < N + 1$ *and* Σ_{r-1} *is a flat space of dimensions* $r - 1$ *disjoint with the singular space* Σ_{N-r} *of* V_{N-1}, *then* V_{N-1} *and* Σ_{r-1} *intersect in a non-degenerate Hermitian variety* V_{r-2} *contained in* Σ_{r-1}.

Let $F_0, F_1, \ldots, F_{r-1}$ be any r independent points in Σ_{r-1}. Also let F_r, $F_{r+1}, \ldots, F_N$ be any $N - r + 1$ independent points in Σ_{N-r}. Now make a non-singular linear transformation $\mathbf{x} = A\mathbf{y}$ such that $F_0, F_1, \ldots, F_{r-1}$, $F_r, \ldots, F_N$ become the fundamental points of the reference system. The equation of V_{N-1} now becomes $\mathbf{y}^T G \mathbf{y}^{(q)} = 0$ where

$$G = ((g_{ij})) \qquad (i, j = 0, 1, \ldots, N),$$

is equivalent to H and is therefore of rank r. Using y-coordinates, the row vector of F_i is $\mathbf{e}_i^T$ for which the $(i + 1)$st coordinate is equal to unity and all other coordinates are equal to zero. The condition for F_i and F_j to be conjugate to each other is $\mathbf{e}_i^T G \mathbf{e}_j^{(q)} = 0$ or $g_{ij} = 0$. Since $F_r, F_{r+1}, \ldots, F_N$ are singular points of V_{N-1}, F_i and F_j are conjugate if (i) $0 \leqslant i \leqslant r - 1$, $r \leqslant j \leqslant N$, (ii) $r \leqslant i \leqslant N$, $r \leqslant j \leqslant N$. This shows that we may write

$$G = \begin{bmatrix} G^* & 0 \\ 0 & 0 \end{bmatrix},$$

where G^* is a Hermitian matrix of order r. Since the rank of G is r, the rank of G^* must also be equal to r. Now the points of V_{r-2} satisfy

$$\mathbf{y}^{*T} G^* \mathbf{y}^{*(q)} = 0, \qquad y_r = y_{r+1} = \ldots = y_N = 0,$$

where $\mathbf{y}^{*T} = (y_0, y_1, \ldots, y_{r-1})$. Hence V_{r-2} is a Hermitian variety of rank r contained in Σ_{r-1}, and is therefore non-degenerate.

COROLLARY. *If* V_{N-1}, Σ_{N-r}, Σ_{r-1}, *and* V_{r-2} *have the same meanings as in the theorem*, C^* *is a point on* V_{r-2} *and* Σ_{r-2} *is the tangent space to* V_{r-2} *at* C^*, *then the tangent space to* V_{N-1} *at* C^* *is the flat space* Σ_{N-1} *of* $N - 1$ *dimensions containing* Σ_{r-2} *and* Σ_{N-r}.

THEOREM 7.2. *If* V_{N-1} *is a degenerate Hermitian variety of rank* $r < N + 1$ *in* PG(N, q^2) *and if* C *is any point belonging to the singular space of* V_{N-1} *and* D *is an arbitrary point of* V_{N-1}, *then any point on the line* CD *belongs to* V_{N-1}.

Let the equation of V_{N-1} be $\mathbf{x}^T H \mathbf{x}^{(q)} = 0$ and let $\mathbf{c}^T$ and $\mathbf{d}^T$ be the row vectors of C and D respectively. Now C and D are self-conjugate, and also C and D are conjugate to each other. Hence

(7.1) $\mathbf{c}^T H \mathbf{c}^{(q)} = 0, \quad \mathbf{d}^T H \mathbf{d}^{(q)} = 0, \quad \mathbf{c}^T H \mathbf{d}^{(q)} = 0, \quad \mathbf{d}^T H \mathbf{c}^{(q)} = 0.$

If B is any point on the line CD, then its row vector $\mathbf{b}^T$ must be of the form $l_1 \mathbf{c}^T + l_2 \mathbf{d}^T$ or $(l_1 \mathbf{c} + l_2 \mathbf{d})^T$. But

$$(l_1 \mathbf{c} + l_2 \mathbf{d})^T H (l_2 \mathbf{c} + l_2 \mathbf{d})^{(q)} = 0,$$

which proves the theorem.

COROLLARY. *If V_{N-1} is as in the theorem and V_{r-2} is the section of V_{N-1} by an $(r-1)$ flat Σ_{r-1} disjoint with the singular space Σ_{N-r} of V_{N-1}, then every point of V_{N-1} lies on some line joining a point of Σ_{N-r} with a point of V_{r-2}.*

From the theorem, if C is a point of Σ_{N-r} and D is a point of V_{r-2}, then any point on the line joining CD belongs to V_{N-1}.

Conversely, let D_0 be any point on V_{N-1}. We have to show that it lies on some line joining a point of Σ_{N-r} with a point of V_{r-2}. This is obviously true if D_0 belongs to Σ_{N-r} or Σ_{r-1}. We may therefore suppose that D_0 does not lie on either of these flat spaces. Let Σ_r be the r-flat containing D_0 and Σ_{r-1}. Then Σ_r intersects Σ_{N-r} in a point C_0 and $C_0 D_0$ intersects Σ_{r-1} in a point P_0. From the theorem, P_0 must be on V_{N-1} and therefore on V_{r-2}. This proves the corollary.

We shall next study the nature of the section of a Hermitian variety with a tangent space. We shall first prove the following:

THEOREM 7.3. *The tangent spaces at two distinct regular points A and B of a Hermitian variety V_{N-1} are identical if and only if the line joining A and B meets the singular space of V_{N-1} in a point. In particular, if V_{N-1} is non-degenerate, then the tangent spaces at A and B must be distinct.*

Let the equation of V_{N-1} be $\mathbf{x}^T H \mathbf{x}^{(q)} = 0$, and let the row vectors of A and B be $\mathbf{a}^T$ and $\mathbf{b}^T$. Then the tangent spaces at A and B have the equations $\mathbf{x}^T H \mathbf{a}^{(q)} = 0$ and $\mathbf{x}^T H \mathbf{b}^{(q)} = 0$. Hence the two tangent spaces are identical if and only if there exists a non-zero element l of $\mathrm{GF}(q^2)$ such that

(7.2) $H\mathbf{a}^{(q)} = lH\mathbf{b}^{(q)} \quad \text{or} \quad (\mathbf{a} - l^{(q)}\mathbf{b})^T H = 0.$

First suppose V_{N-1} is non-degenerate. In this case, H is non-singular. Hence the homogeneous linear equations $\mathbf{c}^T H = 0$ can only be satisfied by $\mathbf{c}^T = 0$. Hence $\mathbf{a}^T = l^{(q)} \mathbf{b}^T$. The vectors of A and B differ only by a non-zero multiple of an element of $\mathrm{GF}(q^2)$. Hence the points A and B must be identical.

Now suppose that V_{N-1} is degenerate and of rank $r < N + 1$. The singular space Σ_{N-r} of V_{N-1} consists of all points with row vector $\mathbf{c}^T$ satisfying $\mathbf{c}^T H = 0$. Hence (7.2) implies that $\mathbf{a}^T - l^{(q)} \mathbf{b}^T = \mathbf{c}^T$ where $\mathbf{c}^T$ is the row vector of some point C belonging to Σ_{N-r}. Hence the line AB meets Σ_{N-r} at C.

https://doi.org/10.4153/CJM-1966-116-0 Published online by Cambridge University Press

COROLLARY. *Let Σ_{N-r+1} be the flat space of $N - r + 1$ dimensions containing a regular point A and the singular space Σ_{N-r} of a degenerate Hermitian variety V_{N-1} of rank $r < N + 1$. Then any point B on Σ_{N-r+1} (which is not on Σ_{N-r}) has the same tangent space as A.*

THEOREM 7.4. *Given a non-degenerate Hermitian variety V_{N-1}, the tangent space at a point C of V_{N-1} intersects V_{N-1} in a degenerate Hermitian variety V_{N-2} of rank $N - 1$ contained in Σ_{N-1}. The singular space of V_{N-2} consists of the single point C.*

Let the equation of V_{N-1} be $\mathbf{x}^T H \mathbf{x}^{(q)} = 0$. Let Σ_{N-1} be the tangent space to V_{N-1} at C. Let $F_0 = C, F_1, \ldots, F_{N-1}$ be N independent points in Σ_{N-1}. We can find a non-singular linear transformation $\mathbf{y} = A\mathbf{x}$ such that $F_0, F_1, \ldots, F_{N-1}$ become the fundamental points of the reference system. Then the equation of Σ_{N-1} becomes $x_N = 0$, and the equation of V_{N-1} becomes $\mathbf{y}^T G \mathbf{y}^{(q)} = 0$, where $G = ((g_{ij}))$ $(i, j = 0, 1, \ldots, N)$ is Hermitian and of rank $N + 1$. Since F_0 is self-conjugate and is conjugate to $F_1, F_2, \ldots, F_{N-1}$, we have

$$g_{0j} = 0 \quad \text{and} \quad g_{i0} = 0 \qquad (i, j = 0, 1, \ldots, N - 1).$$

We can therefore write

$$G = \begin{bmatrix} 0 & \cdot & 0 & 0 & \cdots & 0 & \cdot & g_{0N} \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & \cdot & & & & & \cdot & g_{1N} \\ 0 & \cdot & & & G^{**} & & \cdot & g_{2N} \\ \cdot & \cdot & & & & & \cdot & \cdot \\ 0 & \cdot & & & & & \cdot & g_{N-1,N} \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ g_{N0} & \cdot & g_{N1} & g_{N2} & & g_{N-1,N} & \cdot & g_{NN} \end{bmatrix}, \tag{7.3}$$

where $G^{**} = ((g_{ij}))$, $i, j = 1, 2, \ldots, N - 1$. Now g_{0N} and g_{N0} are non-null since G is non-singular. Also

$$\det G = -g_{0N}\, g_{N0} \det G^{**}. \tag{7.4}$$

It follows that $\det G^{**}$ is non-null so that the rank of G^{**} is $N - 1$. Regarding Σ_{N-1} as a projective space of $N - 1$ dimensions, we have seen that the equation of the section V_{N-2} is $\mathbf{y}^{T*} G^* \mathbf{y}^{*(q)} = 0$ where $\mathbf{y}^{*T} = (y_0, y_1, \ldots, y_{N-1})$ and G^* is the Hermitian matrix obtained by retaining only the first N rows and columns of G. Since G^* is the same as G^{**} except that it has an additional null row and column, rank G^* = rank $G^{**} = N - 1$.

The row vectors of $C = F_0$ when regarded as a point of projective space Σ_{N-1} is $\mathbf{e}_0{}^{*T} = (1, 0, \ldots, 0)$. Since $\mathbf{e}_0{}^{*T} G^* = 0$, C is a singular point of V_{N-1}.

https://doi.org/10.4153/CJM-1966-116-0 Published online by Cambridge University Press

Since the rank of V_{N-2} is $N-1$, the singular space has dimension 0, and must therefore consist of the single point C.

COROLLARY. *Let V_{N-1} be a degenerate Hermitian variety of rank $r < N+1$, with singular space Σ_{N-r}. Let Σ_{N-1} be the tangent space to V_{N-1} at a regular point C. Then Σ_{N-1} intersects V_{N-1} in a Hermitian variety V_{N-2} of $N-2$ dimensions and rank $r-1$ whose singular space is the $(N-r+1)$-flat Σ_{N-r+1} containing C and Σ_{N-r}.*

8. Number of points on a Hermitian variety. Let $S_{N+1}(q^2)$ denote the vector space of row vectors of order $N+1$ with elements from GF(q^2), and let $S_{N+1}(q)$ have a similar meaning with relation to GF(q). To any vector $\mathbf{x}^T = (x_0, x_1, \ldots, x_N)$ belonging to $S_{N+1}(q^2)$, let there correspond a vector $\mathbf{y}^T = (y_0, y_1, \ldots, y_N)$ belonging to $S_{N+1}(q)$ where $y_i = x_i^{q+1}$, $i = 0, 1, \ldots, N$. It follows from the correspondence between the elements of GF(q^2) and GF(q) discussed in § 2 that to each $\mathbf{x}^T$ there corresponds a unique $\mathbf{y}^T$, but to each $\mathbf{y}^T$ with r non-zero coordinates there correspond $(q+1)^r$ vectors $\mathbf{x}^T$ belonging to $S_{N+1}(q)$, each with r non-zero coordinates.

Now let X be any point of PG(N, q^2) with row vector $\mathbf{x}^T$ having r non-zero coordinates. Then any one of the $q^2 - 1$ row vectors $\rho\mathbf{x}^T$ of $S_{N+1}(q^2)$ will represent X, where ρ is any arbitrary non-zero element of GF(q^2). Let $\mathbf{y}^T$ be the row vector of $S_{N+1}(q)$ which corresponds to $\mathbf{x}^T$, and let Y be the point of PG(N, q) with row vector $\mathbf{y}^T$. We then say that Y corresponds to X. The point Y of PG(N, q) is given uniquely by the point X of PG(N, q^2); for if we take $\rho\mathbf{x}^T$ as the vector representing X, then the corresponding vector of $S_{N+1}(q)$ is $a\mathbf{y}^T$ where $a = \rho^{q+1}$, and represents the same point of PG(N, q) as $\mathbf{y}^T$. Conversely, let $\mathbf{y}^T$ be a vector of $S_{N+1}(q)$ representing a point Y of PG(N, q). If $\mathbf{y}^T$ has r non-zero coordinates then we get $(q+1)^r$ distinct vectors of $S_{N+1}(q^2)$ corresponding to $\mathbf{y}^T$. Now Y can be represented by any one of the $q-1$ row vectors $a\mathbf{y}^T$ of $S_{N+1}(q)$, where a is any non-zero element of GF(q). To each of these vectors there correspond $(q+1)^r$ vectors of $S_{N+1}(q^2)$. Thus to the $q-1$ vectors $a\mathbf{y}^T$ (where a ranges over all the non-zero elements of GF(q)), there correspond $(q-1)(q+1)^r$ vectors of $S_{N+1}(q^2)$. But any q^2-1 of these vectors which differ merely by a multiple of some non-zero element ρ of GF(q^2) represent the same point of PG(N, q^2). Hence to each point of PG(N, q) with r non-zero coordinates there correspond $(q-1)(q+1)^r/(q^2-1)$ or $(q+1)^{r-1}$ points of PG(N, q^2).

Now let V_{N-1} be a non-degenerate Hermitian variety in PG(N, q^2). By a suitable choice of the frame of reference we take its equation in the canonical form

$$\sum_{i=0}^{N} x_i \bar{x}_i = 0$$

or

$$x_0^{q+1} + x_1^{q+1} + \ldots + x_N^{q+1} = 0. \tag{8.1}$$

https://doi.org/10.4153/CJM-1966-116-0 Published online by Cambridge University Press

Let Σ be the hyperplane of $\mathrm{PG}(N, q)$ with equation

$$y_0 + y_1 + \ldots + y_N = 0. \tag{8.2}$$

In the correspondence between the points of $\mathrm{PG}(N, q)$ and $\mathrm{PG}(N, q^2)$ just described, if X lies on V_{N-1}, then T lies on Σ and conversely. Let

$$n_r = (q^{r+1} - 1)/(q - 1)$$

denote the number of points on an r-flat in $\mathrm{PG}(N, q)$. The number of points on Σ which have exactly r non-zero coordinates is

$$\binom{N+1}{r}\left[n_{r-2} - \binom{r}{1}n_{r-3} + \binom{r}{2}n_{r-4} + \ldots + (-1)^{r-2}\binom{r}{r-2}n_0\right] = \binom{N+1}{r}[(q-1)^{r-1} - (-1)^{r-1}]/q. \tag{8.3}$$

Hence the total number of points on V_{N-1} is

$$\phi(N, q^2) = \sum_{r=1}^{N+1}\binom{N+1}{r}[(q-1)^{r-1} - (-1)^{r-1}(q+1)^{r-1}/q$$
$$= [q^{N+1} - (-1)^{N+1}][q^N - (-1)^N]/(q^2 - 1).$$

We have thus proved:

THEOREM 8.1. *The number of points on a non-degenerate Hermitian variety* V_{N-1} *in* $\mathrm{PG}(N, q^2)$ *is*

$$\phi(N, q^2) = [q^{N+1} - (-1)^{N+1}][q^N - (-1)^N]/(q^2 - 1). \tag{8.4}$$

COROLLARY. *The number of points on a degenerate Hermitian variety* V_{N-1} *of rank* $r < N + 1$ *in* $\mathrm{PG}(N, q^2)$ *is*

$$(q^2 - 1)f(N - r, q^2)\phi(r - 1, q^2) + f(N - r, q^2) + \phi(r - 1, q^2), \tag{8.5}$$

where $\phi(N, q^2)$ *is given by* (8.4), $f(k, q^2) = [q^{2(k+1)} - 1]/(q^2 - 1)$.

Let Σ_{N-r} be the singular space of V_{N-1}; then the number of points in Σ_{N-r} is $f(N - r, q^2)$. Also let Σ_{r-1} be an $(r - 1)$-flat disjoint from Σ_{N-r}. Then from Theorem 7.1, Σ_{r-1} intersects V_{N-1} in a non-degenerate Hermitian variety V_{r-2} contained in Σ_{r-1}. The number of points on V_{r-2} is $\phi(r - 1, q^2)$. Now from the corollary to Theorem 7.2, every point of V_{N-1} belongs to some line joining a point of Σ_{N-r} with a point of V_{r-2}. Two such lines cannot have a point in common outside of V_{r-2} or Σ_{N-r}. Suppose, if possible, that the points A_1 and A_2 be in Σ_{N-r} and the points B_1 and B_2 in V_{r-2}. If possible, let the lines A_1B_1 and A_2B_2 intersect in P, a point neither in Σ_{N-r} nor in V_{r-2}. Then A_1 and A_2 are distinct. If not, they would coincide with the point of intersection of the two lines, which would mean that P lies in Σ_{N-r}. Similarly B_1 and B_2 are distinct. However, both A_1B_1 and A_2B_2 lie in the plane PA_1A_2. Hence the lines A_1A_2 and B_1B_2 intersect in a point Q, which therefore must be common to Σ_{N-r} and Σ_{r-1}. This contradicts the fact that Σ_{r-1} and Σ_{n-r} are disjoint. Each line joining a point of Σ_{N-r} and V_{r-2} contains $q^2 - 1$ points not contained in either Σ_{N-r} and V_{r-2}. Hence V_{N-1} contains

$$f(N - r, q^2)\phi(r - 1, q^2)(q^2 - 1)$$

points not on Σ_{N-r} or V_{r-2}. This proves the corollary.

9. Flat spaces contained in Hermitian varieties. We shall first prove the following lemma.

LEMMA 9.1. *The line joining two points C and D on a Hermitian variety V_{N-1} is completely contained in V_{N-1} if and only if C and D are conjugate with respect to V_{N-1}.*

Let the equation of V_{N-1} be $\mathbf{x}^T H \mathbf{x}^{(q)} = 0$ where H is Hermitian of order $N + 1$. Let $\mathbf{c}^T$ and $\mathbf{d}^T$ be the row vectors of C and D. Then

$$\mathbf{c}^T H \mathbf{c}^{(q)} = 0, \qquad \mathbf{d}^T H \mathbf{d}^{(q)} = 0. \tag{9.1}$$

The row vector of any point A lying on the line CD can be written as $\mathbf{a}^T = l_1 \mathbf{c}^T + l_2 \mathbf{d}^T = (l_1 \mathbf{c} + l_2 \mathbf{d})^T$. If CD is completely contained in V_{N-1}, we must have

$$(l_1 \mathbf{c} + l_2 \mathbf{d})^T H (l_1 \mathbf{c} + l_2 \mathbf{d})^{(q)} = 0 \qquad \text{for any } (l_1, l_2) \neq (0, 0). \tag{9.2}$$

Hence from (9.1),

$$l_1 l_2^q \mathbf{c}^T H \mathbf{d}^{(q)} + l_2 l_1^q \mathbf{d}^T H \mathbf{c}^{(q)} = 0 \qquad \text{if } (l_1, l_2) \neq (0, 0). \tag{9.3}$$

This implies that $\mathbf{c}^T H \mathbf{d}^{(q)} = 0$, i.e. C and D are conjugate. If this is not so, suppose $\mathbf{c}^T H \mathbf{d}^{(q)} = h \neq 0$. Then from Lemma (3.1), we can find a non-zero element λ of GF(q^2) such that $h\bar{\lambda} + \bar{h}\lambda \neq 0$. Now let us choose $l_1 = 1$, $l_2 = \lambda$; then $l_1 l_2^q = \bar{\lambda}$, $l_2 l_1^q = \lambda$, $\mathbf{d}^T H \mathbf{c}^{(q)} = \bar{h}$ so that from (9.3) we have $h\bar{\lambda} + \bar{h}\lambda = 0$. This is a contradiction.

Conversely, suppose C and D are conjugate. Then $\mathbf{c}^T H \mathbf{d}^{(q)} = 0$ and $\mathbf{d}^T H \mathbf{c}^{(q)} = 0$, so that (9.2) is satisfied. Hence every point of the line CD is on V_{N-1}.

COROLLARY. *The necessary and sufficient condition for any t-flat Σ_t to be completely contained in V_{N-1} is that any two points of Σ_t are conjugate with respect to V_{N-1}. If Σ_t is contained in V_{N-1} and a point C of Σ_t is a regular point of V_{N-1}, then Σ_t is contained in the tangent space to V_{N-1} at C.*

The first part of the corollary is obvious. For the second part, we observe that if D is any point of Σ_t, then D is conjugate to C and is therefore contained in the polar hyperplane of C, which in this case is the tangent space to V_{N-1} at C.

THEOREM 9.1. *If $N = 2t + 1$ or $2t + 2$, then a non-degenerate Hermitian variety V_{N-1} contains flat spaces of dimension t and no higher.*

We can without loss of generality take the equation of V_N in the canonical form $\mathbf{x}^T\mathbf{x}^{(q)} = 0$, i.e., we take $H = I_{N+1}$, the unit matrix of order $N + 1$. Suppose V_N contains a t-flat determined by the $t + 1$ independent points U_0, $U_1, \ldots, U_t$ with row vectors $\mathbf{u}_0, \mathbf{u}_1, \ldots, \mathbf{u}_t$. Any two of these points are conjugate to each other with respect to V_{N-1}. Hence

$$\mathbf{u}_i^T \mathbf{u}_j^{(q)} = 0, \qquad i, j = 0, 1, \ldots, t. \tag{9.4}$$

Let

$$U^T = \begin{bmatrix} u_{00} & u_{01} & \cdots & u_{0N} \\ u_{10} & u_{11} & \cdots & u_{1N} \\ \cdots & \cdots & \cdots & \cdots \\ u_{t0} & u_{t1} & \cdots & u_{tN} \end{bmatrix}, \tag{9.5}$$

be the $(t + 1) \times (N + 1)$ matrix whose row vectors are $\mathbf{u}_0^T, \mathbf{u}_1^T, \ldots, \mathbf{u}\ ^T$. Since the rows of U^T are independent, its rank is $t + 1$. Hence we can find at least $t + 1$ independent columns. We can suppose the first $t + 1$ columns of U^T to be independent; for if this is not true, we can achieve it merely by a permutation of coordinates. Now the equation (9.4) may be rewritten as

$$U^T U^{(q)} = 0. \tag{9.6}$$

Let U_1^T be the matrix consisting of the first $t + 1$ columns of U^T, and U_2^T the matrix consisting of the last $N - t$ columns. Then rank $(U_1^T) = t + 1$, rank $(U_2^T) \leqslant N - t$. Now from (9.6)

$$[U_1^T, U_2^T] \begin{bmatrix} \mathrm{U}_1^{(q)} \\ U_2^{(q)} \end{bmatrix} = 0. \tag{9.7}$$

Hence

$$U_1^T U_1^q + U_2^T U_2^{(q)} = 0. \tag{9.8}$$

Since $x \to x^{(q)}$ is an automorphism of $\mathrm{GF}(q^2)$, rank $U_1^T =$ rank $U_1^q = t + 1$. Hence

$$t + 1 = \operatorname{rank}(U_1^T U_1^{(q)}) = \operatorname{rank}(-U_1^T U_2^{(q)})\ N - t, \tag{9.9}$$

which shows that $N \geqslant 2t + 1$.

Changing t to $t + 1$, we find that if V_{N-1} contains a flat space of dimension $t + 1$, then $N \geqslant 2t + 3$. Hence if $N = 2t + 1$ or $2t + 2$, then V_{N-1} cannot contain a flat space of dimensions higher than t.

We shall next show that if $N = 2t + 1$ or $2t + 2$, we can always find $t + 1$ mutually conjugate points on V_{N-1}. The flat space of t dimensions determined by these points must lie in V_{N-1}. Choose any point U_0 on V_{N-1}. Let Σ_{N-1} be the polar space of U_0. Then Σ_{N-1} intersects V_{N-1} in a degenerate Hermitian variety V_{N-2} contained in Σ_{N-1} of which U_0 is the singular space; cf. Theorem 7.4. Now we can find an $(N - 2)$-flat Σ_{N-2} lying in Σ_{N-1}, disjoint from U_0 and intersecting V_{N-2} in a non-degenerate Hermitian variety V_{N-3} contained in Σ_{N-2}; cf. Theorem 7.1. Let U_1 be any point on V_{N-3}. Since U_1

https://doi.org/10.4153/CJM-1966-116-0 Published online by Cambridge University Press

lies in Σ_{N-1}, it is conjugate to U_0. Now let Σ_{N-3} be the tangent space to V_{N-3} when considered as a variety of the space Σ_{N-2}, and let it intersect V_{N-3} in the Hermitian variety V_{N-4} of which U_1 is the singular space. Again in Σ_{N-3} we can find a flat space Σ_{N-4} of dimension $N - 4$ disjoint from U_1 and intersecting V_{N-4} in a non-degenerate Hermitian variety V_{N-5} contained in Σ_{N-4}. Let U_2 be in V_{N-5}. Then U_2 is conjugate to both U_1 and U_0. Continuing in this way we obtain points $U_0, U_1, \ldots, U_t$ mutually conjugate to one another, U_t lying on V_{N-2t-1}. If $N = 2t + 1$ or $2t + 2$, we shall not be able to carry this process further. The flat space Σ_t determined by $U_0, U_1, \ldots, U_t$ lies completely in V_{N-1}.

Let $\psi(N, t, q^2)$ denote the number of t-flats contained in a non-degenerate Hermitian variety V_{N-1} in $PG(N, q^2)$. Then we know that

$$(9.10)\qquad \psi(N, 0, q^2) = \phi(N, q^2), \qquad \psi(2t + 1, k, q^2) = \psi(2t + 2, k, q^2) = 0 \quad \text{for } k > t,$$

where $\phi(N, q^2)$ is given by (8.4).

We shall next calculate the value of $\psi(N, t, q^2)$ when $N = 2t + 1$ or $2t + 2$.

First suppose $N = 2t + 1$. Let C be any point on V_{2t}. Then the tangent space Σ_{2t} at C to V_{2t} cuts it in a Hermitian variety V_{2t-1} contained in Σ_{2t}, for which C is the singular space. We can find a $(2t - 1)$-flat Σ_{2t-1} contained in Σ_{2t} and disjoint from C intersecting V_{2t-1} in a non-degenerate Hermitian variety V_{2t-2}. Now V_{2t-2} contains $\psi(2t - 1, t - 1, q^2)$ $(t - 1)$-flats. Any of these $(t - 1)$-flats together with C determines a t-flat contained in V_{N-1}. Conversely if Σ_t is a t-flat contained in V_{N-1} and passing through C, then it is contained in Σ_{2t} and intersects Σ_{2t-1} in a $(t - 1)$-flat contained in V_{2t-2}. Hence the number of t-flats contained in V_{N-1} and passing through a fixed point C is $\psi(2t - 1, t - 1, q^2)$. But the number of points on V_{2t} is $\phi(2t + 1, q^2)$, where $\phi(N, q^2)$ is given by (8.4). We thus obtain $\psi(2t-1, t-1, q^2)\phi(2t+1, q^2)$ t-flats by considering all points of V_{2t}. Here each t-flat has been counted $f(t, q^2) = (q^{2(t+1)} - 1)/(q^2 - 1)$ times since this is the number of points on a t-flat. Hence

$$\psi(2t + 1, t, q^2) = \frac{\psi(2t - 1, t - 1, q^2)\phi(2t + 1, q^2)}{f(t, q^2)}$$
$$= (q^{2t+1} + 1)\psi(2t - 1, t - 1, q^2).$$

By successive reduction

$$\psi(2t + 1, t, q^2) = (q^{2t+1} + 1)(q^{2t-1} + 1) \ldots (q + 1),$$

since $\psi(1, 0, q^2) = q + 1$.

In the same manner we can prove that

$$\psi(2t + 2, t, q^2) = (q^{2t+3} + 1)(q^{2t+1} + 1) \ldots (q^3 + 1).$$

https://doi.org/10.4153/CJM-1966-116-0 Published online by Cambridge University Press

THEOREM 9.2. *If $\psi(N, t, q^2)$ denotes the number of t-flats on a non-degenerate Hermitian variety V_{N-1} in* PG(N, q^2), *then*

(9.11) $$\psi(2t+1, t, q^2) = (q^{2t+1}+1)(q^{2t-1}+1)\dots(q+1),$$

(9.12) $$\psi(2t+2, t, q^2) = (q^{2t+3}+1)(q^{2t+1}+1)\dots(q^3+1).$$

10. Some designs associated with a non-degenerate Hermitian variety of two dimensions in PG$(3, q^2)$. Let V_2 be a non-degenerate Hermitian variety in PG$(3, q^2)$. It follows from Theorem 8.1 that V_2 contains $(q^3+1)(q^2+1)$ points. The case $q = 2$ is of special interest. In this case V_2 is a cubic surface with 45 points. Again from Theorems 9.1 and 9.2, V_2 does not contain any plane but is ruled by lines, $(q^2+1)(q+1)$ in number. In the special case $q = 2$, the number of lines is 27. The lines lying on V_2 will be called generators of V_2.

From Theorem 7.4, the tangent plane to V_2 at any point C intersects V_2 in a degenerate Hermitian variety V_1 of rank 2 with C as a singular point. It follows from Theorem 7.1 that if we take a line l in the tangent plane at C, disjoint from C, then l would intersect V_1 in a non-degenerate Hermitian variety V_0 of dimension 0, contained in l. It was shown in § 5 that V_0 consists of a set of $q+1$ distinct points $P_0, P_1, \dots, P_q$. It now follows from the corollary to Theorem 7.2 that V_1 consists of the set of $q+1$ concurrent lines $CP_0, CP_1, \dots, CP_q$. Thus the tangent plane to V_2 at any point C meets V_2 in a set of $q+1$ generators passing through C. Conversely, from the corollary to Lemma 9.4, any generator through C is contained in the tangent plane at C. We have thus shown: *Through any point C of V_2, there pass exactly $q+1$ generators which constitute the intersection with V_2 of the tangent plane at C.* Now through C, there pass q^2+1 lines lying in the tangent plane at C, out of which $q+1$ are generators. The remaining q^2-q lines through C, which lie in the tangent plane meet V_2 only in the single point. Lines meeting V_2 in a single point C will be called *tangents* to V_2 at the point where they meet V_2. Through C, there will pass q^4 lines not lying in the tangent plane at C. Now the $q+1$ generators through C contain q^3+q^2+1 points of V_2. Hence there are q^5 points of V_2 not lying on the tangent plane at C. On the other hand, any line through C not lying on the tangent plane must meet V_2 in a Hermitian variety V_0^*, which must consist of either $q+1$ points or a single point, according as the rank is 2 or 1. Since each of the q^5 points of V_2 not contained in the tangent plane must lie on some line through C, *each of the q^4 lines passing through C and not contained in the tangent plane at C must intersect V_2 in exactly $q+1$ points, one of which is C.* This shows that V_0^* must be of rank 2. Lines intersecting V_2 in $q+1$ points may be called secants. Any arbitrary line not a generator of V_2 must either be a tangent or a secant.

Let l be any generator of V_2. From Theorem 7.3, the tangents to V_2 at two distinct points of l must be distinct. There are exactly q^2+1 points on l, and exactly q^2+1 planes pass through l. Hence *any plane through a generator*

https://doi.org/10.4153/CJM-1966-116-0 Published online by Cambridge University Press

is tangent to V_2 at some point, and intersects V_2 in a set of $q+1$ generators through the point of contact. Let P be a point on V_2 disjoint from a given generator l. Then the plane π containing P and l must be tangent to V_2 at some point C on l. Since P is on the intersection of V_2 and π, CP must be a generator of V_2. Since π can be tangent to V_2 at only one point on CP, so π is not the tangent plane at P. Let π^* be the tangent plane to V_2 at P. Then the $q+1$ generators of V_2 through P lie on π^*. Thus π and π^* intersect in a single generator CP. We have thus shown that *given a generator l of V_2 and a point P of V_2 not on l_1 there passes through P exactly one generator which meets l in a point.*

The concept of a *partial geometry* (r, k, t) was introduced by one of the authors in **(4)**. It is a system of two kinds of undefined elements called "points" and "lines" and an undefined relation of "incidence" satisfying the following axioms:

A1. *Any two points are incident with not more than one line.*

A2. *Each point is incident with r lines.*

A3. *Each line is incident with k points.*

A4. *If the point P is not incident with the line l, there are exactly t lines $(t \geqslant 1)$ through P intersecting l.*

THEOREM 10.1. *The configuration of points and generators of a Hermitian variety V_2 in* PG$(3, q^2)$ *form a partial geometry* $(q+1, q^2+1, 1)$.

All the axioms A1–A4 are satisfied in view of the results already proved.

From the connection established between partial geometries and partially balanced incomplete block (PBIB) designs in **(4)**, it follows that by identifying the points of V_2 with treatments, and the generators of V_2 with blocks, we obtain the PBIB design with parameters

$$(10.1)\quad v = (q^2+1)(q^3+1),\ b = (q+1)(q^3+1),\ r = q+1,\ k = q^2+1,$$
$$n_1 = q^2(q+1),\quad n_2 = q^5,\quad p_{11}^1 = q^2-1,\quad p_{11}^2 = q+1,\quad \lambda_1 = 1,\quad \lambda_2 = 0.$$

This design was otherwise obtained by Ray-Chaudhuri **(14)**. The case $q = 2$ was obtained earlier by Clatworthy and one of the present authors **(6)**. For the definition and other properties of PBIB designs the reader is referred to **(5; 7; 8; 9)**.

Let C_0 and C_1 be two distinct points of V_2 not on the same generator. Denote the line joining C_0 and C_1 by l_1. Then l_1 must be a secant to V_2 and intersects V_2 in $q-1$ other points $C_2, \ldots, C_q$. Let π_0 and π_1 be the tangent planes to V_2 at C_0 and C_1 respectively. Now π_0 cannot pass through C_1. Otherwise C_1 would be on the section of V_2 by π_0 and this would make $C_0\,C_1$ a generator, contrary to the hypothesis. Similarly, π_1 cannot pass through C_0. Let l_2 be the line of intersection of π_0 and π_1. Then l_2 must be skew to l_1. Since l_2 is a line on π_0 disjoint with C_0, l_2 meets V_2 in $q+1$ distinct points $D_0, D_1, \ldots, D_q$. Now D_i $(i = 0, 1, \ldots, q)$ is conjugate to both C_0 and C_1. Hence the tangent plane Σ_i at D_i passes through C_0 and C_1 and so through the line l_1. Thus C_i

https://doi.org/10.4153/CJM-1966-116-0 Published online by Cambridge University Press

and D_j are conjugate $(i, j = 0, 1, \ldots, q - 1)$ and the lines $C_i D_j$ are generators of V_2. We have incidentally shown that *if two points C_0 and C_1 on V_2 do not lie on a generator then there are exactly $q + 1$ points D_i on V_3 such that both $D_i C_0$ and $D_i C_i$ are generators of V_2.*

Now consider the special case $q = 2$. Then V_2 is the cubic surface $x_0^3 + x_1^3 + x_2^3 + x_3^3 = 0$ in $PG(3, 2^2)$. It has 45 points and 27 generators. Through each point there pass three generators and on each generator lie five points. To each point P of V_2 we may associate a set of 12 points, viz. the points (other than P) lying on the three generators through P. This set of points will be called the block corresponding to P. There are exactly 45 blocks, and each point P of V_2 belongs to 12 blocks, viz. the blocks corresponding to the 12 points (other than P) lying on the three generators through P.

Given two distinct points P and Q on V_2, we shall show that there are exactly three blocks containing both P and Q. We have to consider two separate cases. First let P and Q lie on a generator l^*. Now l^* contains three other points besides P and Q, and both P and Q belong to the blocks corresponding to each of these points. Again suppose P and Q lie on a secant. Then from what has been shown above, the line of intersection of the tangent planes at P and Q meets V_2 in $q + 1 = 3$ points D_0, D_1, D_2 such that $D_i P$ and $D_i Q$ $(i = 0, 1, 2)$ are both generators. Hence both P and Q belong to the blocks corresponding to D_0, D_1, and D_2.

Now a balanced incomplete block (BIB) design is a set of v objects or treatments, arranged into b sets or blocks such that (i) each block contains k distinct treatments, (ii) each treatment appears in exactly r blocks, (iii) any pair of objects occurs in exactly λ blocks. The numbers v, b, r, k, λ are called the parameters of the BIB design **(2, 11)**. We may thus state:

THEOREM 10.2. *If V_2 is a non-degenerate Hermitian variety in* $PG(3, 2^2)$, *and if the points of V_2 are identified with treatments, and if corresponding to each point P on V_2 we define a block consisting of all points (other than P) on the generators through P, then the treatments and the blocks form a* BIB *design with parameters*

$$v = b = 45, \qquad r = k = 12, \qquad \lambda = 3.$$

This design has been otherwise obtained by Shrikhande and Singh **(16)** and by Takeuchi **(17)**.

There are many other interesting balanced and partially balanced incomplete block designs associated with Hermitian varieties. These will be discussed in a separate communication.

REFERENCES

1. R. Baer, *Linear algebra and projective geometry* (New York, 1952).

2. R. C. Bose, *On the construction of balanced incomplete block designs,* Ann. Eugen. London, *9* (1939), 358–399.

3. ——— *On the application of finite projective geometry for deriving a certain series of balanced Kirkman arrangements*, Golden jubilee commem. vol., Cal. Math. Soc. (1958–59), 341–354.

4. ——— *Strongly regular graphs, partial geometries and partially balanced designs*, Pacific J. Math., *13* (1963), 389–419.

5. ——— *Combinatorial properties of partially balanced designs and association schemes*, Sankhya, ser. A, *25* (1963), 109–136; and *Contributions to statistics*, presented to Professor P. C. Mahalanobis on the occasion of his 70th birthday (Calcutta, 1964), 21–48.

6. R. C. Bose and W. H. Clatworthy, *Some classes of partially balanced designs*, Ann. Math. Statist., *26* (1955), 212–232.

7. R. C. Bose and D. M. Mesner, *On linear associative algebras corresponding to association schemes of partially balanced designs*, Ann. Math. Statist., *30* (1959), 21–38.

8. R. C. Bose and K. R. Nair, *Partially balanced incomplete block designs*, Sankhya, *4* (1939), 337–372.

9. R. C. Bose and T. Shimamoto, *Classification and analysis of partially balanced designs with two associate classes*, J. Amer. Statist. Assoc., *47* (1952), 151–184.

10. R. Carmichael, *Introduction to the theory of groups of finite order* (New York, 1956), chaps. XI and XII.

11. H. B. Mann, *Analysis and design of experiments* (New York, 1949), chap. IX.

12. E. J. F. Primrose, *Quadrics in finite geometries*, Proc. Cambridge Philos. Soc., *47* (1951), 299–304.

13. D. K. Ray-Chaudhuri, *Some results on quadrics in finite projective geometries based on Galois fields*, Can. J. Math., *14* (1962), 129–138.

14. ——— *Application of the geometry of quadrics for constructing PBIB designs*, Ann. Math. Statist., *33* (1962), 1175–1186.

15. B. Segre, *Lectures on modern geometry* (Rome, 1960), chap. 17.

16. S. S. Shrikhande and N. K. Singh, *On a method of constructing symmetrical balanced incomplete block designs*, Sankhya, ser. A, *24* (1962), 25–32.

17. K. Takeuchi, *On the construction of a series of BIB designs*, Statist. Appl. Res., JUSE, *10* (1963), 48.

University of North Carolina