BARBU C. KESTENBAND

UNITAL INTERSECTIONS IN FINITE PROJECTIVE PLANES

All the definitions in this paper are taken from, or in agreement with [1], [2], [3] and [4].

A square matrix $H = (h_{ij})$ over $GF(q^2)$, q a prime power, is Hermitian if $h_{ij}^q = h_{ji}$ for all i, j. In particular, $h_{ii} \in GF(q)$. If H is Hermitian, then so is $H - \lambda I$ for any $\lambda \in GF(q)$.

Given a Desarguesian projective plane $PG(2, q^2)$, we denote its points by column vectors:

$$\mathbf{u} = \begin{pmatrix} u_1 \\ u_2 \\ u_3 \end{pmatrix}$$

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

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

Two Hermitian matrices H and G are equivalent if there exists a nonsingular matrix A over $GF(q^2)$ such that $A^T H A^{(q)} = G$.

A Hermitian matrix of rank r is equivalent to a diagonal matrix, the first r diagonal entries of which are 1 and the remainder 0 [3, Theorem 4.1].

All Hermitian matrices in this paper will be 3×3, except in Lemma 3.

The curve $\mathbf{x}^T H \mathbf{x}^{(q)} = 0$ in $PG(2, q^2)$, where H is a rank r Hermitian matrix, will be called a rank r unital and denoted by $\{H\}$. A rank 3 unital is a nondegenerate unital. Concerning the term 'unital', see [4].

We shall concern ourselves with the various configurations that arise as intersections of two nondegenerate unitals (see statement of Theorem after Lemma 8).

A unital has $q^2 + 1$, $q^3 + q^2 + 1$ or $q^3 + 1$ points, according to whether the rank is 1, 2 or 3, respectively [3, Theorem 8.1 and Corollary]. A rank 1 unital is actually a line of $PG(2, q^2)$.

If $\mathbf{a}$ is a point and $\{H\}$ a rank 3 unital, the polar of $\mathbf{a}$ with respect to $\{H\}$ is the line $\mathbf{x}^T H \mathbf{a}^{(q)} = 0$. If $\mathbf{a}$ lies on $\{H\}$, its polar is tangent to $\{H\}$; if not, the polar meets $\{H\}$ at $q + 1$ points [2].

LEMMA 1. *Given the Hermitian matrices H_1, H_2, $H_1 \neq cH_2$, consider the collection Γ of all nonzero linear combinations $rH_1 + sH_2$, $r, s \in GF(q)$. Then any two distinct unitals $\{A\}$, $\{B\}$, $A, B \in \Gamma$, intersect on the same set of points. Furthermore, the unitals $\{A\}$, where A ranges through Γ, cover the plane.*

Proof. Let $A = r_1 H_1 + r_2 H_2$, $B = s_1 H_1 + s_2 H_2$. The system of equations $\mathbf{x}^T A \mathbf{x}^{(q)} = 0$, $\mathbf{x}^T B \mathbf{x}^{(q)} = 0$ is equivalent to $\mathbf{x}^T H_1 \mathbf{x}^{(q)} = 0$, $\mathbf{x}^T H_2 \mathbf{x}^{(q)} = 0$, proving the first part.

Geometriae Dedicata 11 (1981) 107–117. 0046–5755/81/0111–0107$01.65.

For the second part, let $\mathbf{x}$ be any point in the plane. If $\mathbf{x}^T H_1 \mathbf{x}^{(q)} = m$, $\mathbf{x}^T H_2 \mathbf{x}^{(q)} = n$, $m, n \neq 0$, the unital $\{nH_1 - mH_2\}$ contains $\mathbf{x}$. □

The next lemma serves to evaluate the cardinality only, of the various configurations that occur when two unitals intersect. However, we will only make use of it in two cases, because it does not, in general, enable one to actually describe the configurations.

LEMMA 2. *Let H be a Hermitian matrix. We denote by m, n, the number of values $\lambda \in GF(q)$ such that $H - \lambda I$ has rank 1, 2, respectively. Then for any fixed $\lambda \in GF(q)$, the unitals $\{H - \lambda I\}$, $\{I\}$, have $m(q - q^2) + nq + q^2 - q + 1$ points in common.*

Proof. Consider the $q + 1$ unitals $\{I\}$, $\{H - \lambda I\}$, λ ranging through $GF(q)$. By Lemma 1, any two unitals in this family meet on the same set and let k be its cardinality. Then k is the solution of $m(q^2 + 1) + n(q^3 + q^2 + 1) + (q + 1 - m - n)(q^3 + 1) - qk = q^4 + q^2 + 1$. □

We will say that two points $\mathbf{u}$, $\mathbf{v}$, are conjugate with respect to the unital $\{I\}$ if $\mathbf{u}^T \mathbf{v}^{(q)} = 0$. A point is self-conjugate if and only if it lies on $\{I\}$. In the sequel, conjugacy and self-conjugacy are always meant with respect to $\{I\}$.

A non-self-conjugate point $\mathbf{u}$ is said to be normalized if $\mathbf{u}^T \mathbf{u}^{(q)} = 1$.

Two subspaces V, W, of a vector space over $GF(q^2)$ will be called conjugate if $\mathbf{v} \in V$, $\mathbf{w} \in W$ implies that $\mathbf{v}$, $\mathbf{w}$ are conjugate.

A matrix U is unitary if $U^T U^{(q)} = I$. Two Hermitian matrices H_1, H_2, are unitary equivalent if $H_2 = U^{-1} H_1 U$, U being unitary.

LEMMA 3. *Let H be an $n \times n$ Hermitian matrix. If the minimal polynomial of H has a factorization $m(x) = p_1(x) \cdots p_k(x)$, where all p_i's have coefficients in $GF(q)$ and are relatively prime, then their null spaces are mutually conjugate.*

Proof. It suffices to prove the case $k = 2$. Each $p_i(x)$ is Hermitian by assumption and thus: $p_i(H)^{(q)} = p_i(H)^T$.

Let $p_1(H)\,\mathbf{w} = p_2(H)\mathbf{v} = \mathbf{0}$ and also let $I = p_1(H)r_1(H) + p_2(H)r_2(H)$.

Then $\mathbf{v} = p_1(H)r_1(H)\mathbf{v}$, $\mathbf{w} = p_2(H)r_2(H)\,\mathbf{w}$. Hence $\mathbf{v}^T = \mathbf{v}^T r_1(H)^T p_1(H)^T$ and $w^{(q)} = p_2(H)^T r_2(H)^T\,\mathbf{w}^{(q)}$ and the conclusion is immediate. □

The purpose of Lemmas 4–7 is to reduce Hermitian matrices with various minimal polynomials to simpler forms, as close to the Jordan canonical forms as their Hermicity permits, through unitary transformations. This is necessary in the proof of the theorem.

LEMMA 4. *If a point is non-self-conjugate, its polar contains $(q^2 - q)/2$ pairs of conjugate points, none of which is self-conjugate.*

Proof. Let $\mathbf{a}$ not be on $\{I\}$. The polar of $\mathbf{a}$ with respect to $\{I\}$ meets $\{I\}$ at $q + 1$ points. Let $\mathbf{b}$ be one of the remaining $q^2 - q$ points. The polar of $\mathbf{b}$ meets the polar of $\mathbf{a}$ at $\mathbf{c}$, which is conjugate with $\mathbf{b}$; also, $\mathbf{c}$ does not lie on

$\{I\}$ for if it did, its polar, which must contain **b**, would be tangent to $\{I\}$, thereby missing **b**. □

LEMMA 5. *A nondegenerate Hermitian matrix with minimal polynomial* $m(x) = (x - \alpha)(x - \beta)(x - \gamma)$ *or* $m(x) = (x - \alpha)(x - \beta)$, α, β, γ *all distinct elements of* $GF(q)$, *is unitary equivalent to a diagonal matrix.*

Proof. In the first case U consists of the normalized eigenvectors, by Lemma 3. In the second case the characteristic polynomial is, say, $(x - \alpha)(x - \beta)^2$. Then **u**, the eigenvector corresponding to α, is conjugate with the null space of $H - \beta I$. On the other hand, **u** cannot be self-conjugate or it would be conjugate with any vector, i.e. **u** would be **0**, contradiction. Thus, by Lemma 4, we find two more non-self-conjugate points which together with **u** and after normalization, make up U. □

LEMMA 6. *A nondegenerate Hermitian matrix with minimal polynomial* $m(x) = (x - \alpha)(x - \delta)^2$ *or* $m(x) = (x - \alpha)p(x)$, $\alpha, \delta \in GF(q)$, $\alpha \neq \delta$, $p(x)$ *irreducible over* $GF(q)$, *is unitary equivalent to*

$$\begin{pmatrix} \alpha & 0 & 0 \\ 0 & \beta & a \\ 0 & a^q & \gamma \end{pmatrix}, \quad a \neq 0.$$

Moreover, in the first case

$$(\beta - \gamma)^2 + 4a^{q+1} = 0 \tag{1}$$

and in the second case

$$(\beta - \alpha)(\gamma - \alpha) \neq a^{q+1} \tag{2}$$

Proof. In both cases the matrix U is obtained as in the second case of the preceding lemma.

(1) holds because the characteristic equation has a double root; (2) holds because equality would entail that α is a double root of the characteristic equation, contradiction. □

LEMMA 7. *A nondegenerate Hermitian matrix H with minimal polynomial* $m(x) = (x - \lambda)^3$ *is unitary equivalent to*

$$\begin{pmatrix} \lambda & c^q & 0 \\ c & \lambda & a^q \\ 0 & a & \lambda \end{pmatrix}, \quad a, c \neq 0.$$

Moreover,

$$a^{q+1} + c^{q+1} = 0. \tag{3}$$

Proof. We shall find three non-self-conjugate, mutually conjugate points $\mathbf{x}, \mathbf{y}, \mathbf{z}$, such that $H\mathbf{x} = \lambda\mathbf{x} + c\mathbf{y}$, $H\mathbf{y} = c^q\mathbf{x} + \lambda\mathbf{y} + a\mathbf{z}$, $H\mathbf{z} = a^q\mathbf{y} + \lambda\mathbf{z}$. To this end we first show that there exists a non-self-conjugate $\mathbf{x}$ such that

$$\mathbf{x}^T(H^T - \lambda I)\mathbf{x}^{(q)} = 0 \tag{4}$$

$$\mathbf{x}^T(H^T - \lambda I)^2\mathbf{x}^{(q)} \neq 0. \tag{5}$$

$H^T - \lambda I$ has rank 2, because it is similar to $\begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix}$. Then $(H^T - \lambda I)^2$ has rank 1.

The rank 2 unital $\{H^T - \lambda I\}$ possesses one singular point, i.e. a point $\mathbf{c}$ such that $\mathbf{c}^T(H^T - \lambda I) = \mathbf{0}^T$. If $\mathbf{b}$ is another point on the unital, it is an easy check that the whole line joining $\mathbf{b}$ and $\mathbf{c}$ is contained in the unital. Therefore $\{H^T - \lambda I\}$ consists of $q + 1$ lines concurrent at $\mathbf{c}$. Now $\{(H^T - \lambda I)^2\}$ is a line, and removing one line from the pencil above still leaves q lines, each with q^2 points. No line, on the other hand, can intersect $\{I\}$ on more than $q + 1$ points and we conclude that there must exist a non-self-conjugate $\mathbf{x}$ on one of these lines, proving (4) and (5).

We now let $c\mathbf{y} = (H - \lambda I)\mathbf{x}$, where c is chosen so that $\mathbf{y}$ has norm 1. The points $\mathbf{x}$ and $\mathbf{y}$ are conjugate by (4); $\mathbf{y}$ is non-self-conjugate by (5).

Next we show that $\mathbf{z}' = (H - \lambda I)\mathbf{y} - c^q\mathbf{x}$ is conjugate with both $\mathbf{x}$ and $\mathbf{y}$, but non-self-conjugate:

$$\begin{aligned} \mathbf{z}'^T\mathbf{x}^{(q)} &= [\mathbf{y}^T(H^T - \lambda I) - c^q\mathbf{x}^T]\mathbf{x}^{(q)} = \mathbf{y}^T(H^T - \lambda I)\mathbf{x}^{(q)} - c^q \\ &= \mathbf{y}^T c^q\mathbf{y}^{(q)} - c^q = 0. \\ \mathbf{z}'^T\mathbf{y}^{(q)} &= [\mathbf{y}^T(H^T - \lambda I) - c^q\mathbf{x}^T]\mathbf{y}^{(q)} \\ &= \mathbf{y}^T(H^T - \lambda I)\mathbf{y}^{(q)} = c^{-q-1}\mathbf{x}^T(H^T - \lambda I)^3\mathbf{x}^{(q)} \end{aligned}$$

and the last expression is 0 because $(H^T - \lambda I)^3$ is the zero matrix.

$$\begin{aligned} \mathbf{z}'^T\mathbf{z}'^{(q)} &= [\mathbf{y}^T(H^T - \lambda I) - c^q\mathbf{x}^T]\,[(H^T - \lambda I)\mathbf{y}^{(q)} - c\mathbf{x}^{(q)}] \\ &= \mathbf{y}^T(H^T - \lambda I)^2\mathbf{y}^{(q)} - c\mathbf{y}^T(H^T - \lambda I)\mathbf{x}^{(q)} - c^q\mathbf{x}^T(H^T - \lambda I)\mathbf{y}^{(q)} + c^{q+1}. \end{aligned}$$

The first term is 0 and the next two are $-c^{q+1}$, so that $\mathbf{z}'^T\mathbf{z}'^{(q)} = -c^{q+1} \neq 0$. This also shows that $\mathbf{z} = (1/a)\mathbf{z}'$ has norm 1, where $a^{q+1} + c^{q+1} = 0$.

It is now a straightforward check that $H\mathbf{z} = a^q\mathbf{y} + \lambda\mathbf{z}$.

Finally,

$$\begin{pmatrix} \mathbf{x}^{(q)^T} \\ \mathbf{y}^{(q)^T} \\ \mathbf{z}^{(q)^T} \end{pmatrix} \cdot H \cdot (\mathbf{x} \quad \mathbf{y} \quad \mathbf{z}) = \begin{pmatrix} \lambda & c^q & 0 \\ c & \lambda & a^q \\ 0 & a & \lambda \end{pmatrix},$$

completing the proof. □

The following lemma will also be needed.

LEMMA 8. *If two nondegenerate unitals have three collinear points in common, then they have $q+1$ points of that line in common.*

Proof. We have to show that (6) and (7) imply (8):

$$\mathbf{a}^T H_i \mathbf{a}^{(q)} = \mathbf{b}^T H_i \mathbf{b}^{(q)} = (\mathbf{a}+r\mathbf{b})^T H_i (\mathbf{a}+r\mathbf{b})^{(q)} = 0, \quad r \neq 0,\ i = 1, 2;\ H_1 \neq H_2, \tag{6}$$

$$(\mathbf{a}+s\mathbf{b})^T H_1 (\mathbf{a}+s\mathbf{b})^{(q)} = 0, \quad s \neq 0,\ s \neq r, \tag{7}$$

$$(\mathbf{a}+s\mathbf{b})^T H_2 (\mathbf{a}+s\mathbf{b})^{(q)} = 0. \tag{8}$$

(8) is equivalent, by (6), to

$$s^{q-1}\mathbf{a}^T H_2 \mathbf{b}^{(q)} + \mathbf{b}^T H_2 \mathbf{a}^{(q)} = 0. \tag{9}$$

From (6) and (7) we also obtain

$$r^{q-1}\mathbf{a}^T H_1 \mathbf{b}^{(q)} + \mathbf{b}^T H_1 \mathbf{a}^{(q)} = r^{q-1}\mathbf{a}^T H_2 \mathbf{b}^{(q)} + \mathbf{b}^T H_2 \mathbf{a}^{(q)} = s^{q-1}\mathbf{a}^T H_1 \mathbf{b}^{(q)} + \mathbf{b}^T H_1 \mathbf{a}^{(q)} = 0. \tag{10}$$

(10) implies $r^{q-1} = s^{q-1}$ ($\mathbf{a}^T H_1 \mathbf{b}^{(q)} \neq 0$, because the polar of $\mathbf{b}$ has only $\mathbf{b}$ in common with the unital) so that (9) holds. □

We are now prepared to prove the main result.

THEOREM. *Let H be a nondegenerate Hermitian matrix and $m(x)$, $f(x)$, its minimal and characteristic polynomial, respectively. The unitals $\{H\}$ and $\{I\}$ intersect on:*

(a) $(q+1)^2$ *points, as in Figure* 1, *if* $m(x) = f(x) = (x-\alpha)(x-\beta)(x-\gamma)$, α, β, γ, *distinct elements of* $GF(q)$;

(b) q^2+q+1 *points, as in Figure* 2, *if* $m(x) = f(x) = (x-\alpha)(x-\delta)^2$, α, δ, *distinct elements of* $GF(q)$;

(c) $q+1$ *collinear points if* $m(x) = (x-\alpha)(x-\beta)$, α, β, *distinct elements of* $GF(q)$;

(d) q^2+1 *points, as in Figure* 3, *if* $m(x) = f(x) = (x-\alpha)p(x)$, $\alpha \in GF(q)$, $p(x)$ *irreducible over* $GF(q)$;

(e) q^2+1 *points, as in Figure* 4, *if* $m(x) = f(x) = (x-\lambda)^3$;

(f) *one point if* $m(x) = (x-\lambda)^2$;

(g) q^2-q+1 *points, no three of which are collinear, if* $f(x)$ *is irreducible over* $GF(q^2)$.

In Figures 1–4 *no three points are collinear unless actually joined by a line in the figure.*

Proof. We will denote points by vectors, as in the foregoing discussion, but also, when convenient, we will use (x_1, x_2, x_3) to denote a point of $PG(2, q^2)$. Throughout this proof z will stand for a primitive root of $GF(q^2)$.

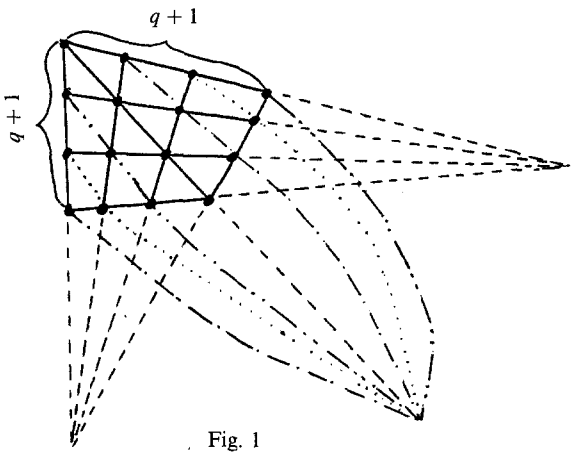

Fig. 1

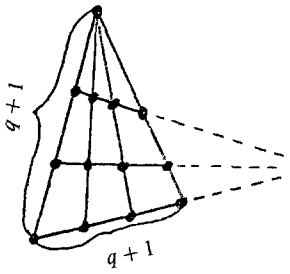

Fig. 2

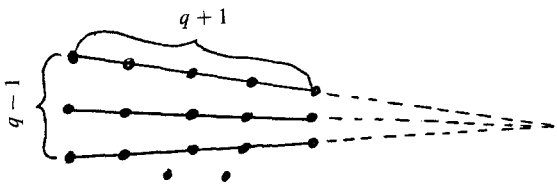

Fig. 3

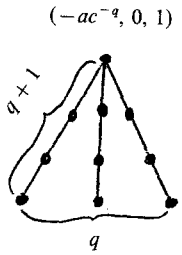

Fig. 4

In all cases we have to find the solutions of the system

$$\mathbf{x}^T H\mathbf{x}^{(q)} = 0, \qquad \mathbf{x}^T\mathbf{x}^{(q)} = 0. \tag{11}$$

(a) We have to solve, by Lemma 5,

$$\alpha x_1^{q+1} + \beta x_2^{q+1} + \gamma x_3^{q+1} = 0$$
$$x_1^{q+1} + x_2^{q+1} + x_3^{q+1} = 0. \tag{12}$$

Let $x_3 = 1$. Hence $(x_1/x_2)^{q+1} = (\beta - \gamma)/(\gamma - \alpha) = z^{r(q+1)}$ for some fixed r. $x_1^{q+1} = (z^r x_2)^{q+1}$. Substitution in (12) gives $(z^m x_2)^{q+1} = -1$, where $z^{m(q+1)} = z^{r(q+1)} + 1$. Therefore $x_2 = z^{s+i(q-1)}$ for some fixed s; $i = 0(1)q$. Then $x_1 = z^{r+s+(i+j)(q-1)}$; $j = 0(1)q$. Thus we have obtained three families of lines:

$$x_2 = z^{s+i(q-1)}x_3, \quad i \in \mathbf{Z}_{q+1}, \text{ concurrent at } (1, 0, 0);$$
$$x_1 = z^{r+j(q-1)}x_2, \quad j \in \mathbf{Z}_{q+1}, \text{ concurrent at } (0, 0, 1);$$
$$x_1 = z^{r+s+(i+j)(q-1)}x_3, \quad i + j \in \mathbf{Z}_{q+1}, \text{ concurrent at } (0, 1, 0).$$

Each line in each family has $q + 1$ points in common with the two unitals.

Further, any two lines belonging to different families intersect within the configuration.

It remains to be shown that no other line of $PG(2, q^2)$ has three points in common with both unitals. To see this, we shall coordinatize the configuration using the additive group $\mathbf{Z}_{q+1}$: each point will be labelled (r, s) and the three families of lines are $r = \text{const.}$, $s = \text{const.}$, $r + s = \text{const.}$

Let $M_1(r_1, s_1)$, $M_2(r_2, s_2)$, $M_3(r_3, s_3)$ be collinear and $r_1 \not\equiv r_2 \not\equiv r_3$, $s_1 \not\equiv s_2 \not\equiv s_3$, $r_1 + s_1 \not\equiv r_2 + s_2 \not\equiv r_3 + s_3$ modulo $q + 1$.

We shall show that they give rise to the so-called Pasch configuration: four lines each of which intersects the other three at three distinct points. This is a contradiction, because nondegenerate unitals cannot contain Pasch configurations ([6], [5]). Specifically, we have to prove that there exist three nonconcurrent lines, each belonging to a different family and passing through M_1, M_2, M_3, respectively.

Consider the following eight lines: $L_1 : r = r_1$; $L_2 : s = s_1$; $L_3 : r = r_2$; $L_4 : s = s_2$; $L_5 : r + s = r_2 + s_2$; $L_6 : r = r_3$; $L_7 : s = s_3$; $L_8 : r + s = r_3 + s_3$.

If L_1, L_4, L_8 are concurrent, we get $r_1 + s_2 \equiv r_3 + s_3 \bmod q + 1$.

If L_2, L_3, L_8 are concurrent, we get $r_2 + s_1 \equiv r_3 + s_3 \bmod q + 1$.

If L_1, L_5, L_7 are concurrent, we get $r_1 + s_3 \equiv r_2 + s_2 \bmod q + 1$.

If L_2, L_5, L_6 are concurrent, we get $r_3 + s_1 \equiv r_2 + s_2 \bmod q + 1$.

But these four congruences imply $r_1 \equiv r_2 \equiv r_3 \bmod q + 1$ for any $q \neq 2$, contradicting the assumption and thereby proving the existence of three lines as required above. This completes the proof, because a minimal polynomial $(x - \alpha)(x - \beta)(x - \gamma)$ with distinct α, β, γ, cannot occur if $q = 2$.

(b) By Lemma 6, we have Equations (12) and

$$\alpha x_1^{q+1} + \beta x_2^{q+1} + \gamma x_3^{q+1} + a^q x_2^q x_3 + a x_2 x_3^q = 0. \tag{13}$$

We shall have to distinguish here between odd and even q.

If q is odd, then $\beta \neq \gamma$ by (1), so we can assume $\beta \neq \alpha$. This implies $x_3 \neq 0$, by (12) and (13). Thus we let $x_3 = 1$.

We show first that the configuration contains exactly one special point for which $x_1 = 0$, i.e. for which $x_2^{q+1} = -1$. (12) and (13) give

$$(\beta - \alpha) x_2^{q+1} + a^q x_2^q + a x_2 + \gamma - \alpha = 0. \tag{14}$$

If we impose here $x_2^{q+1} = -1$, we get $a^q x_2^q + a x_2 + \gamma - \beta = 0$, or

$$a x_2^2 - (\beta - \gamma) x_2 - a^q = 0. \tag{15}$$

(15) has the double root $x_2 = (\beta - \gamma)/2a$ and this value satisfies $x_2^{q+1} = -1$ because of (1). Thus the special point is $(0, (\beta - \gamma)/2a, 1)$ and no other point has $x_1 = 0$. Further, (14) can be transformed into

$$\left(x_2 + \frac{a^q}{\beta - \alpha}\right)^{q+1} = -\left[\frac{\beta + \gamma - 2\alpha}{2(\beta - \alpha)}\right]^2.$$

The right-hand side is not zero, because $\beta + \gamma = 2\delta \neq 2\alpha$. Hence we get $q + 1$ values for x_2, one of which is $(\beta - \gamma)/2a$; to each of the remaining q values there correspond $q + 1$ values for x_1, by (12). This gives a configuration consisting of q sets of $q + 1$ collinear points each, and the special point. The q lines all meet at (1, 0, 0).

We now want to show that any line through the special point that meets one of the other lines within the configuration, meets all lines within it. Specifically, we shall prove that if $(x_1', x_2', 1)$, where x_2' satisfies (14) lies on the line joining the special point to $(x_1, x_2, 1)$, where x_1, x_2 satisfy (12) and (14), then x_1', x_2', too, satisfy (12).

We have $x_1' = ex_1$, $x_2' = ex_2 + (1 - e)(\beta - \gamma)/2a$ for some $e \neq 0$, whence

$$[(\beta - \gamma)/2a - x_2]x_1' = [(\beta - \gamma)/2a - x_2']x_1. \tag{16}$$

Consequently,

$$[(\beta - \gamma)/2a^q - x_2^q]x_1'^q = [(\beta - \gamma)/2a^q - x_2'^q]x_1^q. \tag{17}$$

Multiply (16) and (17), then make use of (1) to obtain

$$\begin{aligned}[-1 + 2(ax_2 + a^q x_2^q)/(\beta - \gamma) + x_2^{q+1}]x_1'^{q+1} \\ = [-1 + 2(ax_2' + a^q x_2'^q)/(\beta - \gamma) + x_2'^{q+1}]x_1^{q+1}.\end{aligned} \tag{18}$$

But $ax_2 + a^q x_2^q = (\alpha - \beta)x_2^{q+1} + \alpha - \gamma$ because of (14), and similarly for x_2'; we substitute this in (18) to obtain, after simple computations, $(1 + x_2^{q+1})x_1'^{q+1} = (1 + x_2'^{q+1})x_1^{q+1}$, which proves the claim, because $1 + x_2^{q+1} = -x_1^{q+1}$ by assumption.

Finally, Lemma 8 shows that in Figure 2 no other three points can be collinear.

If q is even, then $\beta = \gamma$, by (1). We distinguish two cases:

Case I. $\alpha = \beta = \gamma$. Then (12) and (13) give

$$ax_2 x_3^q[1 + (ax_2 x_3^q)^{q-1}] = 0. \tag{19}$$

Therefore, $ax_2 x_3^q = 0$ or $z^{i(q+1)}$, $i = 0(1)q - 2$. $x_3 = 0$ gives $q + 1$ collinear points by (12). $x_3 = 1$ gives q values for x_2. To obtain the special point, let $x_2^{q+1} = 1$ and (19) becomes $x_2^2 = a^{q-1}$, yielding a unique x_2. The remaining $q - 1$ values of x_2 give rise to sets of $q + 1$ collinear points, which together with $x_3 = 0$ and the special point, form the configuration in Figure 2.

We show next that if $(x_1', x_2', 1)$, where $(ax_2')^{q-1} = 1$, lies on the line joining $(0, a^{(q-1)/2}, 1)$ to $(x_1, 1, 0)$, where $x_1^{q+1} = 1$, then $x_1'^{q+1} + x_2'^{q+1} = 1$. We first note that $x_1' = ex_1$, $x_2' = a^{(q-1)/2} + e$, $e \neq 0$. Next, $x_1'^{q+1} = e^{q+1}x_1^{q+1} = e^{q+1}$; $x_2'^2 = a^{q-1} + e^2$; $x_2'^{q-1} = a^{1-q}$, so that $x_2'^{q+1} = 1 + e^2 a^{1-q}$ and therefore $x_1'^{q+1} + x_2'^{q+1} = 1 + e^2(a^{1-q} + e^{q-1})$.

To complete the proof we have yet to demonstrate that $a^{1-q} = e^{q-1}$. To see this, we divide $x_2'^q = a^{(1-q)/2} + e^q$ by $x_2'^{q-1} = a^{1-q}$ and obtain

$x_2' = a^{(q-1)/2} + e^q a^{q-1}$. On the other hand, $x_2' = a^{(q-1)/2} + e$. Hence $e^{q-1}a^{q-1} = 1$, completing the proof.

Case II. $\alpha \neq \beta = \gamma$. (12) and (13) yield

$$(\beta - \alpha)(x_2^{q+1} + x_3^{q+1}) + a^q x_2^q x_3 + a x_2 x_3^q = 0. \tag{20}$$

Hence, $x_2, x_3 \neq 0$. The special point is, as in Case I, $(0, a^{(q-1)/2}, 1)$. To solve (20), let $x_3 = 1$:

$$(\beta - \alpha)x_2^{q+1} + a^q x_2^q + a x_2 + \beta - \alpha = 0. \tag{21}$$

(21) is equivalent to

$$\left(x_2 + \frac{a^q}{\beta - \alpha}\right)^{q+1} = 1 + a^{q+1}/(\beta - \alpha)^2.$$

In the latter equation the right-hand side is not zero, because the eigenvalue of $\begin{pmatrix} \beta & a \\ a^q & \beta \end{pmatrix}$ is $\delta = (\beta^2 - a^{q+1})^{1/2}$ and $a^{q+1} = \beta^2 + \alpha^2$ would entail $\alpha = \delta$, contradiction. Thus we obtain $q + 1$ values for x_2 and the desired configuration.

We now show that if $(x_1', x_2', 1)$, where x_2' satisfies (21), lies on the line joining the special point to $(x_1, x_2, 1)$, where x_1, x_2 satisfy (12) and (21), then $x_1'^{q+1} + x_2'^{q+1} = 1$.

There is an $e \neq 0$ such that $x_1' = ex_1$, $x_2' = ex_2 + (1 - e)a^{(q-1)/2}$; hence

$$[x_2 + a^{(q-1)/2}]x_1' = [x_2' + a^{(q-1)/2}]x_1. \tag{22}$$

(22) implies:

$$[x_2^q + a^{(1-q)/2}]x_1'^q = [x_2'^q + a^{(1-q)/2}]x_1^q \tag{23}$$

and (22) times (23) yields

$$\begin{aligned}[x_2^{q+1} + 1 + a^{(1-q)/2}(x_2 + a^{q-1}x_2^q)]x_1'^{q+1} \\ = [x_2'^{q+1} + 1 + a^{(1-q)/2}(x_2' + a^{q-1}x_2'^q)]x_1^{q+1}.\end{aligned} \tag{24}$$

From (21): $x_2 + a^{q-1}x_2^q = a^{-1}(\beta - \alpha)(1 + x_2^{q+1})$ and similarly for x_2'. Also, $x_2^{q+1} + 1 = x_1^{q+1}$ by assumption. Substitution in (24) reduces it to

$$[1 + a^{(-q-1)/2}(\beta - \alpha)]x_1'^{q+1} = [1 + a^{(-q-1)/2}(\beta - \alpha)](x_2'^{q+1} + 1).$$

We have already seen that the common factor is not zero and this yields the desired result, completing the proof of (b).

(c) By Lemma 5, we have to solve $\alpha x_1^{q+1} + \beta(x_2^{q+1} + x_3^{q+1}) = 0$ together with (12). This leads to $x_1 = 0$ and the two unitals intersect on $q + 1$ points of that line.

(d) Lemma 6 provides again the system (12), (13), where (2) holds.

Case I. $\beta, \gamma \neq \alpha$; this implies $x_2, x_3 \neq 0$. We let $x_3 = 1$ and obtain (14) again.

We first prove that the configuration possesses exactly two special points for which $x_2^{q+1} = -1$, i.e. $x_1 = 0$. To see this, we impose $x_2^{q+1} = -1$ in (14) to obtain (15). It is a straightforward verification that in this case the two roots x_2', x_2'' of (15) satisfy $ax_2' + \gamma = \mu$, $ax_2'' + \gamma = \mu^q$, μ, μ^q, being the roots of $p(x) = 0$. Hence $ax_2'' + \gamma = a^q x_2'^q + \gamma$, so that

$$x_2'' = a^{q-1} x_2'^q \tag{25}$$

and

$$x_2''^{q+1} = x_2'^{q+1}. \tag{26}$$

Moreover, (25) implies $x_2' x_2'' = a^{q-1} x_2'^{q+1}$. On the other hand, (15) shows that $x_2' x_2'' = -a^{q-1}$ and thus we conclude that $x_2'^{q+1} = x_2''^{q+1} = -1$, proving the existence of two special points $(0, x_2', 1)$, $(0, x_2'', 1)$.

Further, (14) is equivalent to

$$[x_2 + a^q/(\beta - \alpha)]^{q+1} = [a^{q+1} - (\beta - \alpha)(\gamma - \alpha)]/(\beta - \alpha)^2 \neq 0,$$

yielding $q + 1$ values for x_2.

We obtain, therefore, the same way as in (b), a configuration consisting of the two special points and $q - 1$ sets of $q + 1$ collinear points each; these $q - 1$ lines all contain $(1, 0, 0)$.

The noncollinearity of any other three points is an immediate consequence of Lemma 8.

Case II. $\alpha = \beta \neq \gamma$; (12) and (13) lead to

$$(\gamma - \beta) x_3^{q+1} + a^q x_2^q x_3 + a x_2 x_3^q = 0. \tag{27}$$

When $x_3 = 0$, (12) and (13) supply $q + 1$ collinear points. When $x_3 = 1$, (27) becomes

$$a^q x_2^q + a x_2 = \beta - \gamma. \tag{28}$$

(28) has q solutions. As in Case I, letting $x_2^{q+1} = -1$ in (28) yields (15). This gives the two special points. The remainder is as in Case I.

The situation $\alpha = \gamma \neq \beta$ is handled in the same manner.

Case III. $\alpha = \beta = \gamma$; this case cannot occur if q is even, because for even q, the characteristic polynomial of $\begin{pmatrix} \beta & a \\ a^q & \beta \end{pmatrix}$ is reducible over $GF(q)$.

From (12) and (13) we deduce that

$$a x_2 x_3^q + (a x_2 x_3^q)^q = 0. \tag{29}$$

The latter equation has q solutions for $x_2 x_3^q$. One of them is 0. Hence $x_3 = 0$ gives $q + 1$ collinear points and $x_3 = 1$ gives q values for x_2. As before, exactly two of the latter satisfy $x_2^{q+1} = -1$: letting $x_3 = 1$, $x_2^{q+1} = -1$ in (29) gives $x_2 = \pm a^{(q-1)/2}$ and both values meet the requirement.

(e) By Lemma 7, the system to solve is (12), together with

$$\lambda x_1^{q+1} + \lambda x_2^{q+1} + \lambda x_3^{q+1} + c^q x_1 x_2^q + c x_1^q x_2 + a^q x_2 x_3^q + a x_2^q x_3 = 0.$$

They lead to

$$t^q + t = 0, \tag{30}$$

where $t = x_2^q(c^q x_1 + a x_3)$. (30) has q solutions: $t = 0, w_1, w_2, \ldots, w_{q-1}$. The value $t = 0$ gives the line $x_2 = 0$ ($c^q x_1 + a x_3 = 0$ is not possible because it would entail, by (3), $x_1^{q+1} + x_3^{q+1} = 0$, contradiction). This line meets both unitals on $q + 1$ points.

When $t \neq 0$ we let $x_2 = 1$ and obtain $q - 1$ lines: $c^q x_1 + a x_3 = w_i x_2$, $i = 1(1)q - 1$. Each of them intersects $\{I\}$ on $q + 1$ points because (3) shows that the point $(c, (-w_i)^{1/q}, a^q)$ is not on $\{I\}$.

All things considered, we have q lines, all of which, moreover, contain $(-ac^{-q}, 0, 1)$. Lemma 8 ensures that no other three points are collinear.

(f) We make use of Lemma 2 with $m = 1$, $n = 0$. This gives one point.

(g) By Lemma 2 again—with $m = n = 0$—we obtain $q^2 - q + 1$ points. Let A be this $(q^2 - q + 1)$-set. By Lemma 1, A is the common intersection of $q + 1$ nondegenerate unitals: $\{I\}, \{H - \lambda I\}, \lambda \in GF(q)$. Therefore, if the line L meets A at $y \geqslant 2$ points, L must intersect each of the $q + 1$ unitals at $q + 1 - y$ points outside A. This, and the fact that the $q + 1$ unitals cover the plane, gives $(q + 1)(q + 1 - y) + y = q^2 + 1$, whence $y = 2$. □

BIBLIOGRAPHY

1. Birkhoff, G. and MacLane, S., *A Survey of Modern Algebra* (3rd edn), 1966.
2. Bose, R.C., 'On the Application of Finite Projective Geometry for Deriving a Certain Series of Balanced Kirkman Arrangements', *Calcutta Math. Soc. Golden Jubilee Vol.*, 1959, pp. 341–354.
3. Bose, R.C. and Chakravarti, I.M., 'Hermitian Varieties in a Finite Projective Space $PG(N, q^2)$', *Can. J. Math.* **18**, 1161–1182 (1966).
4. Dembowski, P., *Finite Geometries*, Springer-Verlag, N.Y. Inc., New York, 1968.
5. Kestenband, B., *Rank 3 matroid designs of prime power index and related designs*, Ph.D. Dissertation, The Graduate School of the City University of New York, 1975.
6. O'Nan, M.E., 'Automorphisms of Unitary Block Designs', *J. Alg.* **20**, 495–511 (1972).

Author's address:

Dept of Mathematics
New York Institute of Technology
Old Westbury, L.I.,
New York 11568
U.S.A.

(Received January 22, 1979)