COLLOQUIUM MATHEMATICUM

VOL. LVII 1989 FASC. 1

A FAMILY OF COMPLETE ARCS IN FINITE PROJECTIVE PLANES

BY

BARBU C. KESTENBAND (OLD WESTBURY, N. Y.)

A *k-cap* in a geometry is a set of k points no three of which are collinear ([5], p. 48). In a finite projective plane it is called a *k-arc*.

An arc is said to be *complete* if it is not properly contained in another arc ([5], p. 148).

In [9] we showed that under certain circumstances the intersection of two unitals in a projective plane $PG(2, q^2)$ is a (q^2-q+1)-arc. These arcs will be referred to as *unital-derived arcs*.

In a later article [10] we proved that the point set of $PG(2n, q^2)$ is a disjoint union of $(q^{2n+1}-1)/(q-1)$ caps, each containing $(q^{2n+1}+1)/(q+1)$ points. Furthermore, these caps, as "large points", form a $PG(2n, q)$ with the incidence relation defined in a natural way. In particular, $PG(2, q^2)$ is a disjoint union of a number of q^2+q+1 unital-derived arcs, constituting the "large points" of a $PG(2, q)$.

At the time that these papers were written we were unaware that the unital-derived arcs in $PG(2, q^2)$ are complete for $q > 2$. If $q = 2$, such an arc comprises three points, and therefore three lines joining them, but three nonconcurrent lines in $PG(2, 4)$ contain twelve points altogether, short of the twenty-one points of the plane.

Later on we demonstrated the completeness of the unital-derived arcs. This is an important fact for the following reason: it was proved long ago by B. Segre ([7], Theorem 10.3.3, p. 233) that in $PG(2, q)$, q even, the cardinality of a complete k-arc which is not an oval (i.e., for which $k < q+2$) satisfies $k \leqslant q-\sqrt{q}+1$, but it was not known whether this bound is sharp. Well, as it turns out, our unital-derived arcs provide the affirmative answer to this question for any $q = 4^m$, $m \geqslant 2$.

We learned, however, that the completeness of the unital-derived arcs was proved by other authors in two separate papers [2] and [6]. The proofs in both papers make use of a partition of $PG(2, q^2)$ into q^2-q+1 Baer subplanes.

Our proof is essentially different in that it is based on considering a new type of correlation of $PG(2, q^2)$, related to the well-known unitary polarities. From our viewpoint, the unital-derived arcs are the absolute points of these correlations (see below).

The general proofs in [2] and [6] are valid for $q \geqslant 4$, the case $q = 3$ being treated separately at the end of each proof. The approach in the present article includes all values of q in the general proof.

The notation we use in this paper is in keeping with [10].

A few well-known definitions are needed.

The points of a Desarguesian projective plane will be denoted by column vectors:

$$x = \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix}.$$

Thus $x^T = (x_1, x_2, x_3)$.

A *correlation* θ of a projective plane is a one-to-one mapping of its points onto its lines and its lines onto its points such that the point x is on line L if and only if the point L^θ is on line x^θ ([8], p. 90). The point a is an *absolute point* of θ if $a \in a^\theta$.

If $\theta^2 = 1$, θ is called a *polarity*.

$A = (a_{ij})$ being any matrix over the finite field $GF(q^2)$, we write $A^{(q)} = (a_{ij}^q)$. Also, A^{-T} will stand for the inverse of A^T.

A square matrix $H = (h_{ij})$ over $GF(q^2)$ is said to be *Hermitian* if $h_{ij}^q = h_{ij}$ for all i, j (see [4], p. 1161). This is equivalent to requiring that $H^T = H^{(q)}$. In particular, $h_{ii} \in GF(q)$. If H is Hermitian, then so is $p(H)$, where $p(x)$ is any polynomial with coefficients in $GF(q)$.

It is known that Desarguesian projective planes $PG(2, q^2)$ admit unitary polarities, which can be defined using Hermitian matrices [8]. A unitary polarity has q^3+1 absolute points, i.e., points that are incident with their own images.

Given a nondegenerate Hermitian matrix $H = (h_{ij})$, it defines a unitary polarity whose absolute points are precisely the q^3+1 points x that satisfy the equation

$$x^T H x^{(q)} = 0$$

or, in the explicit form

$$h_{11} x_1^{q+1} + h_{12} x_1 x_2^q + h_{12}^q x_1^q x_2 + h_{13} x_1 x_3^q + h_{13}^q x_1^q x_3 + h_{22} x_2^{q+1} + h_{23} x_2 x_3^q + h_{23}^q x_2^q x_3 + h_{33} x_3^{q+1} = 0.$$

The structure that is made up of the absolute points and the nonabsolute lines of a unitary polarity is called a *unital* ([8], p. 57). When we refer to a unital, we shall mean its point set.

In agreement with [10] we denote the set of points $\{x\colon x^T H x^{(q)} = 0\}$ by

$\{H\}$. It was shown in [10] that in order to obtain the (q^2-q+1)-arcs in question, one needs to consider a 3×3 Hermitian matrix H with characteristic polynomial $p_3(x)$ primitive irreducible over GF(q).

We then have $p_3(H)=\mathbf{0}$ and the Hermitian matrices H^j $(j=1, 2, \ldots, q^3-1)$ are the nonzero elements of a finite field GF(q^3). Its GF(q) subfield contains the scalar matrices aI_3, $a\in$GF(q).

It was also shown in [10] that if we consider the family

$$\chi=\{H^i\colon i=0, 1, \ldots, q^2+q\},$$

the polynomial $|H^r-\lambda H^s|$ has no roots in GF(q) for any distinct H^r, $H^s\in\chi$. Furthermore, the point set $\{H^r\}\cap\{H^s\}$ is a unital-derived arc and PG$(2, q^2)$ is a disjoint union of such arcs.

Let now H^r, $H^s\in\chi$, z be a primitive root of GF(q^2), and z^t any element of GF$(q^2)\backslash$GF(q). Then the matrix $K=z^tH^r+H^s$ is not a scalar multiple of a Hermitian matrix: if it were, then $(z^t/c)H^r+(1/c)H^s$ would be a Hermitian matrix for some $c\neq 0$. Let $H^r=(a_{ij})$, $H^s=(b_{ij})$ and put $\mu=z^t/c$, $\nu=1/c$. We now get

$$(\mu a_{ij}+\nu b_{ij})^q=\mu a_{ji}+\nu b_{ji}\quad \text{for all } i, j.$$

This becomes

$$(\mu-\mu^q)\,a_{ji}+(\nu-\nu^q)\,b_{ji}=0.$$

But the last equation implies $\mu=\mu^q$, $\nu=\nu^q$, because H^r, H^s are not scalar multiples of each other. Hence $\mu/\nu=(\mu/\nu)^q$, i.e., $\mu/\nu\in$GF(q), which is false, because $\mu/\nu=z^t\notin$GF(q) by assumption.

Having shown this, we use K to define a correlation θ of the projective plane:

$$(1)\qquad \boldsymbol{a}^\theta=\{\boldsymbol{x}\colon \boldsymbol{x}^TK\boldsymbol{a}^{(q)}=0\},\qquad \{\boldsymbol{x}\colon \boldsymbol{x}^T\boldsymbol{b}=0\}^\theta=K^{-T}\boldsymbol{b}^{(q)}.$$

Checking that θ is a correlation:

Let $\boldsymbol{c}\in\{\boldsymbol{x}\colon \boldsymbol{x}^T\boldsymbol{b}=0\}$, i.e., $\boldsymbol{c}^T\boldsymbol{b}=0$. Then we have to prove that

$$\{\boldsymbol{x}\colon \boldsymbol{x}^T\boldsymbol{b}=0\}^\theta\in\boldsymbol{c}^\theta,$$

which means that $(K^{-T}\boldsymbol{b}^{(q)})^TK\boldsymbol{c}^{(q)}=0$. This reduces to $\boldsymbol{b}^{(q)^T}\boldsymbol{c}^{(q)}=0$, which is equivalent to $\boldsymbol{c}^T\boldsymbol{b}=0$.

The converse is proved similarly.

Now θ^2 is a collineation and for any point $\boldsymbol{a}$ we have

$$(2)\qquad \boldsymbol{a}^{\theta^2}=\{\boldsymbol{x}\colon \boldsymbol{x}^TK\boldsymbol{a}^{(q)}=0\}^\theta=K^{-T}(K\boldsymbol{a}^{(q)})^{(q)}=K^{-T}K^{(q)}\boldsymbol{a}.$$

We claim that θ is not a polarity, i.e., that $\theta^2\neq 1$.

By (2) we have to prove that $K^{-T}K^{(q)}\neq lI_3$ for any l. Assume that $K^{-T}K^{(q)}=lI_3$; in other words, $K^{(q)}=lK^T$. This implies successively:

$$K=l^qK^{(q)^T}\Rightarrow K^T=l^qK^{(q)}\Rightarrow(l+1)K^T=(l^q+1)K^{(q)}$$

$$\Rightarrow[(l+1)K]^T=[(l+1)K]^{(q)}\Rightarrow(l+1)K \text{ is a Hermitian matrix.}$$

Thus, if $l \neq -1$, then K is a scalar multiple of a Hermitian matrix, which we know is false.

If $l = -1$, we get $K^{(q)} = -K^T$. Choose any nonzero $u \in \mathrm{GF}(q^2)$ that satisfies $u^{q-1} \neq 1$ and let $B = uK$. We then have

$$B^{(q)} = u^q K^{(q)} = -u^q K^T = -u^{q-1} B^T \neq -B^T.$$

Letting $-u^{q-1} = m$ we obtain $B^{(q)} = mB^T$, which leads, as before, to $(m+1)B = (m+1)uK$ being a Hermitian matrix, so K is again a scalar multiple of a Hermitian matrix. Therefore $\theta^2 \neq 1$.

By (1), the absolute points of θ are those points x which satisfy

$$x^T K x^{(q)} = 0, \quad \text{i.e.,} \quad z^t x^T H^r x^{(q)} + x^T H^s x^{(q)} = 0.$$

As $z^t \notin \mathrm{GF}(q)$, and since $x^T H^r x^{(q)}$ and $x^T H^s x^{(q)}$ are elements of $\mathrm{GF}(q)$, the last equation can only hold if

$$x^T H^r x^{(q)} = x^T H^s x^{(q)} = 0.$$

This discussion shows that the set of absolute points of θ is precisely $\{H^r\} \cap \{H^s\}$. This observation is valid in general: the intersections of nondegenerate unitals, which were exhaustively studied in [9], constitute the sets of absolute points of a special family of correlations: let H_1 and H_2 be two nondegenerate Hermitian matrices. Then the intersection $\{H_1\} \cap \{H_2\}$ is actually the set of absolute points of the correlation θ given by (1), where $K = H_1 + zH_2$, z is any element of $\mathrm{GF}(q^2)\backslash\mathrm{GF}(q)$. In particular, when $\{H_1\} \cap \{H_2\}$ contains one point (see [9]), the corresponding correlation has exactly one absolute point. This constitutes the first example of an infinite family of correlations with one absolute point. Until now only one very simple example has been known of a correlation with exactly one absolute point [1].

Back to our θ^2 defined by (2):

LEMMA 1. *The cyclic group $\langle\theta^2\rangle$ permutes all the points of* PG$(2, q^2)$ *in orbits of equal length, a divisor of q^2-q+1. Moreover, the orbit of each point is a subset of the (unique) unital-derived arc containing it.*

Proof. The characteristic polynomial of H is $p_3(x)$ with coefficients in, and irreducible over, $\mathrm{GF}(q)$. But a polynomial of odd degree with coefficients in $\mathrm{GF}(q)$ is irreducible over $\mathrm{GF}(q)$ if and only if it is irreducible over $\mathrm{GF}(q^2)$ (see [10], Lemma 3). So $p_3(x)$ is irreducible over $\mathrm{GF}(q^2)$ as well. As such, H defines a $\mathrm{GF}(q^6)$, call it Φ, the elements of which are matrices of the form $\varrho H^2 + \sigma H + \tau I_3$, $\varrho, \sigma, \tau \in \mathrm{GF}(q^2)$.

The $\mathrm{GF}(q^3)$ subfield of Φ consists precisely of the Hermitian matrices $\varrho H^2 + \sigma H + \tau I_3$, $\varrho, \sigma, \tau \in \mathrm{GF}(q)$; the $\mathrm{GF}(q^2)$ subfield comprises all scalar matrices τI_3, $\tau \in \mathrm{GF}(q^2)$.

Let the matrix N be a primitive root of Φ. Then N is non-Hermitian and $N^{q^6} = N$.

Let now $K = z^t H^r + H^s$, H^r, $H^s \in \chi$, $z^t \in \mathrm{GF}(q^2)\setminus \mathrm{GF}(q)$, as before. Then $K = N^v$ for some v.

K defines the correlation θ given by (1) and the collineation θ^2 determined by (2).

By (2) we have $a^{\theta^{2g}} = (K^{-T}K^{(q)})^g a$ for any g. Hence the orbit length of a given point a under $\langle \theta^2 \rangle$ is the smallest positive integer g for which a is an eigenvector of $(K^{-T}K^{(q)})^g$.

Since $K \in \Phi$, we have $K = \varrho H^2 + \sigma H + \tau I_3$ for some $\varrho, \sigma, \tau \in \mathrm{GF}(q^2)$, whence

$$K^{T(q)} = \varrho^q H^2 + \sigma^q H + \tau^q I_3.$$

It follows that $K + K^{T(q)}$ and $KK^{T(q)}$ are Hermitian matrices (check!). This in turn shows that if $K = N^v$, then $K^{T(q)} = N^{vq^3}$:

Assume, contrariwise, that $K^{T(q)} \neq N^{vq^3}$. Then $K^{T(q)} = N^{vq^3} + N^w$ for some integer w and we have

$$(K + K^{T(q)})^{q^3} = (N^v + N^{vq^3} + N^w)^{q^3} = N^{vq^3} + N^v + N^{wq^3},$$

$$(KK^{T(q)})^{q^3} = N^{vq^3}(N^{vq^3} + N^w)^{q^3} = N^{vq^3}(N^v + N^{wq^3}).$$

But $(K + K^{T(q)})^{q^3}$, $(KK^{T(q)})^{q^3}$ must equal $K + K^{T(q)}$, $KK^{T(q)}$, respectively, because they are Hermitian matrices, and thus belong to the $\mathrm{GF}(q^3)$ subfield of Φ. This gives first

$$N^{vq^3} + N^v + N^{wq^3} = N^v + N^{vq^3} + N^w,$$

whence $N^{wq^3} = N^w$. Next,

$$N^{vq^3}(N^v + N^{wq^3}) = N^v(N^{vq^3} + N^w),$$

which now reduces to

$$(N^{vq^3} - N^v)N^w = 0.$$

Here $N^{vq^3} \neq N^v$ because $K \notin \mathrm{GF}(q^3)$.

As no nonzero matrix in Φ is singular, the last equation cannot be valid, proving our assertion that

$$K = N^v \Rightarrow K^{T(q)} = N^{vq^3}.$$

This in turn leads to

$$K^{-T}K^{(q)} = (N^{-v})^T(N^{vq^3})^T = N^{v(q^3-1)^T}.$$

Therefore

$$(K^{-T}K^{(q)})^g = N^{gv(q^3-1)^T}. \tag{3}$$

Thus the orbit length of a point a is the smallest g for which a is an eigenvector of $N^{gv(q^3-1)^T}$.

For any integer w and any point $\boldsymbol{a}$, the vector $N^w \boldsymbol{a}$ has entries in the original $GF(q^2)$, because so do N and $\boldsymbol{a}$. Hence, if $\boldsymbol{a}$ is to be an eigenvector of N^w, the corresponding eigenvalue must be an element of $GF(q^2)$. On the other hand, if ξ is a characteristic root of N, then ξ^w is a characteristic root of N^w. The powers of ξ belonging to $GF(q^2)$ are of the form $\beta(q^6-1)/(q^2-1)$, β an integer. Thus the only powers of N whose characteristic roots are in $GF(q^2)$ are of the form $\beta(q^4+q^2+1)$.

But $N^{\beta(q^4+q^2+1)}$ is an element of the $GF(q^2)$ subfield of Φ, i.e.,

$$N^{\beta(q^4+q^2+1)} = \zeta I_3 \quad \text{for some } \zeta.$$

Thus for a certain point $\boldsymbol{a}$ to be an eigenvector of $N^{gv(q^3-1)^T}$, we must have $N^{gv(q^3-1)^T} = \zeta I_3$, and then all the points of the plane are eigenvectors. That is why the orbit length is the same for all the points.

Now, in order to find the common length, observe that

$$N^{gv(q^3-1)} = N^{\beta(q^4+q^2+1)},$$

whence the orbit length is the smallest positive number g for which

$$q^4+q^2+1 \mid gv(q^3-1) \quad \text{or} \quad q^2-q+1 \mid gv(q-1).$$

This yields

$$g = (q^2-q+1)/(q^2-q+1,\, v(q-1)). \tag{4}$$

Therefore, g is a divisor of q^2-q+1, as desired.

To prove the last claim of the lemma, let

$$\boldsymbol{a} \in \{H^r\} \cap \{H^s\}, \qquad H^r, H^s \in \chi.$$

We have to show that $\boldsymbol{a}^{\theta^2} \in \{H^r\} \cap \{H^s\}$ as well. By (2) we get

$$\boldsymbol{a}^{\theta^2} \in \{H^r\} \Leftrightarrow K^{-T} K^{(q)} \boldsymbol{a} \in \{H^r\} \Leftrightarrow (K^{-T} K^{(q)} \boldsymbol{a})^T H^r (K^{-T} K^{(q)} \boldsymbol{a})^{(q)} = 0$$
$$\Leftrightarrow \boldsymbol{a}^T K^{(q)T} K^{-1} H^r K^{-T(q)} K \boldsymbol{a}^{(q)} = 0.$$

Multiplication in Φ being commutative, the last equation can be reduced to $\boldsymbol{a}^T H^r \boldsymbol{a}^{(q)} = 0$, which holds by assumption.

Similarly, $\boldsymbol{a}^{\theta^2} \in \{H^s\} \Leftrightarrow \boldsymbol{a} \in \{H^s\}$, which completes the proof.

In the definition of $K = z^t H^r + H^s$, z^t can be chosen in q^2-q different ways. On the other hand, we have seen that, as a member of Φ, K can be written as $K = N^v$. Now we need to prove the following

LEMMA 2. *If* $K = z^t H^r + H^s = N^v$, *as* z^t *ranges through* $GF(q^2)\backslash GF(q)$, *the exponents* v *range through the nonzero residues modulo* q^2-q+1.

Proof. We have to show that $z^t \neq z^{t'}$ implies

$$v \not\equiv v' \pmod{q^2-q+1},$$

where

$$z^t H^r + H^s = N^v, \quad z^{t'} H^r + H^s = N^{v'}, \quad z^t, z^{t'} \in \mathrm{GF}(q^2)\backslash \mathrm{GF}(q).$$

Assume $v = v' + h(q^2 - q + 1)$ for some h. Then

$$z^t H^r + H^s = (z^{t'} H^r + H^s) N^{h(q^2-q+1)}. \tag{5}$$

But $N^{h(q^2-q+1)} = N^{h(q^4+q^2+1)} N^{-hq(q^3+1)}$.

Here, the first matrix on the right-hand side is a scalar matrix: its (q^2-1)-st power is $N^{h(q^6-1)}$, and since N is a primitive root of $\mathrm{GF}(q^6)$, the latter equals I_3. Hence $N^{h(q^4+q^2+1)} \in \mathrm{GF}(q^2)$, and all the elements of this subfield are scalar matrices.

The second matrix on the right-hand side is Hermitian, because it belongs to the $\mathrm{GF}(q^3)$ subfield of Φ. Hence $N^{h(q^2-q+1)} = z^c H^f$ for some c, f, and (5) becomes

$$z^t H^r + H^s = z^c (z^{t'} H^{r+f} + H^{s+f}). \tag{6}$$

Here, f is not a multiple of q^2+q+1, for if it were, H^f would be a scalar matrix aI_3 and (6) would then reduce to

$$(z^t - az^{c+t'}) H^r + (1 - az^c) H^s = 0.$$

As H^r, H^s are not linearly dependent, this gives $az^c = 1$, and then $z^t = z^{t'}$, in conflict with our assumption.

Next we show that if (6) holds, then

$$\{H^r\} \cap \{H^s\} = \{H^{r+f}\} \cap \{H^{s+f}\}. \tag{7}$$

Let $\boldsymbol{a} \in \{H^r\} \cap \{H^s\}$. This implies successively

$$\boldsymbol{a}^T H^r \boldsymbol{a}^{(q)} = \boldsymbol{a}^T H^s \boldsymbol{a}^{(q)} = 0 \Rightarrow \boldsymbol{a}^T (z^t H^r + H^s) \boldsymbol{a}^{(q)} = 0$$

$$\Rightarrow z^{t'} \boldsymbol{a}^T H^{r+f} \boldsymbol{a}^{(q)} + \boldsymbol{a}^T H^{s+f} \boldsymbol{a}^{(q)} = 0.$$

But $\boldsymbol{a}^T H^{r+f} \boldsymbol{a}^{(q)}$, $\boldsymbol{a}^T H^{s+f} \boldsymbol{a}^{(q)} \in \mathrm{GF}(q)$ (easy check) and unless they both vanish, we get the contradiction $z^{t'} \in \mathrm{GF}(q)$. Hence $\boldsymbol{a} \in \{H^{r+f}\} \cap \{H^{s+f}\}$. The converse is proved in a like manner. So (7) holds.

It was shown in [10], p. 1304, that the unitals under consideration and their intersections (the unital-derived arcs) can be viewed as the "large lines" and "large points", respectively, of a projective plane $\mathrm{PG}(2, q)$ with the incidence relation defined in a natural way: a large point is *incident* with a large line if and only if the points of the unital-derived arc belong to the unital. Now, if several lines are concurrent in a projective plane, any two of their equations are independent, but any of the other equations is a linear combination of those two.

Thus (7) can only hold if H^{r+f}, H^{s+f} are linear combinations of H^r, H^s. On the other hand, as was shown in [10], p. 1305, the exponents of H in the

$q+1$ linear combinations of H^r, H^s must form a Singer difference set with parameters (see [11])

$$v = q^2+q+1, \quad k = q+1, \quad \lambda = 1.$$

In our case the difference set must include r, s, $r+f$, $s+f$. As

$$f \not\equiv 0 \ (\mathrm{mod}\, q^2+q+1)$$

and also

$$r \not\equiv s \ (\mathrm{mod}\, q^2+q+1),$$

at least three of these four numbers are distinct modulo q^2+q+1; here is why:

If both $r \equiv s+f$ and $s \equiv r+f \ (\mathrm{mod}\, q^2+q+1)$, we get

$$2r \equiv 2s \ (\mathrm{mod}\, q^2+q+1),$$

i.e., $r \equiv s \ (\mathrm{mod}\, q^2+q+1)$, a contradiction.

If r, s, $r+f$, $s+f$ are all distinct, the difference f will occur twice, violating $\lambda = 1$. If, say, $r = s+f$, we have the three distinct numbers $s+f$, s, $s+2f$, so the difference f appears twice in any case.

This final contradiction completes the proof.

THEOREM. *If H^r, H^s are any two distinct Hermitian matrices in χ, the point set $\{H^r\} \cap \{H^s\}$ is a complete (q^2-q+1)-arc for any prime power $q > 2$.*

Proof. As a consequence of Lemma 2 (and this is why we proved it), z^t can be chosen so that

$$v \equiv 1 \ (\mathrm{mod}\, q^2-q+1).$$

In this case (4) yields $g = q^2-q+1$. Hence, for an appropriate choice of t, the group $\langle \theta^2 \rangle$, where θ is defined by (1), will be transitive on each of the unital-derived arcs that partition $\mathrm{PG}(2, q^2)$.

Assume now that a unital-derived arc, call it D, is incomplete; then there is a point $\boldsymbol{b} \notin D$ such that the lines $[\boldsymbol{b}, \boldsymbol{d}]$ are tangent to D for all $\boldsymbol{d} \in D$. The point $\boldsymbol{b}$ must belong to a Hermitian arc, say B. It can then be shown that, $\boldsymbol{d} \in D$ being fixed, the lines $[\boldsymbol{b}, \boldsymbol{d}]$ are tangent to D for all $\boldsymbol{b} \in B$:

By what has been found earlier, the points of B can be labelled $\boldsymbol{b}$, $\boldsymbol{b}^{\theta^{2i}}$, $i = 1, .., q^2-q$. Likewise the points of D.

If now for some i the line $[\boldsymbol{b}^{\theta^{2i}}, \boldsymbol{d}]$ met D at $\boldsymbol{d}^{\theta^{2j}}$ also, it would follow that the line $[\boldsymbol{b}, \boldsymbol{d}^{\theta^{-2i}}]$ intersects D again at $\boldsymbol{d}^{\theta^{2j-2i}}$, and this cannot be.

Since B has q^2-q+1 points, it takes at least $1+(q^2-q)/2$ distinct lines to join $\boldsymbol{d}$ to all the points in B and none of them meets D again. Then $\boldsymbol{d}$ is also incident with q^2-q lines within D. Besides, B and D are contained in a (unique) unital, because any two large points are contained in a unique large line by the axioms for projective geometry. Then through each point on a unital there passes exactly one line tangent to that unital [3], so d is contained in one more line.

Summing up, d is contained in at least $1+(q^2-q)/2+q^2-q+1$ lines. But this number is strictly greater than q^2+1 for $q > 2$, and the proof is completed.

COROLLARY. *The point set of a Desarguesian plane* $PG(2, q^2)$, $q > 2$, *is a disjoint union of* q^2+q+1 *complete unital-derived arcs.*

REFERENCES

[1] R. W. Ball, *Dualities of finite projective planes*, Duke Math. J. 15 (1948), pp. 929–940.

[2] E. Boros and T. Szőnyi, *On the sharpness of a theorem of B. Segre*, Combinatorica 6 (1986), pp. 261–268.

[3] R. C. Bose, *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.

[4] – and I. M. Chakravarti, *Hermitian varieties in a finite projective space* $PG(N, q^2)$, Canad. J. Math. 17 (1966), pp. 1161–1182.

[5] P. Dembowski, *Finite Geometries*, Springer-Verlag, N. Y., Inc., 1968.

[6] J. C. Fisher, J. W. P. Hirschfeld and J. A. Thas, *Complete arcs in planes of square order*, Ann. Discrete Math. 30 (1986), pp. 243–250.

[7] J. W. P. Hirschfeld, *Projective Geometries over Finite Fields*, Clarendon Press, Oxford 1979.

[8] D. R. Hughes and F. C. Piper, *Projective Planes*, Springer-Verlag, 1973.

[9] B. C. Kestenband, *Unital intersections in finite projective planes*, Geometriae Dedicata 11 (1981), pp. 107–117.

[10] – *Projective geometries that are disjoint unions of caps*, Canad. J. Math. 32 (1980), pp. 1299–1305.

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

NEW YORK INSTITUTE OF TECHNOLOGY
DEPT. OF MATHEMATICS
OLD WESTBURY, N.Y. 11568, U.S.A.

Reçu par la Rédaction le 25.4.1986;
en version modifiée le 3.9.1987