COMBINATORICA 6 (3) (1986) 261—268

ON THE SHARPNESS OF A THEOREM OF B. SEGRE

E. BOROS and T. SZŐNYI

Received 5 October 1984

The theorem of B. Segre mentioned in the title states that a complete arc of $PG(2, q)$, q even which is not a hyperoval consists of at most $q-\sqrt{q}+1$ points. In the first part of our paper we prove this theorem to be sharp for $q=s^2$ by constructing complete $q-\sqrt{q}+1$-arcs. Our construction is based on the cyclic partition of $PG(2, q)$ into disjoint Baer-subplanes. (See Bruck [1]). In his paper [5] Kestenband constructed a class of $(q-\sqrt{q}+1)$-arcs but he did not prove their completeness. In the second part of our paper we discuss the connections between Kestenband's and our constructions. We prove that these constructions result in isomorphic $(q-\sqrt{q}+1)$-arcs. The proof of this isomorphism is based on the existence of a traceorthogonal normal basis in $GF(q^3)$ over $GF(q)$, and on a representation of $GF(q)^3$ in $GF(q^3)^3$ indicated in Jamison [4].

Introduction

As usual (see Singer [9]) we represent $PG(2, q)$ as $GF(q^3) \bmod GF(q)$, q is a power of a prime. This means that the points of $PG(2, q)$ are the nonzero elements of $GF(q^3)$ and the elements x and y represent the same point of $PG(2, q)$ if and only if $x=\lambda y$ for some $\lambda \in GF(q)$. The point of $PG(2, q)$ represented by $x \in GF(q^3)$ will be denoted by (x).

Let us choose a self-dual basis in the vector space $GF(q^3)$ over $GF(q)$ (see Seroussi and Lempel [8]). The natural scalar product with respect to this basis can be given by $(a, b)=\mathrm{Tr}(a, b)$ where (a, b) denotes the scalar product of a and b and $\mathrm{Tr}(x)=x+x^q+x^{q^2}$. Then the lines of $PG(2, q)$ are the sets

$$[u] := \{(x) \in (GF(q^3) \bmod GF(q)) \mid \mathrm{Tr}(ux) = 0\} \quad \text{for} \quad u \in GF(q^3).$$

If ω is a primitive element of $GF(q^3)$ i.e. $GF(q^3)=\{0, \omega^0, \omega^1, \ldots, \omega^{q^3-2}\}$ then the points of $PG(2, q)$ can be identified with the set $\{1, \omega^1, \omega^2, \ldots, \omega^{q^2+q}\}$. Clearly the multiplication with ω induces a cyclic collineation on $PG(2, q)$.

If $q=s^2$ then cyclic partitions of $PG(2, q)$ can be given in two different ways: The subsets

$$\mathrm{Baer}(u) := \{\omega^{u+i(q-\sqrt{q}+1)} \mid i = 0, 1, \ldots, q+\sqrt{q}\}$$

for $u=0, 1, \ldots, q+\sqrt{q}$ form a cyclic partition of $PG(2, q)$ into disjoint subplanes

AMS subject classification (1980): 05 B 25, 51 E 15, 51 E 20

of order $\sqrt{q}$ (so called *Baer-subplanes*) (see Bruck [1] or Yff [11]). Moreover a line g of $PG(2, q)$ belongs to one (and only one) subplane Baer(u). (We say that the line g belongs to Baer(u) if $|g \cap \text{Baer}(u)| \geqq 2$).

The other natural cyclic partition of $PG(2, q)$ $(q = s^2)$ is related to arcs.

A *k-arc* is a set of k points in $PG(2, q)$ that has no three collinear points. A k-arc is said to be *complete* if there is no $(k+1)$-arc containing it. A line of $PG(2, q)$ is a *tangent* (*chord*) to the k-arc K if they have one (two) point(s) in common. $(q+1)$-arcs are called *ovals*, $(q+2)$-arcs are called *hyperovals*. If a complete k-arc is not a (hyper)oval, then

$$k \leqq q - \frac{\sqrt{q}}{4} + \frac{7}{4} \quad \text{for} \quad q \quad \text{odd},$$

$$k \leqq q - \sqrt{q} + 1 \quad \text{for} \quad q \quad \text{even}.$$

These estimations are due to B. Segre [7] who developed them using algebro-geometric methods, in particular the Hasse—Weil estimation. Recently J. A. Thas [10] proved this result for even q-s using only the Bèzout inequality.

The subsets $\text{Arc}(t) := \{\omega^{t+j(q+\sqrt{q}+1)} \mid j = 0, 1, \ldots, q-\sqrt{q}\}$ for $t = 0, 1, \ldots, q+\sqrt{q}$ form also a cyclic partition of $PG(2, q)$ if q is a square.

In the first part of this paper it is shown that these cyclic subsets are complete $(q-\sqrt{q}+1)$-arcs:

Theorem 1.1. *Let* $q = s^2$, $s \geqq 3$ *and* $0 \leqq t \leqq q+\sqrt{q}$. *Then* $\text{Arc}(t)$ *is a complete* $(q-\sqrt{q}+1)$*-arc of* $PG(2, q)$.

In his paper Kestenband [5] characterizes the intersections of unitals (Hermitian curves). He shows that if two unitals have $q-\sqrt{q}+1$ points in common then these points form an arc. However the completeness of these arcs is not proved in [5].

Using a trace-orthogonal normal basis of $GF(q^3)$ over $GF(q)$ (Lemma 2.7) the following theorem is proved in the second part of this paper.

Theorem 2.9. *Let* $q = s^2$. *Then every* $(q-\sqrt{q}+1)$*-arc which is the intersection of two unitals is projectively equivalent to* $\text{Arc}(o)$, *hence it is complete if* $s > 2$.

Results on the structure of unitals also follows.

Whenever possible, we use the standard notations, cf. e.g. Hirschfeld [3] or Lidl—Niederreiter [6].

1. The construction of cyclic complete $(q-\sqrt{q}+1)$-arcs

The cyclic collineation mentioned above will be the mapping $T: \omega^i \to \omega^{i+1}$ induced by the multiplication with the primitive element ω.

The mapping $S: x \to x^{s^3}$ is an involutory automorphism of $GF(q^3)$ hence it induces an involutory collineation of $PG(2, q)$. The fixed points of this Baer-involution are exactly the points of the Baer-subplane Baer(0).

Before the proof of Theorem 1.1 we need two lemmas.

Lemma 1.2. $|\mathrm{Arc}(0)\cap\mathrm{Baer}(u)|=1$ for every u.

Proof. Let $\omega^x, \omega^y\in\mathrm{Arc}(0)\cap\mathrm{Baer}(u)$. From the definitions of Arc (0) and Baer (u) it follows that $q-\sqrt{q}+1$ and $q+\sqrt{q}+1$ both divide $x-y$, and since they are relatively prime, q^2+q+1 is a divisor of $x-y$. Hence ω^x and ω^y represent the same point of PG$(2, q)$. As the number of distinct Baer-subplanes of form Baer $(u)=$ $=|\mathrm{Arc}(0)|=q-\sqrt{q}+1$ the lemma immediately follows. ∎

Lemma 1.3. *Let g be an arbitrary line of* Baer (u) *not containing* $x\in\mathrm{Arc}(0)\cap\mathrm{Baer}(u)$. *Then* $|g\cap\mathrm{Arc}(0)|$ *is even.*

Proof. First we prove the lemma for $u=0$.

The involutory collineation $S: x\to x^{s^3}$ fixes Baer (0) pontwise and Arc (0) setwise because

$$\omega^{j(q+\sqrt{q}+1)}S=\omega^{(q-\sqrt{q}+1-j)(q+\sqrt{q}+1)}.$$

Therefore $\mathrm{Arc}(0)\setminus\{\omega^0\}$ is divided into disjoint pairs under the action of S. Since g is a line of Baer (0), $gS=g$, so $(g\cap\mathrm{Arc}(0))S=(gS)\cap(\mathrm{Arc}(0)S)=(g\cap\mathrm{Arc}(0))$ and since $\omega^0\notin g$ the intersection $g\cap\mathrm{Arc}(0)$ contains both members of certain pairs of Arc (0).

Now the lemma follows by applying the collineation $T^{u(q-\sqrt{q}+1)}$ that maps Baer (0) into Baer (u) and fixes Arc (0) setwise. ∎

Proof of Theorem 1.1. Since Arc(t) can be obtained from Arc(0) by applying the t^{th} power of the cyclic collineation T, it is sufficient to prove that Arc (0) is a complete arc.

First we show that Arc (0) is an arc.

From Lemma 1.3. it follows that among the lines of the subplane Baer (u) only those $\sqrt{q}+1$ lines could be tangents to Arc (0) which are incident to $x\in\mathrm{Arc}(0)\cap$ $\cap\mathrm{Baer}(u)$. So Arc (0) has at most $(\sqrt{q}+1)(q-\sqrt{q}+1)$ tangents. On the other hand $|\mathrm{Arc}(0)|=q-\sqrt{q}+1$ and so at least $q+1-(q-\sqrt{q})=\sqrt{q}+1$ tangents pass through every point of Arc (0). Therefore Arc (0) has at least $(\sqrt{q}+1)(q-\sqrt{q}+1)$ tangent lines. This means that the number of tangents is exactly $(\sqrt{q}+1)(q-\sqrt{q}+1)$, and the tangents of Arc (0) at $x\in\mathrm{Arc}(0)\cap\mathrm{Baer}(u)$ are the lines of Baer (u) containing x.

Now let g be a line of Baer(v) $(v\neq u)$ through $x\in\mathrm{Arc}(0)\cap\mathrm{Baer}(u)$. From $x\in g$ and $x\notin\mathrm{Baer}(v)$ it follows that g is not a tangent to Arc (0), so by Lemma 1.3. $|g\cap\mathrm{Arc}(0)|\geqq 2$. Since the number of such lines is $q-\sqrt{q}$, $|g\cap\mathrm{Arc}(0)|=2$ for every non-tangent line through x. This proves that Arc (0) is indeed an arc.

Next we show the completeness of Arc (0). Suppose indirectly that there is a point $x\in\mathrm{Arc}(t)$ $t\neq 0$ for which $\mathrm{Arc}(0)\cup\{x\}$ is also an arc. The collineation group $\{T^{j(q+\sqrt{q}+1)}\mid j=0, 1, \ldots, q-\sqrt{q}\}$ leaves Arc (0) invariant and acts transitively on the points of Arc (t), hence for every $y\in\mathrm{Arc}(t)$: $\mathrm{Arc}(0)\cup\{y\}$ will be an arc, too. This means that for every $x\in\mathrm{Arc}(0)$ and $y\in\mathrm{Arc}(t)$ the line g joining them is a tangent to Arc (0). Since Arc (t) is also an arc, $|g\cap\mathrm{Arc}(t)|\leqq 2$. From this it

follows that at least $(q-\sqrt{q}+1)/2$ tangents pass through a point x of Arc (0). But this is a contradiction for $s>3$ since $(q-\sqrt{q}+1)/2>\sqrt{q}+1$ if $s>3$.

In the case $q=4$ Arc $(0)=\{\omega^0, \omega^7, \omega^{14}\}$ cannot be complete but for $q=9$ an explicit calculation shows that Arc $(0)=\{\omega^0, \omega^{13}, \omega^{26}, \omega^{39}, \omega^{52}, \omega^{65}, \omega^{78}\}$ will be a complete arc. ∎

2. Cyclic arcs and intersections of unitals

In this section the connections between cyclic arcs and intersections of unitals will be investigated.

Consider the natural homogenous coordinates in PG$(2, q)$ $(q=s^2)$, i.e. the points of the plane are represented by the vectors $\underline{x}=(x_0, x_1, x_2)$ of GF$(q)^3$. Then the unitals are exactly the curves defined by the equation $\underline{x}^s H \underline{x}'=0$, where $\underline{x}^s=(x_0^s, x_1^s, x_2^s)$ is the conjugate of $\underline{x}$ and $H=(h_{ij})$ is an Hermitian matrix, i.e. $h_{ij}=h_{ij}^s$ for $0\leqq i, j\leqq 2$.

Remark 2.1. Kestenband shows in [5] that the intersection of two arbitrary unitals is projectively equivalent to the intersection of unitals given by $\underline{x}^s I \underline{x}'=0$ and $\underline{x}^s H \underline{x}'=0$, where I is the unit matrix and H is an Hermitian matrix. Moreover he proves that if this intersection contains exactly $q-\sqrt{q}+1$ points then it forms an arc and the characteristic polynomial of H is irreducible over GF(q).

First we show that the cyclic arcs can be given as intersections of unitals, too.

We remark that a line $[u]$ belongs to Baer(0) if and only if $(u)\in$Baer(0).

Lemma 2.2. *Let* $(a)\in$Baer(0) *and* $U(a)=\{(x)|\mathrm{Tr}(ax^{q\sqrt{q}+1})=0\}$. *Then* $U(a)$ *is a unital.*

Proof. Consider the mapping $\pi_a: (x)\to[ax^{q\sqrt{q}}]$, $[u]\to(a^{-1}u^{q\sqrt{q}})$. It is easy to check that π_a is a correlation and it will be a polarity if and only if (a) belongs to Baer(0). If (x) and (y) are absolute points of π_a then the line joining them contains $\sqrt{q}+1$ absolute points, so π_a is a unitary polarity for $(a)\in$Baer(0) and its absolute points form the unital $U(a)$. ∎

Lemma 2.3. *If the arc* Arc(t) *and the unital* $U(a)$ *have a common point, then* Arc(t) *is contained in* $U(a)$.

Proof. Let (x) be a common point of Arc(t) and $U(a)$, then any further point of Arc(t) can be represented by $y=x\omega^{i(q+\sqrt{q}+1)}$. Then we have

$$\mathrm{Tr}(ay^{q\sqrt{q}+1}) = \mathrm{Tr}(ax^{q\sqrt{q}+1}\,\omega^{i(q+\sqrt{q}+1)(q\sqrt{q}+1)}) =$$

$$= \omega^{i(q+\sqrt{q}+1)(q\sqrt{q}+1)}\,\mathrm{Tr}(ax^{q\sqrt{q}+1}) = 0$$

because $\omega^{i(q+\sqrt{q}+1)(q\sqrt{q}+1)}=\omega^{i(q^2+q+1)(\sqrt{q}+1)}$ belongs to GF(q) and $\mathrm{Tr}(ax^{q\sqrt{q}+1})=0$ as $(x)\in U(a)$. Hence $(y)\in U(a)$. ∎

Corollary 2.4. *An arbitrary unital of* $\mathrm{PG}(2, q)$, $q=s^2$ *can be partitioned into disjoint cyclic* $(q-\sqrt{q}+1)$*-arcs.* ∎

Theorem 2.5. *Let* (x) *be a point of* $\mathrm{Arc}(t)$. *Then* $\mathrm{Arc}(t)$ *is the intersection of any pair of the* $\sqrt{q}+1$ *unitals* $U(a)$ *with* $(a)\in\mathrm{Baer}(0)\cap[x^{q\sqrt{q}+1}]$.

Remark 2.6. It follows from the theorem of Kestenband [5] that exactly these unitals contain $\mathrm{Arc}(t)$, because his theorem implies that the intersection of two unitals cannot contain a $(q-\sqrt{q}+1)$-arc whenever they intersect in more than $q-\sqrt{q}+1$ points.

Proof of Theorem 2.5. If (a) is a point of the line $[x^{q\sqrt{q}+1}]$ i.e. $\mathrm{Tr}(ax^{q\sqrt{q}+1})=0$, then $(x)\in U(a)$, and $U(a)$ is a unital if $(a)\in\mathrm{Baer}(0)$ by Lemma 2.2. As $(x^{q\sqrt{q}+1})$ belongs to $\mathrm{Baer}(0)$ the line $[x^{q\sqrt{q}+1}]$ is a line of $\mathrm{Baer}(0)$, hence $[x^{q\sqrt{q}+1}]$ meets $\mathrm{Baer}(0)$ in $\sqrt{q}+1$ points. Thus we get $\sqrt{q}+1$ unitals $U(a)$ containing (x), and hence by Lemma 2.3. $\mathrm{Arc}(t)$ is contained by all these unitals. Then the Theorem follows by Remark 2.6. ∎

For the strengthening of this theorem a special basis of $\mathrm{GF}(q^3)$ over $\mathrm{GF}(q)$ is needed.

Lemma 2.7. *For any prime-power* q *there is a traceorthogonal normal basis of* $\mathrm{GF}(q^3)$ *over* $\mathrm{GF}(q)$, *i.e. there is an element* $d\in\mathrm{GF}(q^3)$ *satisfying*

(i) d, d^q, d^{q^2} *are independent elements over* $\mathrm{GF}(q)$

(ii) $\mathrm{Tr}(d^{q+1})=0$, *and*

(iii) $\mathrm{Tr}(d^2)=\sigma\neq 0$.

Proof. Let $L=\{(x)\in\mathrm{GF}(q^3)\bmod\mathrm{GF}(q)\,|\,\mathrm{Tr}(x)=0\}$. According to Singer [9] this is a difference basis in the multiplicative group $\mathrm{GF}(q^3)$ mod $\mathrm{GF}(q)$, i.e.

$$\text{if } xy^{-1}=uv^{-1} \text{ then } (x)=(y) \text{ or } (x)=(u), \tag{2.1}$$

whenever x, y, u, v are elements of L.

We distinguish two cases:

Case a. $3\nmid q-1$.

Let $(x)\in L$ be an arbitrary element, $x\notin\mathrm{GF}(q)$ and let $d=x^{q+1}$. We prove that d satisfies the required conditions.

First we show that $\mathrm{Tr}(d)\neq 0$. Assume indirectly that $\mathrm{Tr}(d)=0$. Then x, x^q, x^{q^2} and $x^{q+1}, x^{q^2+q}, x^{1+q^2}$ are all elements of L. Now $(x^{q+1})\neq(x^q)$ as $x\notin\mathrm{GF}(q)$ and $(x^q)\neq(x^{q^2})$ as $3\nmid q-1$. Thus the equation $x^{q+1}\cdot(x^q)^{-1}=x^{1+q^2}\times$ $\times(x^{q^2})^{-1}$ is a contradiction by (2.1). Next we prove that $\{d, d^q, d^{q^2}\}$ is a basis over $\mathrm{GF}(q)$. Since $3\nmid q-1$, the elements d^q-d and $d^{q^2}-d^q$ are independent over $\mathrm{GF}(q)$, hence from the dependence of d, d^q and d^{q^2} the relation $d=\alpha(d^q-d)+\beta(d^{q^2}-d^q)$ would follow for some $\alpha, \beta\in\mathrm{GF}(q)$. Thus $\mathrm{Tr}(d)=\alpha\,\mathrm{Tr}(d^q-d)+\beta\,\mathrm{Tr}(d^{q^2}-d^q)=0$, as a contradiction.

In order to prove (ii) we calculate $\mathrm{Tr}(d^{q+1})$. $\mathrm{Tr}(d^{q+1})=\mathrm{Tr}(x^{(q+1)^2})=$ $=\mathrm{Tr}(x^{q^2+q+1}\cdot x^q)=x^{q^2+q+1}\,\mathrm{Tr}(x^q)=0$, since $x^q\in L$ and $x^{q^2+q+1}\in\mathrm{GF}(q)$.

Finally we prove $\mathrm{Tr}(d^2)\neq 0$ indirectly. It follows from $\mathrm{Tr}(d^2)=0$ that d^2, d^{2q}, d^{2q^2} and $d^{q+1}, d^{q^2+q}, d^{1+q^2}$ are elements of L. Now $(d^2)\neq(d^{q+1})\neq(d^{2q})$ as $3\nmid q-1$, thus $d^{q+1}\cdot(d^2)^{-1}=d^{2q}\cdot(d^{q+1})^{-1}$ gives a contradiction by (2.1).

Case b. $3|q-1$.

Let ω be a primitive element of $\mathrm{GF}(q^3)$ and let $\tau=\omega^{q^2+q+1}$, $y_i=\omega^{i(q^2+q+1)/3}$, $\lambda_i=\tau^{i(q-1)/3}$ for $i=1, 2$. The following relations can easily be verified.

$$y_1^2=y_2,\quad y_1y_2=\tau,\quad y_2^2=\tau y_1.$$

$$y_i^q=\lambda_i y_i \quad \text{for} \quad i=1,2 \quad \text{and} \tag{2.2}$$

$$\lambda_1^3=\lambda_2^3=1,\quad \lambda_1\lambda_2=1,\quad \lambda_1+\lambda_2=-1.$$

Let α, β be arbitrary nonzero elements of $\mathrm{GF}(q)$ and let $d=\alpha^2y_2+\beta^2\tau y_1-\alpha\beta\tau$. It can be proved that d satisfies the required conditions.

Clearly $(y_1)\neq(y_2)$ and $\mathrm{Tr}(y_i)=(1+\lambda_i+\lambda_i^2)y_i=0$ for $i=1, 2$. Since $1\notin L$, $\{1, y_1, y_2\}$ is a basis of $\mathrm{GF}(q^3)$ over $\mathrm{GF}(q)$. Then using (2.2) d, d^q and d^{q^2} can be expressed as follows:

$$d=\alpha^2y_2+\beta^2\tau y_1-\alpha\beta\tau,$$

$$d^q=\alpha^2\lambda_2y_2+\beta^2\tau\lambda_1y_1-\alpha\beta\tau, \tag{2.3}$$

$$d^{q^2}=\alpha^2\lambda_2^2y_2+\beta^2\tau\lambda_1^2y_1-\alpha\beta\tau.$$

(2.3) means that $\{d, d^q, d^{q^2}\}$ can be obtained from $\{y_1, y_2, 1\}$ by a linear transformation. Since the determinant of this transformation is $3\alpha^2\beta^2\tau^2(\lambda_1-\lambda_2)\neq 0$ and $y_1, y_2, 1$ are independent over $\mathrm{GF}(q)$ we have (i).

To prove (ii) we start with $\mathrm{Tr}(d^{q+1})=\mathrm{Tr}(d^qd)$. Then applying (2.2) and (2.3) we get

$$\mathrm{Tr}(d^{q+1})=\mathrm{Tr}\big((\alpha^2y_2+\beta^2\tau y_1-\alpha\beta\tau)(\alpha^2\lambda_2y_2+\beta^2\tau\lambda_1y_1-\alpha\beta\tau)\big)=$$

$$=\mathrm{Tr}\big(\alpha^2\beta^2\tau^2(\lambda_1+\lambda_2+1)\big)=0.$$

Finally, again by (2.2) and (2.3)

$$\mathrm{Tr}(d^2)=\mathrm{Tr}\big((\alpha^2y_2+\beta^2\tau y_1-\alpha\beta\tau)\big)=\mathrm{Tr}(3\alpha^2\beta^2\tau^2)=9\alpha^2\beta^2\tau^2\neq 0,$$

which proves (iii). ∎

In the following we need an explicit description of an isomorphism φ between $\mathrm{GF}(q)^3$ and $P=\{(x, x^q, x^{q^2})|x\in\mathrm{GF}(q)\}$. Then φ gives an isomorphism between $\mathrm{PG}(2, q)$ and $\bar{P}=\{(x, x^q, x^{q^2})|x\in\mathrm{GF}(q^3)^*\bmod\mathrm{GF}(q)\}$, too. This representation of $\mathrm{GF}(q)^3$ in $\mathrm{GF}(q^3)^3$ was indicated in Jamison [4, pp. 258—259]. He observed that the linear mappings of the vector space $\mathrm{GF}(q)^3$ can be obtained in this representation by applying matrices of the form

$$[A, B, C]=\begin{pmatrix} A & B & C \\ C^q & A^q & B^q \\ B^{q^2} & C^{q^2} & A^{q^2}\end{pmatrix}$$

where $A, B, C\in\mathrm{GF}(q)$.

Now let $\{d, d^q, d^{q^2}\}$ be a self-orthogonal normal basis of $GF(q^3)$ over $GF(q)$ given by Lemma 2.7., and let

$$D = \begin{pmatrix} d & d^q & d^{q^2} \\ d^q & d^{q^2} & d \\ d^{q^2} & d & d^q \end{pmatrix}$$

be a circulant matrix. Then for every $\xi \in GF(q)^3$ let $\varphi(\xi) = D\xi$ be the corresponding of P. It is clear that φ is linear over $GF(q)$ and, as $D^2 = \sigma I$, the inverse of φ can be defined for every $\underline{x} \in P$ as $\varphi^{-1}(\underline{x}) = \sigma^{-1} D\underline{x}$. Hence φ is an isomorphism between $GF(q)^3$ and P. Therefore φ can naturally be extended to the linear transformations by conjugation with D, i.e. for any linear transformation T of $GF(q)^3$ let $\varphi(T) = \sigma^{-1} DTD$ be the corresponding linear transformation of P.

Remark 2.8. *φ has the following properties*:

(i) $\varphi(I) = [1, 0, 0,]$.

(ii) $(\varphi(\underline{\alpha}), \varphi(\underline{\beta})) = \sigma(\underline{\alpha}, \underline{\beta})$, *thus φ preserves the collinearity as a* $PG(2, q) \to P$ *mapping.*

(iii) $\det(\varphi(T)) = \det(T)$.

(iv) $\underline{\xi} \in GF(q)$ *is an eigenvector of the linear transformation T corresponding to the eigenvalue $\lambda \in GF(q)$ if and only if $\varphi(\xi) - \sigma^{-1} D\xi$ is an eigenvector of $\varphi(T)$ with the eigenvalue $\lambda \in GF(q)$. Consequently $\varphi(T)$ has the same characteristic polynomial as T has.*

(v) *If* $\varphi(T) = [A, B, C]$ *then* $\varphi(T') = [A, C^q, B^{q^2}]$ *i.e.* $\varphi(T') = (\varphi(T))'$.

(vi) *If* $q = s^2$, $d \in GF(s)$ *and* $\varphi(T) = [A, B, C]$ *then* $\varphi(\overline{T}) = [A^s, B^s, C^s] = \overline{\varphi(T)}$, *where $\overline{U}$ denotes the conjugate of the matrix U.*

(vii) *Let* $q = s^2$ *and* $d \in GF(s)$, *then T is Hermitian if and only if* $A \in GF(s)$ *and* $B^s = C$ *hold for* $\varphi(T) = [A, B, C]$. ∎

Theorem 2.9. *Let $q = s^2$. Then every $(q - \sqrt{q} + 1)$-arc which is the intersection of two unitals is projectively equivalent to* Arc(0), *hence it is complete.*

Proof. Choose $d \in GF(s)$ according to Lemma 2.7 and consider the isomorphism $\varphi: GF(q)^3 \to P$ described above, and the unitals $U_1 = \{\underline{x} \in GF(q)^3 | \underline{x}^s I \underline{x}' = 0\}$ and $U_2 = \{\underline{x} \in GF(q)^3 | \underline{x}^s H \underline{x}' = 0\}$ as in Remark 2.1. Moreover let $H = [A, B, C]$.

The matrices H and so by virtue of (vii) Remark 2.8. $[A, B, C]$ are Hermitian, hence the coefficients of their characteristic polynomial f (see (iv) of Remark 2.8) belong to $GF(s)$. Therefore the roots $\lambda, \lambda^q, \lambda^{q^2}$ of f are contained in $GF(s^3)$. It follows from the irreducibility of f (see Remark 2.1) that these eigenvalues of H and so of $[A, B, C]$ belong to $GF(s^3) \setminus GF(q)$, moreover λ, λ^q and λ^{q^2} are pairwise different, otherwise $\lambda \in GF(s)$ would follow.

Now a linear mapping V can be constructed that acts on $\bar{P}$ and transforms $\varphi(U_1) = U(1)$ into itself and $\varphi(U_2)$ into $U(\lambda)$ (for the notation see Lemma 2.2). Hence $U_1 \cap U_2$ is projectively equivalent to $U(1) \cap U(\lambda)$ proving the statement by Theorem 2.5.

For the construction of V consider an arbitrary right-eigenvector $(x, y, z)' \in GF(q^3)^3$ of the matrix $[A, B, C]$ corresponding to the eigenvalue λ. Then the vectors $(z^q, x^q, y^q)'$ and $(y^{q^2}, z^{q^2}, x^{q^2})'$ are right-eigenvectors of $[A, B, C]$ corresponding to

the eigenvalues λ^q, λ^{q^2}. Let W be the matrix formed by these vectors as column vectors, i.e. $W=[x, y, z]'$. As H (and hence $[A, B, C]$) is Hermitian, the rows of W^* ($W^*=\overline{W}'$ is the adjoint of W) are the left-eigenvectors of $[A, B, C]$ corresponding to the eigenvalues λ, λ^q and λ^{q^2}.

It is well-known that a left-eigenvector is orthogonal to a right-eigenvector if they correspond to different eigenvalues. Hence $W^*W=\mu[1, 0, 0]$ and $W^*[A, B, C]W=\mu[\lambda, 0, 0]$ for some element μ of GF(q).

Then the theorem follows from these equations with $V=W^*$. ∎

Added in proof: The results of Section 1, Corollary 2.4, and Theorem 2.5 were proved independently by Fisher, Hirschfeld, and Thas, at the same time [12].

References

[1] R. H. BRUCK, Quadratic extension of cyclic planes, *Proc. Symp. in Appl. Math. (X)*, 1960, (ed. by R. BELLMAN and M. HALL Jr.), 15—44.
[2] M. HALL, Jr., Cyclic projective planes, *Duke Math. Journal* **14** (1947), 1079—1090.
[3] J. W. P. HIRSCHFELD, *Projective Geometries over Finite Fields*, Clarendon Press, Oxford, 1979.
[4] R. E. JAMISON, Covering finite fields with cosets of subspaces, *Journ. Comb. Th. (A)* **22** (1977), 253—266.
[5] B. C. KESTENBAND, Unital intersections in finite projective planes, *Geometriae Ded.* **11** (1981), 107—117.
[6] R. LIDL and H. NIEDERREITER, *Finite Fields, Encyclopaedia of Math.* **20**, Addison—Wesley, 1983.
[7] B. SEGRE, Introduction to Galois geometries, (ed. by J. W. P. HIRSCHFELD), *Memorie Accad. Naz. Lincei (VIII)*, **5** (1967), 133—236.
[8] G. SEROUSSI and A. LEMPEL, Factorization of symmetric matrices and trace-orthogonal bases in finite fields, *SIAM J. Computing* **9** (1980), 758—767.
[9] J. SINGER, A theorem in finite projective geometry and some applications to number theory, *Trans. Amer. Math. Soc.* **43** (1938), 377—385.
[10] J. A. THAS, Elementary proofs of two fundamental theorem of B. Segre without using the Hasse—Weil theorem, *Journ. of Comb. Th. (A)* **34** (1983), 381—348.
[11] P. YFF, On subplane partition of a finite projective plane, *Journal of Comb. Th. (A)* **22** (1977), 118—122.
[12] J. C. FISHER, J. W. P. HIRSCHFELD and J. A. THAS, Complete arcs in planes of square order, *Annals of Discrete Math.*, **30** (1986), 243—250.

Endre Boros and Tamás Szőnyi

Computer and Automation Institute
Hungarian Academy of Sciences
Budapest, Hungary