Math. Proc. Camb. Phil. Soc. (1988), **104**, 435
Printed in Great Britain

Partitioning projective planes into arcs

By BARBU C. KESTENBAND
Department of Mathematics, New York Institute of Technology, New York 11568, *U.S.A.*

(*Received* 13 *October* 1987; *revised* 4 *January* 1988)

We show how to partition certain classes of finite projective planes into equicardinal arcs. Several partitions of this kind are to be found in the recent literature and they have aroused a certain amount of interest on two counts, as we shall shortly see.

A *t-cap* in a geometry is a set of t points no three of which are collinear, and a t-cap in a plane is called a *t-arc*. An arc is called *complete* if it is not properly contained in another arc.

In [7] we showed that a Desarguesian projective geometry $\mathrm{PG}(2n, q^2)$ is a disjoint union of $(q^{2n+1}-1)/(q-1)$ caps, each cap consisting of $(q^{2n+1}+1)/(q+1)$ points. It was further proved that these caps constitute the 'large points' of a geometry $\mathrm{PG}(2n, q)$ with the incidence relation defined in a natural way.

For $n = 1$ we have that $\mathrm{PG}(2, q^2)$ is a disjoint union of q^2+q+1 arcs, each of cardinality q^2-q+1. These (q^2-q+1)-arcs are also complete, as has been proved in three different papers [**1**, **4**, **8**]. This fact is important in that it settles (for q even) an old question raised by a theorem of B. Segre (see [**5**], p. 233). He showed that in $\mathrm{PG}(2, q)$, for q even, the cardinality of a complete 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 was sharp. The arcs that we constructed, being complete (for any $q \geqslant 3$, even or not) and having the required cardinality, provide the affirmative answer (for q even).

For q odd, the problem is more complicated, in that complete k-arcs with $k > q-\sqrt{q}+1$ are known to exist (e.g. for $q = 9$ there are complete 8-arcs). For an up-to-date survey of this problem, see [**10**].

On the other hand, G. L. Ebert [**3**] has found a new method of proof for the results in [**7**], which further enabled him to partition $\mathrm{PG}(2n-1, q)$, with n an even number and q any prime power, into $(q^n-1)/(q-1)$ equicardinal caps; these (q^n+1)-caps are the 'large points' of a $\mathrm{PG}(n-1, q)$ with a natural incidence relation. In turn, this partition leads to a new family of balanced incomplete block designs, as shown in [**3**].

Our new result is summed up in the theorem below. However we need to introduce a few definitions and the appropriate notation first.

If A is an invertible matrix, we write A^{-T} for $(A^{-1})^T$.

Next, $A = (a_{ij})$ being any matrix over a field, we write $A^{\phi} = (a_{ij}^{\phi})$, where ϕ stands for a map from the field to itself. If $a_{ij}^{\phi} = a_{ij}^{s}$ (raising to the power s), then we write $A^{(s)} = (a_{ij}^{s})$.

A square matrix $H = (h_{ij})$ over the finite field $\mathrm{GF}(q^2)$, where q is a prime power, is said to be Hermitian over $\mathrm{GF}(q^2)$ if $h_{ij}^{q} = h_{ji}$ for all i, j. This is equivalent to requiring that $H^{(q)} = H^T$. It implies in particular that $h_{ii} \in \mathrm{GF}(q)$ for each i. If H is Hermitian,

https://doi.org/10.1017/S0305004100065634 Published online by Cambridge University Press

so is $p(H)$, where p is any polynomial with coefficients in GF(q). A symmetric matrix over GF(q) is Hermitian over GF(q^2) because $z^q = z$ for all $z \in$ GF(q).

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

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

A *correlation* θ of a projective plane is a one-to-one mapping of its points onto its lines and its lines on to its points, such that a point $\mathbf{x}$ is on line L if and only if the point L^θ is on line $\mathbf{x}^\theta$.

To any correlation θ of a Desarguesian plane there corresponds a non-singular matrix A and an automorphism ϕ of the underlying field, such that θ can be represented as follows:

$$\mathbf{a}^\theta = \{\mathbf{x} : \mathbf{x}^T A \mathbf{a}^\phi = 0\}, \quad \{\mathbf{x} : \mathbf{x}^T \mathbf{b} = 0\}^\theta = A^{-T} \mathbf{b}^\phi; \tag{1}$$

see theorem 2·27 of [**6**]. The point $\mathbf{a}$ is called an absolute point of the correlation θ if $\mathbf{a} \in \mathbf{a}^\theta$. If θ is a correlation, θ^2 is a collineation of the plane. By (1), the image of $\mathbf{a}$ under θ^2 is

$$\mathbf{a}^{\theta^2} = \{\mathbf{x} : \mathbf{x}^T A \mathbf{a}^\phi = 0\}^\theta = A^{-T} A^\phi \mathbf{a}^{\phi^2}. \tag{2}$$

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

It is known (see [**6**], p. 57) that a non-degenerate Hermitian matrix H over GF(q^2) defines a polarity of PG$(2, q^2)$, with $\phi = (q)$. These polarities are called unitary. Their absolute points are the $q^3 + 1$ points $\mathbf{x}$ that satisfy the equation $\mathbf{x}^T H \mathbf{x}^{(q)} = 0$ (see [**6**], II.8). These points (together with the non-absolute lines, but this will not interest us here) form a so-called unital. We shall denote the point-set of the unital $\{\mathbf{x} : \mathbf{x}^T H \mathbf{x}^{(q)} = 0\}$ by $\{H\}$.

The complete $(q^2 - q + 1)$-arcs we mentioned above were obtained as intersections of unitals of a special family. In [**3**], however, the same arcs are arrived at by different means. Later we became aware that the arcs in question are the sets of absolute points of certain correlations. This viewpoint proved fruitful in that it enabled us to prove their completeness (in [**8**]). In [**1**, **4**], different methods are employed to demonstrate this fact.

In the present paper we use these correlations to arrive at more general partitions of projective planes into arcs.

Consider the projective plane PG$(2, q^{2^m})$, where $m \geqslant 1$, containing $q^{2^{m+1}} + q^{2^m} + 1$ points. It is easy to prove the following factorization:

$$\begin{aligned} q^{2^{m+1}} + q^{2^m} + 1 = (q^2 + q + 1)(q^2 - q + 1)(q^4 - q^2 + 1) \\ \times (q^8 - q^4 + 1) \dots (q^{2^{m-1}} - q^{2^{m-2}} + 1)(q^{2^m} - q^{2^{m-1}} + 1). \end{aligned} \tag{3}$$

We will avoid awkward notation by writing Q_r instead of q^{2^r} for all $r \geqslant 0$. Then we have $Q_r^2 = Q_{r+1}$, and (3) becomes

$$\begin{aligned} Q_{m+1} + Q_m + 1 = (Q_1 + Q_0 + 1)(Q_1 - Q_0 + 1)(Q_2 - Q_1 + 1) \\ \times (Q_3 - Q_2 + 1) \dots (Q_{m-1} - Q_{m-2} + 1)(Q_m - Q_{m-1} + 1). \end{aligned} \tag{4}$$

https://doi.org/10.1017/S0305004100065634 Published online by Cambridge University Press

In this article we present the following result:

THEOREM. PG $(2, Q_m)$, *where* $m \geqslant 1$, *can be partitioned into equicardinal arcs in* m *different ways: for each* $l \in \{1, 2, \ldots, m\}$ *the point-set of* PG $(2, Q_m)$ *is a disjoint union of* $(Q_l - Q_{l-1} + 1)$*-arcs.*

Proof. Denote PG $(2, Q_l)$ by Π_l for each l.

For each $l \in \{1, 2, \ldots, m\}$, Π_m contains a subplane $\Pi_l = \text{PG}(2, Q_l)$, whose points are of the form

$$\mathbf{a} = \begin{pmatrix} a_1 \\ a_2 \\ a_3 \end{pmatrix}$$

with $a_1, a_2, a_3 \in \text{GF}(Q_l)$. We fix l and concentrate for the time being on Π_l, ignoring the Π_m in which it is embedded.

We will be making frequent use of results in [7] and [8]. However in those papers we were dealing with planes over GF (q^2) rather than GF (Q_l). Thus, whenever we refer to them in the present context, q and q^2 will have to be replaced by Q_{l-1}, Q_l, respectively.

Let H' be a symmetric 3×3 matrix over GF (Q_{l-1}). Then, as explained earlier, H' is Hermitian over GF (Q_l). Let the characteristic polynomial of H' be $p_3'(x)$ and assume that it is irreducible over GF (Q_{l-1}). The existence of such matrices is a consequence of theorem 34·5 on p. 59 of [9].

Since $p_3'(H') = \mathbf{0}$, the polynomials $p(H')$ over GF (Q_{l-1}) form a field GF (Q_{l-1}^3). Now let H be a primitive root of the latter, satisfying its characteristic equation $p_3(H) = \mathbf{0}$, which is primitive and irreducible over GF (Q_{l-1}).

The matrices H^j with $j = 1, 2, \ldots, Q_{l-1}^3 - 1$ are the non-zero elements of GF (Q_{l-1}^3). Its GF (Q_{l-1}) subfield comprises the scalar matrices eI_3 with e ranging through GF (Q_{l-1}).

It was shown in [7] on p. 1300 that the polynomial $|H^r - \lambda H^s|$ has no roots in GF (Q_{l-1}) for any distinct numbers $r, s \in \{0, 1, \ldots, Q_l + Q_{l-1}\}$. Furthermore the theorem on p. 1302 in [7] (with $n = 1$) states that the point-set $\{H^r\} \cap \{H^s\}$ is a $(Q_l - Q_{l-1} + 1)$-arc and Π_l is a disjoint union of (a number of $Q_l + Q_{l-1} + 1$) such arcs.

Now let H^r, H^s be Hermitian matrices as in the preceding paragraph, and let t be any element of GF $(Q_l) \backslash$ GF (Q_{l-1}). Consider the matrix $K = tH^r + H^s$, which is symmetric (because H is), but not a scalar multiple of a Hermitian matrix over GF (Q_l) (see [8], p. 3).

We use K to define a correlation θ of Π_l (see (1)) with companion automorphism $\phi = (Q_{l-1})$:

$$\mathbf{a}^\theta = \{\mathbf{x} : \mathbf{x}^T K \mathbf{a}^{(Q_{l-1})} = 0\}, \quad \{\mathbf{x} : \mathbf{x}^T \mathbf{b} = 0\}^\theta = K^{-1} \mathbf{b}^{(Q_{l-1})}. \tag{5}$$

As K is not a scalar multiple of a Hermitian matrix, θ is not a polarity (this was explained in [8] on p. 3). By (2), we have for any point $\mathbf{a} \in \Pi_l$

$$\mathbf{a}^{\theta^2} = K^{-1} K^{(Q_{l-1})} \mathbf{a}^{(Q_{l-1}^2)} = K^{-1} K^{(Q_{l-1})} \mathbf{a}^{(Q_l)} = K^{-1} K^{(Q_{l-1})} \mathbf{a}. \tag{6}$$

We will show now that the set of absolute points of θ is precisely the $(Q_l - Q_{l-1} + 1)$-arc $\{H^r\} \cap \{H^s\}$.

https://doi.org/10.1017/S0305004100065634 Published online by Cambridge University Press

The absolute points of θ are those points $\mathbf{x} \in \Pi_l$ that lie on $\mathbf{x}^\theta$, i.e., by (5), they satisfy the equation $\mathbf{x}^T K \mathbf{x}^{(Q_{l-1})} = 0$. But $K = tH^r + H^s$, so this equation becomes

$$t\mathbf{x}^T H^r \mathbf{x}^{(Q_{l-1})} + \mathbf{x}^T H^s \mathbf{x}^{(Q_{l-1})} = 0. \tag{7}$$

We claim that the scalars $\mathbf{x}^T H^r \mathbf{x}^{(Q_{l-1})}$ and $\mathbf{x}^T H^s \mathbf{x}^{(Q_{l-1})}$ are in $\mathrm{GF}(Q_{l-1})$. We have

$$[\mathbf{x}^T H^r \mathbf{x}^{(Q_{l-1})}]^{Q_{l-1}} = \mathbf{x}^{(Q_{l-1})T} H^{r(Q_{l-1})} \mathbf{x}^{(Q_l)} = \mathbf{x}^{(Q_{l-1})T} H^r \mathbf{x}$$
$$= [\mathbf{x}^{(Q_{l-1})T} H^r \mathbf{x}]^T = \mathbf{x}^T H^{rT} \mathbf{x}^{(Q_{l-1})} = \mathbf{x}^T H^r \mathbf{x}^{(Q_{l-1})},$$

which proves that $\mathbf{x}^T H^r \mathbf{x}^{(Q_{l-1})} \in \mathrm{GF}(Q_{l-1})$. A similar proof holds for the other element.

Now, since $t \notin \mathrm{GF}(Q_{l-1})$ by assumption, (7) implies

$$\mathbf{x}^T H^r \mathbf{x}^{(Q_{l-1})} = \mathbf{x}^T H^s \mathbf{x}^{(Q_{l-1})} = 0,$$

for if not, then $t \in \mathrm{GF}(Q_{l-1})$.

This argument demonstrates that the arc $\{H^r\} \cap \{H^s\}$ is the set of absolute points of θ, as desired.

By lemma 1 in [8], the cyclic group of collineations $\langle \theta^2 \rangle$ permutes all the points of Π_l in orbits of equal length, a divisor of $Q_l - Q_{l-1} + 1$. Moreover the orbit of each point is a subset of the (unique) arc containing it.

Further, we have shown in [8] that as a consequence of lemma 2, the element t that is used in defining K can be chosen in such a way that the orbits of all the points in Π_l have length $Q_l - Q_{l-1} + 1$. So we assume from now on that all the orbits of $\langle \theta^2 \rangle$ are $(Q_l - Q_{l-1} + 1)$-arcs of Π_l.

We now switch our attention to the 'big' plane Π_m.

Lemma 3 in [7] asserts that 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 $\mathrm{GF}(q^2)$. Therefore p_3, the characteristic polynomial of our matrix H, being irreducible over $\mathrm{GF}(Q_{l-1})$, is irreducible over $\mathrm{GF}(Q_l), \ldots, \mathrm{GF}(Q_m)$ as well. Thus the polynomials $p(H)$ with coefficients in $\mathrm{GF}(Q_l)$, $\mathrm{GF}(Q_m)$, form a $\mathrm{GF}(Q_l^3)$ and a $\mathrm{GF}(Q_m^3)$, respectively. We refer to the latter fields as Φ_l and Φ_m.

The elements of Φ_m are the matrices $\alpha H^2 + \beta H + \gamma I_3$ with $\alpha, \beta, \gamma \in \mathrm{GF}(Q_m)$. Taking $\alpha, \beta, \gamma \in \mathrm{GF}(Q_l)$ we obtain its subfield Φ_l.

Let M stand for a primitive root of Φ_m. Then the matrix $L = M^{(Q_m^3-1)/(Q_l^3-1)}$ is a primitive root of Φ_l.

Consider the matrix-induced collineation Ω of Π_m that maps each point $\mathbf{a}$ onto $K^{-1}K^{(Q_{l-1})}\mathbf{a}$. We will prove that all the orbits under the cyclic group $\langle \Omega \rangle$ are $(Q_l - Q_{l-1} + 1)$-arcs.

The restriction of Ω to Π_l is θ^2 (see (6)). On p. 6 of [8] it is shown that $K^{-T}K^{(q)} = N^{v(q^3-1)^T}$ (the matrices there are not necessarily symmetric), where N is a primitive root of $\mathrm{GF}(q^6)$. By adapting this to our situation here, we get

$$K^{-1}K^{(Q_{l-1})} = L^{v(Q_{l-1}^3-1)} \tag{8}$$

where v is an integer. Hence, for any positive integer g,

$$\mathbf{a}^{\Omega^g} = [K^{-1}K^{(Q_{l-1})}]^g \mathbf{a} = L^{gv(Q_{l-1}^3-1)}\mathbf{a}.$$

https://doi.org/10.1017/S0305004100065634 Published online by Cambridge University Press

We denote $gv(Q_{l-1}^3-1)$ by w. The orbit length of $\mathbf{a}$ is the smallest g for which $\mathbf{a}^{\Omega^g} = \nu\mathbf{a}$, in other words

$$L^w\mathbf{a} = \nu\mathbf{a},$$

for some $\nu \in \mathrm{GF}(Q_m)$. Thus $\mathbf{a}$ must be an eigenvector of L^w.

The entries of L are from $\mathrm{GF}(Q_l)$, whereas those of $\mathbf{a}$ are from $\mathrm{GF}(Q_m)$. It follows that $\nu \in \mathrm{GF}(Q_m)$. However $\nu = \xi^w$, where ξ is an eigenvalue of L. As ξ satisfies the same irreducible equation over $\mathrm{GF}(Q_l)$ that L does, it generates the same field Φ_l. Thus $\nu = \xi^w \in \Phi_l$. On the other hand, the ν that we want must be in $\mathrm{GF}(Q_m)$. So $\nu \in \Phi_l \cap \mathrm{GF}(Q_m)$. Since $(3\cdot 2^l, 2^m) = 2^l$, we have $\Phi_l \cap \mathrm{GF}(Q_m) = \mathrm{GF}(Q_l)$, so that $\nu \in \mathrm{GF}(Q_l)$. Hence $L^w \in \mathrm{GF}(Q_l)$ as well. However the $\mathrm{GF}(Q_l)$ subfield of Φ_l consists of the scalar matrices γI_3, where γ ranges through $\mathrm{GF}(Q_l)$.

In conclusion, for $\mathbf{a}$ to be an eigenvector of L^w, we must have $L^w = \gamma I_3$; but then all the points of Π_m are eigenvectors of L^w. Hence the smallest g is the same for all the points, i.e. all the orbits have the same length. As it has been established already that the orbits of $\langle\theta^2\rangle$ in Π_l have length $Q_l - Q_{l-1} + 1$, we see that this is the length of all the orbits of $\langle\Omega\rangle$ in Π_m.

It remains to be shown that they are arcs.

Let $\mathbf{a}, \mathbf{b}, \mathbf{c} \in \Pi_m \backslash \Pi_l$ belong to the same orbit under $\langle\Omega\rangle$. We will exhibit a collineation that maps them onto three points of Π_l belonging to the same arc. This will prove the non-collinearity of $\mathbf{a}, \mathbf{b}, \mathbf{c}$.

Our Φ_m has a subfield $\mathrm{GF}(Q_m)$ comprised of matrices γI_3 with $\gamma \in \mathrm{GF}(Q_m)$. Since M is a primitive root of Φ_m, these scalar matrices must be of form $M^{\sigma(Q_m^3-1)/(Q_m-1)} = M^{\sigma(Q_{m+1}+Q_m+1)}$ for some integer σ. Hence the smallest power of M that is a scalar matrix is the $(Q_{m+1}+Q_m+1)$st. But this is the number of points of Π_m. On the other hand, no power of M that is not a scalar matrix can have eigenvalues in Q_m. Hence, if Γ is the collineation induced by M on Π_m, the cyclic group $\langle\Gamma\rangle$ acts regularly on its points.

We have also seen that $K^{-1}K^{(Q_{l-1})}$ is a power of L (see (8)), where L in turn is a power of M. Therefore there exists an integer u so that

$$K^{-1}K^{(Q_{l-1})} = M^u.$$

Because $\mathbf{a}, \mathbf{b}, \mathbf{c}$ are in one orbit, we have $\mathbf{b} = M^{ui}\mathbf{a}$, $\mathbf{c} = M^{uj}\mathbf{a}$, for some i, j.

Now let $\mathbf{d}$ be any point of Π_l. There exists an integer z such that $\mathbf{d} = M^z\mathbf{a}$, because of the transitivity of $\langle\Gamma\rangle$. Then let $\mathbf{e} = M^z\mathbf{b}$ and $\mathbf{f} = M^z\mathbf{c}$. We have

$$\mathbf{e} = M^zM^{ui}\mathbf{a} = M^{ui}\mathbf{d} \quad \text{and} \quad \mathbf{f} = M^zM^{uj}\mathbf{a} = M^{uj}\mathbf{d},$$

which shows that $\mathbf{d}, \mathbf{e}, \mathbf{f}$ are in the same arc in Π_l. Therefore $\mathbf{a}, \mathbf{b}, \mathbf{c}$ are not collinear either, and this concludes the proof.

REFERENCES

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

[2] R. C. Bose and I. M. Chakravarti. Hermitian varieties in a finite projective space $\mathrm{PG}(N, q^2)$. *Canad. J. Math.* **17** (1966), 1161–1182.

[3] G. R. Ebert. Partitioning projective geometries into CA's. *Canad. J. Math.* **37** (1985), 1163–1175.

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

[5] J. W. P. Hirschfeld. *Projective Geometries over Finite Fields* (Clarendon Press, 1979).

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

https://doi.org/10.1017/S0305004100065634 Published online by Cambridge University Press

[7] B. C. KESTENBAND. Projective geometries that are disjoint unions of caps. *Canad. J. Math.* **32** (1980), 1299–1305.
[8] B. C. KESTENBAND. A family of complete arcs in finite projective planes. *Colloq. Math.* (to appear).
[9] J. MACDUFFEE. *The Theory of Matrices* (Chelsea, 1946).
[10] J. A. THAS. Complete arcs and algebraic curves in PG$(2, q)$. *J. Algebra* **106** (1987), 451–464.

https://doi.org/10.1017/S0305004100065634 Published online by Cambridge University Press