Can. J. Math., Vol. XXXVII, No. 6, 1985, pp. 1163-1175

PARTITIONING PROJECTIVE GEOMETRIES INTO CAPS

GARY L. EBERT

1. Introduction. In **[2]** by means of a fairly lengthy argument involving Hermitian varieties it was shown that $PG(2n, q^2)$ can be partitioned into $(q^{2n+1} + 1)/(q + 1)$-caps. Moreover, these caps were shown to constitute the "large points" of a $PG(2n, q)$ in a natural way. In **[3]** a similar argument was used to show that once two disjoint $(n - 1)$-subspaces are removed from $PG(2n - 1, q^2)$, the remaining points can be partitioned into $(q^{2n} - 1)/(q^2 - 1)$-caps.

The purpose of this paper is to give a short proof of the results found in **[2]**, and then use the technique developed to partition $PG(2n - 1, q)$ into $(q^n + 1)$-caps for n even and q any prime-power. Moreover, these caps can be treated in a natural way as the "large points" of a $PG(n - 1, q)$. Special attention will be paid to the case $n = 2$, where the theorem says that $PG(3, q)$ can be partitioned into ovoids so long as $q > 2$. Designs based on this ovoidal fibration will then be constructed.

2. Background. Let $\Sigma = PG(d, q)$ denote the desarguesian d-dimensional projective geometry over the finite field $GF(q)$. A *k-cap* in Σ is a collection of k points in Σ with no three collinear. We will represent Σ in the following way. Since the finite field $GF(q^{d+1})$ is a $(d + 1)$-dimensional vector space over $GF(q)$, the points of Σ can be thought of as the 1-dimensional subspaces of this vector space. If β is a primitive element of $GF(q^{d+1})$ and $N = (q^{d+1} - 1)/(q - 1)$, then β^N is a primitive element of the subfield $GF(q)$. Hence the points of Σ can be identified with the field elements $\beta^0, \beta^1, \beta^2, \dots, \beta^{N-1}$. If $0 \leqq i \neq j \leqq N - 1$, the line L joining β^i and β^j will consist of the points

$$\{\beta^j\} \cup \{\beta^i + a\beta^j : a \in GF(q)\},$$

where $\beta^i + a\beta^j$ is computed as some β^k in the field $GF(q^{d+1})$ and then the exponent k is read modulo N.

3. Partitioning $PG(2n, q^2)$. Theorem (1) below contains the results found in **[2]**, although the proof is quite different.

Received May 14, 1984. This work was supported in part by the National Research Council of Canada.

https://doi.org/10.4153/CJM-1985-063-1 Published online by Cambridge University Press

THEOREM 1. *Let n be any positive integer and q be any prime-power. Set*

$$N = (q^{2n+1} - 1)/(q - 1) \text{ and } M = (q^{2n+1} + 1)/(q + 1).$$

Then $\Sigma = PG(2n, q^2)$ can be partitioned into N disjoint M-caps. Moreover, these caps can be treated as the "large points" of a $PG(2n, q)$.

Proof. Let β be a primitive element of $GF(q^{2(2n+1)})$. Then

$$|\beta| = (q^2 - 1)NM$$

and we can identify the points of Σ with the field elements β^0, $\beta^1, \ldots, \beta^{NM-1}$. Let

$$\Omega_0 = \{\beta^0, \beta^N, \beta^{2N}, \ldots, \beta^{(M-1)N}\} \text{ and}$$

$$\Omega_i = \Omega_0\beta^i \quad \text{for } i = 1, 2, \ldots, N - 1.$$

Clearly Σ is the disjoint union $\Omega_0 \uplus \Omega_1 \uplus \ldots \uplus \Omega_{N-1}$. As Ω_i is a multiplicative coset of Ω_0, each Ω_i will necessarily be an M-cap if we can show Ω_0 is an M-cap.

By way of contradiction suppose that three points of Ω_0 are collinear. Without loss of generality we can write

$$1 + a\beta^{iN} = b\beta^{jN},$$

where a and b are nonzero elements of $GF(q^2)$ and $1 \leqq i \neq j \leqq M - 1$. Then

$$\begin{aligned}
&(1 + a\beta^{iN})(1 + a\beta^{iN})^{q^{2n+1}} = b^{q+1}\beta^{jN(q^{2n+1}+1)} \\
&= b^{q+1}\beta^{jNM(q+1)} \in GF(q) \\
&\Rightarrow (1 + a\beta^{iN})(1 + a^q\beta^{iNq^{2n+1}}) \in GF(q) \\
&\Rightarrow a\beta^{iN} + a^q\beta^{iNq^{2n+1}} \in GF(q).
\end{aligned}$$

Since

$$a\beta^{iN} \cdot a^q\beta^{iNq^{2n+1}} = a^{q+1}\beta^{iNM(q+1)} \in GF(q),$$

$$f(x) = (x - a\beta^{iN})(x - a^q\beta^{iNq^{2n+1}})$$

is a quadratic polynomial over $GF(q)$ having $a\beta^{iN}$ as a root. Thus $a\beta^{iN} \in GF(q^2)$ and hence $\beta^{iN} \in GF(q^2)$, a contradiction. We therefore, have partitioned Σ into M-caps.

Since $\beta^{M(q+1)}$ and $\beta^{NM(q+1)}$ are primitive elements of the subfields $GF(q^{2n+1})$ and $GF(q)$, respectively, we can identify the points of $PG(2n, q)$ with

$$\langle\beta^{M(q+1)}\rangle/\langle\beta^{NM(q+1)}\rangle$$

as described in Section 2. Now $\Omega_0 = \langle\beta^N\rangle/\langle\beta^{NM}\rangle$ is a multiplicative

https://doi.org/10.4153/CJM-1985-063-1 Published online by Cambridge University Press

subgroup of order M in the cyclic group $\langle\beta\rangle/\langle\beta^{NM}\rangle$, and each Ω_i is a multiplicative coset of Ω_0. Hence the caps can be treated as the elements of

$$\frac{\langle\beta\rangle/\langle\beta^{NM}\rangle}{\langle\beta^{N}\rangle/\langle\beta^{NM}\rangle} \cong \langle\beta^{M(q+1)}\rangle/\langle\beta^{NM(q+1)}\rangle.$$

That is, the caps constitute the "large points" of a $PG(n,q)$, proving the theorem.

We now go a step further and determine how the lines of Σ meet the M-caps in the above partition.

THEOREM 2. *Using the notation from the proof of Theorem* 1, *let* L_s *denote the secant line to* Ω_0 *joining* β^0 *and* β^{sN} *for some* $1 \leqq s \leqq M - 1$. *Then* L_s *is tangent to exactly* $q + 1$ *of the above* M*-caps and hence secant to* $q(q - 1)/2$ *of them. The points of tangency correspond to the field elements*

$$\{\beta^{sN} + \beta^{jNM} : j \equiv s \ (\mathrm{mod}\ q - 1) \text{ and } 1 \leqq j \leqq q^2 - 1\}.$$

Proof. Let P denote any point of L_s other than β^0 or β^{sN}. Then P is identified with $\beta^{sN} + a$ for some $0 \neq a \in GF(q^2)$. Clearly $P \in \Omega_i$ for some $1 \leqq i \leqq N - 1$. To determine if L_s meets Ω_i in another point (at most one such point, of course), we find all $0 \neq b \in GF(q^2)$ with $(\beta^{sN} + a)/(\beta^{sN} + b)$ corresponding to a point of Ω_0. That is, we find all $0 \neq b \in GF(q^2)$ with

$$((\beta^{sN} + a)/(\beta^{sN} + b))^{q^t+1} \in GF(q),$$

where $t = 2n + 1$. The last statement is equivalent to

$$\frac{d + a\beta^{sNq^t} + a^q\beta^{sN} + a^{q+1}}{d + b\beta^{sNq^t} + b^q\beta^{sN} + b^{q+1}} \in GF(q),$$

where $d = \beta^{sN(q^t+1)} \in GF(q)$. Rewriting again we have

$$a\beta^{sNq^t} + a^q\beta^{sN} = e(b\beta^{sNq^t} + b^q\beta^{sN}) + f,$$

where $e \neq 0, f \in GF(q)$, and hence

$$(a - eb)\beta^{sNq^t} + (a^q - eb^q)\beta^{sN} \in GF(q).$$

A polynomial argument similar to that given above now shows that necessarily

$$(a - eb)^q\beta^{sN} \in GF(q^2),$$

and hence $b = a/e$ as $\beta^{sN} \notin GF(q^2)$. Letting

$$\gamma = a\beta^{sNq^t} + a^q\beta^{sN},$$

another polynomial argument shows that $\gamma \notin GF(q)$.

Thus we are faced with the problem of finding all $0 \neq c \in GF(q)$ such that

https://doi.org/10.4153/CJM-1985-063-1 Published online by Cambridge University Press

$$\frac{d + \gamma + a^{q+1}}{d + c\gamma + c^2a^{q+1}} \in GF(q),$$

and then setting $b = ca$ for all such c. Equivalent formulations of this problem are:

$$\frac{d + \gamma + a^{q+1}}{d/c + \gamma + ca^{q+1}} \in GF(q)$$

or

$$\frac{d + \gamma + a^{q+1}}{d/c + \gamma + ca^{q+1}} = 1 \quad (\text{as } \gamma \notin GF(q))$$

or

$$(*) \quad a^{q+1}c^2 - (d + a^{q+1})c + d = 0.$$

Clearly $c = 1$ (hence $b = a$) satisfies the quadratic equation (*). In fact, for either q even or q odd, it is easily seen that $c = 1$ and $c = d/a^{q+1}$ are the two (not necessarily distinct) roots of (*).

Thus we conclude that the line L_s is tangent to Ω_i at $P \sim \beta^{sN} + a$ precisely when

$$a^{q+1} = d = \beta^{sN(q^t+1)}.$$

Since β^{NM} is a primitive element of $GF(q^2)$, we can write $a = \beta^{jNM}$ for some $1 \leqq j \leqq q^2 - 1$. Then

$$\begin{aligned} &a^{q+1} = \beta^{sN(q^t+1)} \\ &\Leftrightarrow \beta^{jNM(q+1)} = \beta^{sNM(q+1)} \\ &\Leftrightarrow jNM(q + 1) \equiv sNM(q + 1) \pmod{NM(q^2 - 1)} \\ &\Leftrightarrow j \equiv s \pmod{q - 1}. \end{aligned}$$

Thus there are $q + 1$ choices for j (or a), and hence L_s is tangent to $q + 1$ of the above M-caps. Since L_s has $q^2 + 1$ points and the M-caps partition Σ, L_s must be secant to $q(q - 1)/2$ M-caps.

COROLLARY. *There are $NM(q^{2n} - 1)/(q^2 - 1)$ lines of Σ that are tangent to $q + 1$ M-caps in our partition and hence secant to $q(q - 1)/2$ of them. The remaining $NM(q^{2n} - 1)(q^{2n} - q^2)/(q^4 - 1)$ lines of Σ are necessarily tangent to $q^2 + 1$ of the M-caps. In particular, when $n = 1$, every line of $PG(2, q^2)$ is tangent to precisely $q + 1$ of the M-caps.*

Proof. Say that a line of Σ is of type A if it is tangent to precisely $q + 1$ of the M-caps in our partition. Using Theorem 2 and the collineations of Σ corresponding to multiplication by β^{tN} for appropriate t, we see that every secant to Ω_0 is of type A. Using the collineations of Σ corresponding to

https://doi.org/10.4153/CJM-1985-063-1 Published online by Cambridge University Press

multiplication by $\beta^{\pm i}$, we then see that every secant to Ω_i is also of type A. There are $N \cdot \binom{M}{2}$ such secants, each line being counted above $q(q - 1)/2$ times. This accounts for $NM(q^{2n} - 1)/(q^2 - 1)$ distinct lines of Σ, all of type A. Subtracting from $NM(q^{2n-1})(q^{2n} + 1)/(q^4 - 1)$, the total number of lines in Σ, we obtain $NM(q^{2n} - 1)(q^{2n} - q^2)/(q^4 - 1)$ lines necessarily secant to none of the M-caps in our partition and hence tangent to $q^2 + 1$ of them. When $n = 1$, there are no such lines.

4. Partitioning $PG(d, q)$ **for** $d \equiv 3 \pmod 4$. In this section we consider projective geometries of (odd) dimensions congruent to 3 modulo 4 with no restriction on the ground field. Specifically, we have the following partition theorem.

THEOREM 3. *Let $n \geqq 2$ be an even integer and q be any prime-power. Set $N = (q^n - 1)/(q - 1)$ and $M = q^n + 1$. Then $\Sigma = PG(2n - 1, q)$ can be partitioned into N disjoint M-caps. Moreover, these caps constitute the "large points" of a $PG(n - 1, q)$.*

Proof. Analogously to the proof of Theorem 1, let β denote a primitive element of $GF(q^{2n})$. Then $|\beta| = NM(q - 1)$ and β^{NM} is a primitive element of the subfield $GF(q)$. Identify the points of Σ with the elements $\beta^0, \beta^1, \ldots, \beta^{NM-1}$. Let

$$\Omega_0 = \{\beta^{sN}: s = 0, 1, 2, \ldots, M - 1\} \quad \text{and}$$

$$\Omega_i = \Omega_0\beta^i \quad \text{for } i = 1, 2, \ldots, N - 1.$$

Then $\Sigma = \Omega_0 \uplus \Omega_1 \uplus \ldots \uplus \Omega_{N-1}$ and it suffices to show that no three points of Ω_0 are collinear.

By way of contradiction we can assume without loss of generality that

$$1 + a\beta^{iN} = b\beta^{jN},$$

where a and b are nonzero elements of $GF(q)$ and $1 \leqq i \neq j \leqq M - 1$. Then

$$(1 + a\beta^{iN})(1 + a\beta^{iN})^{q^n} = b\beta^{jN(q^n+1)} = b\beta^{jNM} \in GF(q)$$

$$\Rightarrow \beta^{iN} + \beta^{iNq^n} \in GF(q)$$

as before.

A polynomial argument once again shows that $\beta^{iN} \in GF(q^2)$ and hence

$$\beta^{iN(q^2-1)} = 1.$$

Thus $|\beta| \,\big|\, iN(q^2 - 1)$, implying that

$$M \,\big|\, i(q + 1).$$

https://doi.org/10.4153/CJM-1985-063-1 Published online by Cambridge University Press

Since $M = q^n + 1$ with n even, the least common multiple

$$[M, q + 1] = \begin{cases} M(q + 1) \text{ if } q \text{ is even} \\ M(q + 1)/2 \text{ if } q \text{ is odd.} \end{cases}$$

As $1 \leqq i \leqq M - 1$, we conclude that $i = M/2$ (and q is odd). But now reversing the roles of i and j, we obtain the contradiction that $i = j$. Hence Σ is partitioned into M-caps.

As in the proof of Theorem 1, the cosets $\Omega_0, \Omega_1, \ldots, \Omega_{N-1}$ can be identified with the elements of

$$\frac{\langle\beta\rangle/\langle\beta^{NM}\rangle}{\langle\beta^N\rangle/\langle\beta^{NM}\rangle} \cong \langle\beta^M\rangle/\langle\beta^{NM}\rangle.$$

Since β^{NM} and β^M are primitive elements of $GF(q)$ and $FG(q^n)$, respectively, the points of $PG(n - 1, q)$ can also be identified with $\langle\beta^M\rangle/\langle\beta^{NM}\rangle$, completing the proof.

LEMMA 1. *Using the notation from the proof of Theorem* 3, *assume that q is odd and let $s = M/2$. Let L be the secant line to Ω_0 joining β^0 and β^{sN}. Then L is tangent to no M-cap in our partition and hence is secant to $(q + 1)/2$ of them. In fact, L is secant to Ω_i precisely for*

$$i = 0, 2N/(q + 1), 4N/(q + 1), \ldots, (q - 1)N/(q + 1).$$

Proof. Since $\beta^{sN} = \beta^{NM/2} \in GF(q^2)$ and $\beta^{NM/(q+1)}$ is a primitive element of $GF(q^2)$, it is easy to see that the $q + 1$ points of L correspond to the field elements $\beta^0, \beta^{NM/(q+1)}, \beta^{2NM/(q+1)}, \ldots, \beta^{qNM/(q+1)}$. Since $M = q^n + 1$ with n even,

$$NM/(q + 1) \equiv 2N/(q + 1) \pmod{N}$$

and the result now follows.

THEOREM 4. *Again using the notation of Theorem* 3, *let L_s be the secant line to Ω_0 joining β^0 and β^{sN} for any $1 \leqq s \leqq M - 1$ with $s \neq M/2$.*

a) *For odd prime-powers q we have two possibilities for L_s:*

i) *If s is odd, L_s is tangent to no M-cap in our partition and hence secant to $(q + 1)/2$ of them.*

ii) *If s is even, L_s is tangent to precisely* 2 *M-caps in our partition and hence secant to $(q - 1)/2$ of them. The points of tangency correspond to $\beta^{sN} \pm \beta^{sNM/2}$.*

b) *For even prime-powers q, L_s is necessarily tangent to* 1 *M-cap of our partition and hence secant to $q/2$ of them. The point of tangency corresponds to $\beta^{sN} + \sqrt{\beta^{sNM}}$.*

Proof. As in the proof of Theorem 2, any point P of L_s other than β^0 or β^{sN} is identified with the field element $\beta^{sN} + a$, for some $0 \neq a \in GF(q)$. Clearly $P \in \Omega_i$ for some $1 \leqq i \leqq N - 1$, and L_s meets Ω_i in at most one

https://doi.org/10.4153/CJM-1985-063-1 Published online by Cambridge University Press

other point. Determining how L_s meets Ω_i is equivalent to finding all $0 \neq b \in GF(q)$ such that

$$((\beta^{sN} + a)/(\beta^{sN} + b))^{q^n+1} \in GF(q).$$

An equivalent formulation of the last statement is

$$\frac{d + a\gamma + a^2}{d + b\gamma + b^2} \in GF(q),$$

where

$$d = \beta^{sN(q^n+1)} = \beta^{sNM} \in GF(q) \quad \text{and} \quad \gamma = \beta^{sN} + \beta^{sNq^n}.$$

The usual polynomial argument shows that $\gamma \notin GF(q)$ since $s \neq M/2$ implies that $\beta^{sN} \notin GF(q^2)$. Rewriting as before, we have

$$\frac{bd/a + b\gamma + ba}{d + b\gamma + b^2} = 1$$

(as $\gamma \notin GF(q)$) or

$$(*) \quad b^2 - (d/a + a)b + d = 0.$$

For q even or odd the roots of (*) are $b = a$ and $b = d/a$. Hence L_s is tangent to Ω_i at $P \sim \beta^{sN} + a$ precisely when

$$a^2 = d = \beta^{sNM}.$$

Since β^{NM} is a primitive element of $GF(q)$ and $0 \neq a \in GF(q)$, we see that when q is odd there are 0 or 2 choices for such an a according as s is odd or even. When q is even, there is always a unique solution for such an a. The result now follows.

COROLLARY 1. *For odd prime-powers q the lines of Σ are partitioned as follows*:

i) $\frac{1}{2}NM^2/(q + 1)$ *lines tangent to no M-cap in our partition and hence secant to* $(q + 1)/2$ *of them*,

ii) $\frac{1}{2}NM(M - 2)/(q - 1)$ *lines tangent to* 2 *M-caps in our partition and hence secant to* $(q - 1)/2$ *of them*,

iii) $NM(q^{2n-1} - q^{n+1})/(q^2 - 1)$ *lines tangent to* $q + 1$ *M-caps in our partition and hence secant to none of them.*

In particular, when $n = 2$, *every line of* $PG(3, q)$ *is of type* (i) *or type* (ii).

Proof. Since n is even and q is odd, $M/2 = (q^n + 1)/2$ is odd. Using Lemma 1, Theorem 4, and the usual collineation argument, secant lines to Ω_0 must be either of type (i) or type (ii). Moreover, the secants to Ω_0 of

https://doi.org/10.4153/CJM-1985-063-1 Published online by Cambridge University Press

type (i) are the lines joining β^{iN} and β^{jN} where $0 \leqq i < j \leqq M - 1$ and $j - i$ is odd. The number of such lines is

$$2(1 + 2 + 3 + \ldots + (M - 2)/2) + M/2 = M^2/4.$$

Hence the number of secants to Ω_0 of type (ii) is

$$\binom{M}{2} - M^2/4 = M(M - 2)/4.$$

Another collineation argument shows the same results hold for each Ω_k, $0 \leqq k \leqq N - 1$. As each line of type (i) is counted above $(q + 1)/2$ times and each line of type (ii) is counted $(q - 1)/2$ times, the number of distinct lines of type (i) and (ii) is

$$\frac{1}{2}NM^2/(q + 1) \quad \text{and} \quad \frac{1}{2}NM(M - 2)/(q - 1),$$

respectively. Subtracting these numbers from $NM(q^{2n-1} - 1)/(q^2 - 1)$, the total number of lines in Σ, we see there are $NM(q^{2n-1} - q^{n+1})/(q^2 - 1)$ lines unaccounted for, all of which are necessarily secant to none of the M-caps in our partition.

COROLLARY 2. *For even prime-powers q the lines of Σ are partitioned as follows*:

i)′ NMq^{n-1} *lines tangent to* 1 *of the M-caps in our partition and hence secant to $q/2$ of them,*

ii)′ $NM(q^{2n-1} - q^{n+1} + q^{n-1} - 1)/(q^2 - 1)$ *lines tangent to $q + 1$ M-caps in our partition and hence secant to none of them.*

Proof. This follows from Theorem 4 as above.

5. Designs obtained by partitioning $PG(3, q)$. We apply the results of the previous section to the special case when $n = 2$ and $q > 2$. In particular, we have $\Sigma = PG(3, q)$ partitioned into $q + 1$ disjoint $(q^2 + 1)$-caps. With $q > 2$ these caps are necessarily ovoids (see [**1**] and [**4**]). If q is odd, the lines of Σ are partitioned into $(q^2 + 1)^2/2$ type (i) lines (tangent to none of the ovoids) and $(q^2 + 1)(q + 1)^2/2$ type (ii) lines (tangent to 2 of the ovoids). If q is even, the lines of Σ are partitioned as $q(q + 1)(q^2 + 1)$ of type (i)′ (tangent to 1 of the ovoids) and $q^2 + 1$ of type (ii)′ (tangent to all of the ovoids).

Moreover, every plane of Σ must meet each of the $q + 1$ ovoids in a point or an oval (circle of the corresponding inversive plane). A simple counting argument then shows that each plane of Σ is tangent to 1 of the ovoids in our partition and meets the other q ovoids in disjoint ovals. Thus a by-product of Section 4 is a method for partitioning a desarguesian plane of order $q > 2$ into q disjoint ovals and one special point.

https://doi.org/10.4153/CJM-1985-063-1 Published online by Cambridge University Press

We now look at the problem of determining which pairs of ovoids can serve as the ovoids tangent to a line of type (ii) when q is odd.

LEMMA 2. *Let q be an odd prime-power. If β is a primitive element of $GF(q^4)$ and t is an integer with $1 \leqq t \leqq (q^2 - 1)/2$, then*

$$1 - \beta^{2t(q+1)(q^2-1)}$$

is a non-square in $GF(q^4)$.

Proof. As $|\beta| = (q^2 - 1)(q^2 + 1)$ and $1 \leqq t \leqq (q^2 - 1)/2$, we know

$$\beta^{t(q+1)(q^2-1)} \neq \pm 1.$$

Let

$$\gamma = (1 + \beta^{t(q+1)(q^2-1)})/(1 - \beta^{t(q+1)(q^2-1)}).$$

Then γ is a nonzero element of $GF(q^4)$ and

$$\gamma^{q^2-1} = \left(\frac{1 + \beta^{-t(q+1)(q^2-1)}}{1 - \beta^{-t(q+1)(q^2-1)}}\right)\left(\frac{1 - \beta^{t(q+1)(q^2-1)}}{1 + \beta^{t(q+1)(q^2-1)}}\right) = -1.$$

Hence

$$\gamma^{(q^2-1)(q^2+1)/2} = (-1)^{(q^2+1)/2} = -1$$

and γ is a non-square in $GF(q^4)$. Thus

$$1 - \beta^{2t(q+1)(q^2-1)} = \gamma(1 - \beta^{t(q+1)(q^2-1)})^2$$

is also a non-square in $GF(q^4)$.

THEOREM 5. *Let q be an odd prime-power and $\{i, j\}$ be distinct integers with $0 \leqq i, j \leqq q$. Then $\Sigma = PG(3, q)$ has a line L (necessarily of type (ii)) tangent to Ω_i and Ω_j if and only if $i + j$ is odd.*

Proof. First suppose that L is a line tangent to both Ω_i and Ω_j, and hence necessarily secant to $(q - 1)/2$ of the ovoids in our partition. The usual collineation argument allows us to assume L is secant to Ω_0 and passes through β^0. By Theorem 4 we know L joins β^0 and $\beta^{2t(q+1)}$ for some $1 \leqq t \leqq (q^2 - 1)/2$. Moreover, the points where L is tangent to Ω_i and Ω_j correspond to

$$\beta^{2t(q+1)} + \beta^{t(q+1)(q^2+1)} = \beta^{u(q+1)}\beta^i$$

and

$$\beta^{2t(q+1)} - \beta^{t(q+1)(q^2+1)} = \beta^{v(q+1)}\beta^j$$

for some integers u, v. By Lemma 2 we see that

$$\beta^{(u+v)(q+1)}\beta^{i+j} = \beta^{4t(q+1)}(1 - \beta^{2t(q+1)(q^2-1)})$$

https://doi.org/10.4153/CJM-1985-063-1 Published online by Cambridge University Press

is a non square in $GF(q^4)$. As $(u + v)(q + 1)$ is even with q odd, this implies that $i + j$ must be odd.

Conversely, suppose that $i + j$ is odd. A collineation argument allows us to assume $i = 0$ and j is odd. Let π be the tangent plane to Ω_0 at β^0. Then π meets Ω_k in a conic C_k for $k = 1, 2, \dots, q$. Also each line of π through β^0 is tangent to exactly one of $C_1, C_2, \dots, C_q$. A simple counting argument then shows that β^0 is interior to $(q - 1)/2$ of the C_k's and exterior to $(q + 1)/2$ of them. Therefore there exist lines tangent to Ω_0 and Ω_k for $(q + 1)/2$ choices of k. By the argument in the above paragraph k must be odd. As $1 \leqq k \leqq q$, every odd integer k between 1 and q is used. In particular, there exists a line L tangent to Ω_0 and Ω_j.

Recall that an (r, λ)-*design* D is an incidence structure consisting of b blocks and v varieties such that a) every variety is incident with r blocks, and b) every pair of distinct varieties is incident with λ blocks. If all blocks are incident with the same number of varieties, say k, then D is called a *balanced incomplete block design* (BIBD).

THEOREM 6. *For every odd prime-power q there exists an (r, λ)-design with parameters*

$$b = q^2 + q + 2, v = q + 1, r = (q^2 + 1)/2,$$
$$\text{and } \lambda = (q - 1)^2/4.$$

The block sizes are $(q - 1)/2$ and $(q + 1)/2$.

Proof. For varieties take the $q + 1$ ovoids in our partition of $\Sigma = PG(3, q)$. For blocks take the orbits of the lines of Σ under the collineation θ corresponding to multiplication by β^{q+1}. If $[L]$ denotes the orbit of a line L under θ, clearly every line of $[L]$ is tangent and secant to the same ovoids as L.

Letting L_s again denote the secant line to Ω_0 joining β^0 and $\beta^{s(q+1)}$, the type (ii) secants to Ω_0 are partitioned into $(q^2 - 1)/4$ orbits of $q^2 + 1$ lines each (namely $[L_2], [L_4], [L_6], \dots, [L_{(q^2-1)/2}]$), while the type (i) secants to Ω_0 are partitioned into $(q^2 - 1)/4$ orbits of $q^2 + 1$ lines each ($[L_1], [L_3], [L_5], \dots, [L_{(q^2-3)/2}]$) and one orbit of $(q^2 + 1)/2$ lines ($[L_{(q^2+1)/2}]$). The secants to Ω_i, for $1 \leqq i \leqq q$, are similarly partitioned. Since each type (ii) orbit is counted above $(q - 1)/2$ times and each type (i) orbit is counted $(q + 1)/2$ times, we obtain $(q + 1)^2/2$ distinct type (ii) orbits and $(q^2 + 3)/2$ distinct type (i) orbits (2 of which are "short" orbits). Thus the total number of blocks is

$$b = (q + 1)^2/2 + (q^2 + 3)/2 = q^2 + q + 2.$$

We define incidence by saying a block $[L]$ and a variety Ω_i are incident if and only if L is secant to Ω_i. Thus the only block sizes are $(q - 1)/2$ and $(q + 1)/2$. The above paragraph shows that Ω_0 is incident with $(q^2 + 1)/2$

https://doi.org/10.4153/CJM-1985-063-1 Published online by Cambridge University Press

blocks, and the usual collineation argument implies the same is true for any Ω_i.

Next let Ω_i and Ω_j be distinct varieties. Suppose first that $i + j$ is odd. If P is any point of Ω_i and π_p is the tangent plane to Ω_i at P, the proof of Theorem 5 shows that P is an exterior point to the conic $C_j = \pi_p \cap \Omega_j$. Thus there are 2 lines in π_p through P tangent to C_j and $(q - 1)/2$ lines in π_p through P secant to C_j. These are necessarily the only lines of Σ through P tangent to Ω_i and meeting Ω_j. Allowing P to vary over Ω_i, we see there are precisely $2(q^2 + 1)$ lines tangent to both Ω_i and Ω_j, while there are precisely $(q^2 + 1)(q - 1)/2$ lines tangent to Ω_i and secant to Ω_j. By symmetry there also are exactly $(q - 1)(q^2 + 1)/2$ lines secant to Ω_i and tangent to Ω_j. If x denotes the number of distinct lines secant to both Ω_i and Ω_j, counting the (not necessarily distinct) lines PQ with $P \in \Omega_i$ and $Q \in \Omega_j$ gives us

$$4x + 2(q - 1)(q^2 + 1) + 2(q^2 + 1) = (q^2 + 1)^2 \quad \text{or}$$

$$x = (q^2 + 1)(q - 1)^2/4.$$

Remembering that one "short" orbit consists of lines secant to $\Omega_0, \Omega_2, \Omega_4, \dots, \Omega_{q-1}$ (by Lemma 1) and the other "short" orbit consists of lines secant to $\Omega_1, \Omega_3, \Omega_5, \dots, \Omega_q$, we conclude that the above x lines are partitioned into orbits under θ all of which have size $q^2 + 1$. That is, $\lambda = (q - 1)^2/4$ in this case.

Finally, suppose $i + j$ is even. Using the same notation as in the above paragraph, the proof of Theorem 5 now implies that P is interior to C_j for every $P \in \Omega_i$. A similar counting argument produces

$$x = (q^2 + 1)(q^2 - 2q - 1)/4.$$

Since i and j are either both even or both odd, there is one "short" orbit of $(q^2 + 1)/2$ lines counted in the above x lines. The remaining $(q^2 + 1)(q^2 - 2q - 3)/4$ lines are partitioned into $(q^2 - 2q - 3)/4$ orbits of size $q^2 + 1$. Thus

$$\lambda = 1 + (q^2 - 2q - 3)/4 = (q - 1)^2/4$$

in this case as well, proving the result.

THEOREM 7. *For every $q = 2^h$ with $h \geqq 2$ there exists a* BIBD *with parameters*

$$b = q(q + 1),\ v = q + 1,\ r = q^2/2,\ k = q/2,$$
$$\textit{and } \lambda = q(q - 2)/4.$$

Proof. The argument is completely analogous to that given above with the ovoids of our partition taken as varieties, the line orbits under θ of type (i)′ taken as blocks, and incidence again defined by secancy. It should

https://doi.org/10.4153/CJM-1985-063-1 Published online by Cambridge University Press

be noted that this time all orbits consist of $q^2 + 1$ lines. Also, since there are only $q^2 + 1$ lines of Σ tangent to more than 1 ovoid, $P \in \Omega_i$ is never the knot of the oval $\pi_p \cap \Omega_j$ and hence there is precisely 1 line of π_p through P tangent to Ω_j. The remaining details are left to the reader.

Example 1. Letting $q = 5$ in Theorem 6, we construct an (r, λ)-design with parameters $b = 32$, $v = 6$, $r = 13$, and $\lambda = 4$. The block sizes are 2 and 3. To simplify the notation we designate the ovoid Ω_i simply by i and the block $\{\Omega_i, \Omega_j, \Omega_k\}$ by ijk where $i < j < k$. With this notation the varieties are {0, 1, 2, 3, 4, 5} and the blocks are {013, 034, 035, 025, 014, 023, 024, 124, 145, 125, 134, 135, 235, 245, 01, 01, 02, 04, 05, 05, 12, 12, 13, 15, 23, 23, 24, 34, 34, 35, 45, 45}. There are 14 distinct blocks of size 3 (none repeated) and 12 distinct blocks of size 2 (6 of which have multiplicity 2).

Example 2. We let $q = 7$ in Theorem 6 and use the shorthand notation introduced above to construct an (r, λ)-design with $b = 58$, $v = 8$, $r = 25$, and $\lambda = 9$. The block sizes are 3 and 4. Specifically, we take as varieties {0, 1, 2, 3, 4, 5, 6, 7} and as blocks {0135, 0127, 0346, 0357, 0247, 0123, 0146, 0245, 0256, 0236, 0167, 0567, 0246, 1246, 1457, 1234, 1257, 1356, 1367, 1347, 1357, 2357, 2345, 2467, 3456, 4567, 013, 014, 015, 016, 023, 027, 034, 037, 045, 047, 056, 057, 124, 125, 126, 127, 134, 145, 156, 167, 235, 236, 237, 245, 256, 267, 346, 347, 356, 367, 457, 467}. There are no repeated blocks in this design, as will presumably be the case whenever $q \geqq 7$ and hence the minimum block size at least 3. It should also be noted that there are 13 "big" blocks and 12 "small" blocks incident with each variety, while there are either 5 "big" blocks and 4 "small" blocks or else 7 "big" blocks and 2 "small" blocks incident with each unordered pair of distinct varieties. The pairs for which $\lambda = 7 + 2$ are {02, 06, 13, 17, 24, 35, 46, 57}. However, we apparently do not get an association scheme here, at least not in any natural way.

Example 3. We let $q = 8$ in Theorem 7 to construct a (9, 4, 12)-BIBD. Specifically, we take as varieties {0, 1, 2, 3, 4, 5, 6, 7, 8} and as blocks {0124, 0125, 0126, 0127, 0135, 0136, 0138, 0147, 0148, 0157, 0158, 0168, 0234, 0236, 0237, 0245, 0248, 0258, 0267, 0278, 0345, 0346, 0356, 0367, 0368, 0378, 0456, 0457, 0468, 0478, 0567, 0578, 1235, 1236, 1237, 1238, 1246, 1247, 1258, 1268, 1345, 1347, 1348, 1356, 1378, 1456, 1457, 1467, 1478, 1567, 1568, 1678, 2346, 2347, 2348, 2357, 2358, 2456, 2458, 2467, 2567, 2568, 2578, 2678, 3457, 3458, 3468, 3567, 3578, 3678, 4568, 4678}. None of the 72 blocks is repeated, and it appears this BIBD is new.

6. Concluding remarks. It should be possible to construct more designs based on the results of Sections 3 and 4. When $n > 2$ in Theorem 3, the fact that the caps in our partition of $\Sigma = PG(2n - 1, q)$ form a copy of

https://doi.org/10.4153/CJM-1985-063-1 Published online by Cambridge University Press

$PG(n - 1, q)$ could prove useful in an induction argument aimed at constructing spreads or packings of Σ. It would also be interesting to know when the M-caps of Theorems 1 and 3 are complete.

This research was originally motivated by the search for proper 2-covers of $\Sigma = PG(3, q)$. By a proper 2-cover of Σ we mean a set of $2(q^2 + 1)$ lines doubly covering the points of Σ but which cannot be partitioned into two spreads. The author is grateful to A. Bruen, who posed the existence question for proper 2-covers, U. Ott, and B. Rothschild for stimulating conversations concerning 2-covers of $PG(3, 2)$ and $PG(3, 3)$. In a future paper ovoidal fibrations will be used to show proper 2-covers exist in $PG(3, q)$ for all odd prime powers q.

The author would also like to thank R. Biggs for his computer programming help in constructing example (3). Finally it should be mentioned that A. Brouwer has independently fibrated $PG(3, q)$ into ovoids for odd q.

References

1. A. Barlotti, *Un'estensione del teorema di Segre-Kustaanheimo*, Boll. Un. Mat. Ital. *10* (1955), 498-506.
2. B. C. Kestenband, *Projective geometries that are disjoint unions of caps*, Can. J. Math. *32* (1980), 1299-1305.
3. ——— *Hermitian configurations in odd-dimensional projective geometries*, Can. J. Math. *33* (1981), 500-512.
4. B. Qvist, *Some remarks concerning curves of the second degree in a finite plane*, Ann. Acad. Sci. Fenn. *134* (1952), 1-27.

University of Delaware,
Newark, Delaware

https://doi.org/10.4153/CJM-1985-063-1 Published online by Cambridge University Press