DIFFERENCE SETS AND PLANAR POLARITIES

by MICHAEL J. GANLEY

(Received 15 March, 1973; revised 28 June, 1973)

1. Introduction. A *block design* is a finite set p of elements called *points*, where $|p| = v$, together with certain distinguished subsets of p called *blocks*, such that

(i) each block contains k points,
(ii) each point is contained in r blocks, and
(iii) two distinct points are contained in precisely λ blocks.

If we let b denote the number of blocks, then we have

$$vr = bk \qquad \text{and} \qquad \lambda(v-1) = r(k-1),$$

and we say that the design is a (v, k, λ)-*design*. If $v=b$, then we say that the design is *symmetric*, and we have

$$\lambda(v-1) = k(k-1).$$

A *polarity* of a (necessarily symmetric) block design is a mapping ρ : points $\leftrightarrow$ blocks, such that ρ preserves incidence and $\rho^2 = I$, the identity mapping. If a point (or block) is incident with its image under ρ, then we say that the point (or block) is *absolute*. In an earlier paper [3] the concept of planar polarity was introduced (see §2 for the definition of planar) and it was shown that in certain cases the set of absolute points and non-absolute blocks themselves form a block design. Except in the case of projective planes, for which all polarities are planar, there are remarkably few examples of such polarities.

In an attempt to discover new planar polarities it is natural to investigate those designs **B** which arise from abelian difference sets, as all such **B** admit polarities. Abelian difference sets are studied in §3 of this paper, whilst in §4 we specialize to cyclic difference sets. Unfortunately, in the latter, we only obtain one new example of a planar polarity, which occurs in a block design having parameters (37, 9, 2), and in this case the set of absolute points and non-absolute blocks do not form a design.

In §2 basic definitions and results are given, although for more detailed information the reader is referred to Baumert [1], Dembowski [2], Hall [5] and Mann [7].

2. Preliminary discussion. We suppose that **B** is a symmetric (v, k, λ)-design, so that $\lambda(v-1)=k(k-1)$. If **B** admits a polarity ρ, the following results give some information concerning the number of absolute points $a(\rho)$ of ρ.

RESULT 1 (see Dembowski [2, p. 64]). $a(\rho) = k+\alpha(k-\lambda)^{\frac{1}{2}}$, *where* α *is an integer having opposite parity to* v. *In particular, if* $k-\lambda$ *is non-square, then* $a(\rho) = k$.

A polarity will be called *planar* if each absolute point is incident with exactly one absolute block.

https://doi.org/10.1017/S0017089500002263 Published online by Cambridge University Press

RESULT 2 [3]. *If ρ is planar, then* $a(\rho) \leqq \dfrac{v-k}{(k-\lambda)^{\frac{1}{2}}}+1$.

RESULT 3 [3]. *If ρ is planar, then* $a(\rho) = \dfrac{v-k}{(k-\lambda)^{\frac{1}{2}}}+1$ *if and only if the set of absolute points and non-absolute blocks of ρ forms a block design. If this is the case, then the design has parameters*

$$\left(\frac{v-k}{(k-\lambda)^{\frac{1}{2}}}+1, \quad (k-\lambda)^{\frac{1}{2}}+1, \quad \lambda\right).$$

Results 2 and 3 were first proved by Seib [8] in the particular case of $\lambda = 1$. From Results 1 and 2 we have the following lemma.

LEMMA 1. *If* **B** *admits a planar polarity ρ and if $k-\lambda$ is non-square (and hence v is odd by the Bruck–Ryser Theorem), then* $k \geqq \lambda^2+\lambda+1$.

Proof. From Results 1 and 2,

$$k-1 < \frac{v-k}{(k-\lambda)^{\frac{1}{2}}},$$

i.e. $$(k-\lambda)(k-1)^2 < (v-k)^2,$$

i.e. $$\lambda^2(k-\lambda)(k-1)^2 < \lambda^2(v-k)^2 = (k-\lambda)^2(k-1)^2;$$

so $$k-\lambda > \lambda^2 \qquad \text{or} \qquad k \geqq \lambda^2+\lambda+1.$$

There are few known examples of planar polarities. These include the following:

(i) All polarities of finite projective planes (i.e. when $\lambda = 1$). (See for instance [2, p. 9].)

(ii) Certain trivial examples; in particular, polarities having no absolute points, and also when **B** is a $(v, v-1, v-2)$-design and $a(\rho) = 2$. (See [3].)

A third example is given by the following theorem.

THEOREM 1. *Let $PG(d, q)$ denote the d-dimensional projective space over the finite field $GF(q)$. If $d \geqq 3$, then $PG(d, q)$ admits planar polarities if and only if $d = 3$ and q is odd.*

Proof. We merely sketch the proof, as it is essentially contained in Dembowski [2, pp. 41–51]. Firstly note that $PG(d, q)$ is a symmetric block design with parameters

$$v = \frac{q^{d+1}-1}{q-1}, \qquad k = \frac{q^d-1}{q-1}, \qquad \lambda = \frac{q^{d-1}-1}{q-1}.$$

The polarities of $PG(d, q)$ are of three possible types, namely orthogonal, unitary or symplectic; and since for the latter possibility every point is absolute, such a polarity can never be planar. For unitary polarities, we must have $q = s^2$, and the number of absolute points is given by

$$a(\rho) = \frac{\prod_{i=d}^{i=d+1} (s^i-(-1)^i)}{(s^2-1)}.$$

https://doi.org/10.1017/S0017089500002263 Published online by Cambridge University Press

Straightforward calculation shows that, if $d \geqq 3$, then this number is always greater than

$$\frac{v-k}{(k-\lambda)^{\frac{1}{2}}}+1.$$

In the case of orthogonal polarities [2, p. 46], it is easy to show in the manner indicated above, that, when q is odd, if such a polarity is planar, then $d = 3$ and the polarity is of index 1. In this case the absolute points and blocks are precisely the points and tangent hyperplanes of some non-degenerate quadric in $PG(3, q)$ and so the polarity must be planar.

Finally, if q is even, by a result in [2, p. 44], the absolute points of an orthogonal polarity in $PG(d, 2^e)$ are precisely the points of some hyperplane in the space, and so

$$a(\rho) = \frac{q^d-1}{q-1} > \frac{v-k}{(k-\lambda)^{\frac{1}{2}}}+1,$$

and thus ρ cannot be planar. This completes the proof of the theorem.

REMARKS. It should be pointed out that not all orthogonal polarities in $PG(3, q)$, q odd, are planar, but only those of index 1 (see Dembowski [2]). In this case $a(\rho) = q^2+1$, which is the maximal number of absolute points attainable. Consequently, the set of absolute points and non-absolute hyperplanes forms a design with parameters $(q^2+1, q+1, q+1)$. Any block design with such parameters is known as an *inversive plane* or *Möbius plane* (Dembowski [2, Chapter 6]).

Now suppose that **B** is any design admitting a polarity ρ. Then we can construct the *complementary design* **B*** having parameters (v^*, k^*, λ^*), where $v^* = v$, $k^* = v-k$ and $\lambda^* = v-2k+\lambda$. The points of **B*** are the points $p_1, \ldots, p_v$ of **B**, and the blocks of **B*** are the point sets $b_i = p-p_i\rho$, for $i = 1, 2, \ldots v$. It is clear that **B*** so defined is a design and has the parameters stated above. Also **B*** admits a polarity $\rho^*: p_i \leftrightarrow b_i$, and $a(\rho^*) = v-a(\rho)$.

LEMMA 2. *Suppose that* **B** *is nontrivial (i.e.* $k-\lambda > 1$*) and admits a planar polarity* ρ*; then the polarity* ρ^* *of* **B*** *is not planar.*

Proof. If both ρ and ρ^* are planar, then, by Result 2,

$$a(\rho) \leqq \frac{v-k}{(k-\lambda)^{\frac{1}{2}}}+1 \qquad \text{and} \qquad a(\rho^*) \leqq \frac{v^*-k^*}{(k^*-\lambda^*)^{\frac{1}{2}}}+1 = \frac{k}{(k-\lambda)^{\frac{1}{2}}}+1.$$

Hence $a(\rho)+a(\rho^*) = v \leqq \dfrac{v}{(k-\lambda)^{\frac{1}{2}}} + 2$. So $(v-2)(k-\lambda)^{\frac{1}{2}} \leqq v$. Thus either $k-\lambda = 1$ or $v^2 \geqq 2(v-2)^2$, which gives $v \leqq 6$; so **B** is trivial.

As an analagous result to Lemma 1, we have

LEMMA 3. *Suppose that* $k-\lambda$ *is non-square; then, if* ρ^* *is planar we must have* $k \leqq \frac{3}{2}\lambda+1$.

The proof is straightforward and so we shall omit it.

3. Abelian difference sets and planar polarities. In our search for planar polarities it is natural to look at those (v, k, λ)-designs that are determined by abelian difference sets, as

https://doi.org/10.1017/S0017089500002263 Published online by Cambridge University Press

all such designs admit polarities which can be described very easily. We begin with a little terminology.

Let $\mathcal{G}$ be a finite abelian group of order v and suppose that $\mathcal{G}$ is written additively. Let $\mathcal{D}$ be a subset of $\mathcal{G}$, with $|\mathcal{D}| = k$, such that every non-identity element of $\mathcal{G}$ can be represented in the form $d_1 - d_2$, with $d_1, d_2 \in \mathcal{D}$, in exactly λ distinct ways. Let $n = k - \lambda$. Then we say that $\mathcal{D}$ is a (v, k, λ, n)-*difference set*. A *translate* of $\mathcal{D}$, written $\mathcal{D}+g$, is the set of elements $\{d+g : d \in \mathcal{D}\}$ for some element $g \in \mathcal{G}$. Also, if t is an integer, then we define $t\mathcal{D} = \{td : d \in \mathcal{D}\}$. With the elements of $\mathcal{G}$ as points and the translates of $\mathcal{D}$ as blocks, it is easy to see that we obtain a symmetric (v, k, λ)-design.

Throughout this section we shall assume that, if $\mathbf{B}$ is a (v, k, λ)-design, then it has been obtained, in the manner described above, from a (v, k, λ, n) abelian difference set.

LEMMA 4. *The mapping ρ of $\mathbf{B}$ given by $\rho : g \leftrightarrow \mathcal{D} - g$ is a polarity of $\mathbf{B}$; moreover, the point g is absolute if and only if $2g \in \mathcal{D}$. In particular, if v is odd, then $a(\rho) = k$.*

Proof. The proof is trivial. For the final part, note that the mapping $\theta : g \to 2g$ is an automorphism of $\mathcal{G}$.

Again, unless otherwise stated, throughout this section we shall assume that the polarity ρ of $\mathbf{B}$ is of the type described in Lemma 4. We now translate the idea of planar polarity into the language of difference sets.

DEFINITION. Let $\mathcal{D}$ be an abelian difference set. We say that $\mathcal{D}$ *satisfies condition* P if, for every pair of distinct elements $g, h \in \mathcal{G}$ for which $2g, 2h \in \mathcal{D}$, we have $g + h \notin \mathcal{D}$.

LEMMA 5. *The polarity ρ defined in Lemma 4 is planar if and only if $\mathcal{D}$ satisfies condition* P.

The proof is trivial.

LEMMA 6. *If $|\mathcal{G}| = v$ is odd, then $\mathcal{D}$ satisfies condition* P *if and only if $\mathcal{D}$ does not contain 3 elements in arithmetic progression.*

Proof. Suppose that $g \in \mathcal{G}$ and $2g \in \mathcal{D}$; then there exists $d \in \mathcal{D}$ with $g = \frac{1}{2}d$. Since, if v is odd, ρ has k absolute points, then every absolute point is of the form $\frac{1}{2}d$ for some $d \in \mathcal{D}$. Condition P says that, for all distinct $d_i, d_j \in \mathcal{D}$, $\frac{1}{2}d_i + \frac{1}{2}d_j \notin \mathcal{D}$, i.e. $d_i + d_j \notin 2\mathcal{D}$. Clearly this is equivalent to the statement that $\mathcal{D}$ does not contain 3 elements in arithmetic progression.

That Lemma 6 is not true in the case when v is even can be seen by considering the following example.

Let $\mathcal{G}$ be the cyclic group of order 40; then the set

$$\mathcal{D} = \{1, 2, 3, 5, 6, 9, 14, 15, 18, 20, 25, 27, 35\}$$

is a difference set in $\mathcal{G}$ having parameters (40, 13, 4, 9). Simple calculation shows that the absolute points of ρ are the points $\{1, 3, 7, 9, 10, 21, 23, 27, 29, 30\}$ and that $\mathcal{D}$ satisfies condition P. However, $\mathcal{D}$ certainly contains 3 elements in arithmetic progression. The block design obtained in this case is $PG(3, 3)$, which, as we have already noted, admits planar polarities.

DEFINITION. The integer t is said to be a *multiplier* of $\mathcal{D}$ if $t\mathcal{D} = \mathcal{D}+g$ for some $g\in\mathcal{G}$.

RESULT 4 (The Multiplier Theorem; see for instance Baumert [1, p. 54]). *Let $\mathcal{D}$ be a (v, k, λ, n) difference set, and let n_0 be a divisor of n, where $(n_0, v) = 1$ and $n_0 > \lambda$. If, for every prime p dividing n_0, there is an integer j_p such that $p^{j_p} \equiv t \pmod{v}$, then t is a multiplier of $\mathcal{D}$.*

COROLLARY. *If v is odd and $n = 2^\alpha w$, where w is odd and $2^\alpha > \lambda$, then 2 is a multiplier of every difference set $\mathcal{D}$ having parameters (v, k, λ, n).*

THEOREM 2. *If $|\mathcal{G}| = v$ is odd, and $\mathcal{D}$ admits 2 as a multiplier, then $\mathcal{D}$ satisfies condition* P *if and only if $\lambda = 1$.*

Proof. We need only show that if $\mathcal{D}$ satisfies condition P, then $\lambda = 1$. By Lemma 6, every translate of $\mathcal{D}$ must satisfy condition P, and, since the multiplier 2 must fix at least one translate of $\mathcal{D}$ [7, p. 80], then we may as well assume that $2\mathcal{D} = \mathcal{D}$. So, from Lemma 6, we must have that $d_i+d_j\notin\mathcal{D}$ for all distinct $d_i, d_j\in\mathcal{D}$. Now if $d\in\mathcal{D}$ and $d\neq 0$, then there exist $d_i, d_j\in\mathcal{D}$ such that $d_i-d_j = d$, i.e. $d_i = d+d_j$. However, this is not possible unless $d_j = d$ (and hence $d_i = 2d$) and so d can be represented uniquely as a difference of elements of $\mathcal{D}$. Hence $\lambda = 1$, as claimed.

COROLLARY. *If v is odd and $n = 2^\alpha w$, where w is odd and $2^\alpha > \lambda > 1$, then no abelian difference set with parameters (v, k, λ, n) can satisfy condition* P.

4. Cyclic difference sets and planar polarities. We continue with the hypotheses of §3 and the additional assumption that $\mathcal{G}$ is cyclic.

LEMMA 7. *If v is odd, then $a(\rho) = k$. If v is even, then $a(\rho) = k\pm(k-\lambda)^{\frac{1}{2}}$.*

Proof. See Lemma 4 for the case when v is odd. For v even, we want the number of elements $g\in\mathcal{G}$ for which $2g\in\mathcal{D}$. As v is even and $\mathcal{G}$ is cyclic, then each even residue of $\mathcal{D}$ gives rise to two absolute points and each odd residue gives rise to no absolute points. Suppose that $\mathcal{D}$ contains x even residues, and hence $k-x$ odd residues. By counting the odd residues in $\mathcal{G}$, we obtain

$$2x(k-x) = \tfrac{1}{2}\lambda v,$$

i.e.
$$4x^2-4kx+\lambda v = 0$$

i.e.
$$x = \tfrac{1}{2}(k\pm(k-\lambda)^{\frac{1}{2}}),$$

using $\lambda(v-1) = k(k-1)$. Hence the number of absolute points of ρ is $k\pm(k-\lambda)^{\frac{1}{2}}$.

REMARK. In the case when v is even, if ρ is defined with respect to $\mathcal{D}$ and $a(\rho) = k-(k-\lambda)^{\frac{1}{2}}$, then the polarity ρ' defined with respect to $\mathcal{D}+1$ has $a(\rho') = k+(k-\lambda)^{\frac{1}{2}}$. For instance, in $PG(3, q)$, where q is odd, we have $a(\rho) = q^2+1$, which is the maximum possible for a planar polarity, and $a(\rho') = (q+1)^2$, and so ρ' is not planar. This, in particular, explains why not all orthogonal polarities in $PG(3, q)$, q odd, are planar, as claimed in the remarks after Theorem 1.

LEMMA 8. *For $\mathcal{G}$ cyclic and ρ planar, we have*

(i) $k \geqq \lambda^2+\lambda$ *if* v *is odd,*

(ii) $\begin{cases} k \geqq \lambda^2+3\lambda+1 \text{ if } v \text{ is even and } a(\rho) = k+(k-\lambda)^{\frac{1}{2}}, \\ k \geqq \lambda^2-\lambda+1 \text{ if } v \text{ is even and } a(\rho) = k-(k-\lambda)^{\frac{1}{2}}. \end{cases}$

Proof. The proof of (i) is the same as that of Lemma 1. A similar method for (ii), using Lemma 7 and Result 2, gives a cubic inequality for $(k-\lambda)^{\frac{1}{2}}$ in terms of λ, whence $(k-\lambda)^{\frac{1}{2}} > \lambda$ or $\geqq \lambda-1$ according as $a(\rho) = k \pm (k-\lambda)^{\frac{1}{2}}$, respectively.

Using Lemma 8 we have the following result.

THEOREM 3. *Let $\mathcal{D}$ be a cyclic difference set with parameters (v, k, λ, n), with $k \leqq 100$, $n > 1$ and $k < \frac{1}{2}v$. Then the polarity ρ of* **B**, *as described in Section* 3, *is planar if*

(i) $\lambda = 1$,

(ii) $\mathbf{B} = PG(3, q)$ *with q odd and* $a(\rho) = k-(k-\lambda)^{\frac{1}{2}} = q^2+1$,

or (iii) $(v, k, \lambda, n) = (37, 9, 2, 7)$.

Moreover, with the possible exception of $(v, k, \lambda, n) = (400, 57, 8, 49)$ *or* $(820, 91, 10, 81)$, *with* $a(\rho) = 50$ *and* 82 *respectively, no other sets $\mathcal{D}$ satisfy condition* P. *Finally, whenever $k < \frac{1}{2}v$, the polarity ρ^* of the complementary design* $\mathbf{B}^*$ *to* **B** *is never planar.*

Proof. It has been shown [**1**, p. 145] that the only parameter sets (v, k, λ, n) with $k \leqq 100$, $n > 1$, $k < \frac{1}{2}v$, for which cyclic difference sets can exist are those which appear in Baumert's table [**1**, pp. 150–158]. Applying Lemma 8 to these parameter sets, we find that ρ can be planar only if (i) $\lambda = 1$, (ii) $(v, k, \lambda, n) = (q^3+q^2+q+1,\ q^2+q+1,\ q+1,\ q^2)$ with $q = 3, 5, 7$ or 9 and $a(\rho) = q^2+1$, or (iii) $(v, k, \lambda, n) = (37, 9, 2, 7)$.

Now all polarities of finite projective planes (i.e. for $\lambda = 1$) are planar, and those polarities of $PG(3, q)$, with q odd and $a(\rho) = q^2+1$, are also planar, by Theorem 1. As Baumert's table is complete for $k \leqq 50$, it follows that the only possible exceptions to (ii) are when $q = 7$ or 9; i.e., there may exist other designs with parameters (400, 57, 8) or (820, 91, 10), which are not isomorphic to the corresponding $PG(3, q)$, and yet which arise from cyclic difference sets, for which the polarity ρ is planar, with $a(\rho) = 50$ or 82 respectively.

For case (iii), all difference sets with parameters (37, 9, 2, 7) are equivalent to the set $\mathcal{D}_0 = \{1, 7, 9, 10, 12, 16, 26, 33, 34\}$. As $\mathcal{D}_0$ does not contain 3 elements in arithmetic progression, it follows from Lemma 6 that the polarity ρ is planar.

Now consider the polarity ρ^* associated with the complementary difference set $\mathcal{D}^*$ of $\mathcal{D}$, having parameters $(v, v-k, v-2k+\lambda, n)$. If v is odd, then, by Lemma 7, $a(\rho^*) = v-k$, whereas if v is even, $a(\rho^*) = v-k \pm (k-\lambda)^{\frac{1}{2}}$. Suppose that v is odd; then, if ρ^* is planar, we have, by Result 2, $v-k \leqq \dfrac{k}{(k-\lambda)^{\frac{1}{2}}} + 1$. Using the fact that $\lambda(v-1) = k(k-1)$, we have

$$\lambda \geqq (k-1-\lambda)(k-\lambda)^{\frac{1}{2}}.$$

Now, if $k < \frac{1}{2}v$, it is clear that $\lambda < \frac{1}{2}k$, so that the above equation gives $\lambda > (\lambda-1)\lambda^{\frac{1}{2}}$, i.e. $\lambda > (\lambda-1)^2$, i.e. $\lambda = 1$ or $\lambda = 2$.

If $\lambda = 2$, then, from above, we have $2 \geqq (k-3)(k-2)^{\frac{1}{2}}$, so that $k \leqq 4$. But then we do not have $\lambda < \frac{1}{2}k$. Hence if $\lambda = 2$, ρ^* is never planar. Finally, if $\lambda = 1$, then, by Lemma 2, ρ^* cannot be planar.

A similar argument for the case when v is even will complete the proof of the theorem.

The difference set having parameters (37, 9, 2, 7) is truly exceptional, as we shall demonstrate. Let p be a prime of the form $p = 4x^2+1$, where x is odd; then the biquadratic residues modulo p form a difference set having parameters

$$(v, k, \lambda, n) = (4x^2+1, x^2, \tfrac{1}{4}(x^2-1), \tfrac{1}{4}(3x^2+1)),$$

(see Baumert [**1**, p. 120]), and the difference set with parameters (37, 9, 2, 7) belongs to this family. We denote by $\mathscr{F}$ the family of designs arising from such difference sets.

THEOREM 4. *The only nontrivial member* **B** *of* $\mathscr{F}$ *which admits a planar polarity is the design having parameters* (37, 9, 2).

Proof. We remark first of all that we are now no longer merely considering the polarities that are associated directly with the difference set, but any polarity of **B**.

We wish to know when $n = k-\lambda = \frac{1}{4}(3x^2+1)$ is a square. Suppose that $3x^2+1 = y^2$, so that $12x^2+4 = 4y^2$. We also have that $12x^2+3 = 3p$, for some prime p, and hence $4y^2-1 = 3p$, so that $3p = (2y-1)(2y+1)$, which gives $3 = 2y-1$ and $p = 2y+1$, yielding a trivial design having parameters (5, 1, 0). Thus we may assume that **B** has n a non-square. Hence, from Lemma 1, if **B** admits a planar polarity, then $x^2 \geqq (\frac{1}{4}(x^2-1))^2 + \frac{1}{4}(x^2-1)+1$. This can only happen if $x = 1$ or 3. Disregarding $x = 1$, we obtain the design **B** having parameters (37, 9, 2) and, as we have already seen, this design admits a planar polarity.

We can use a similar proof to that given above to show that in all of the following families of cyclic difference sets, no polarity of the corresponding block design can be planar. (See Hall [**5**, pp. 141–2] for details.)

(i) Quadratic residues in $GF(q)$ ($q \equiv 3 \pmod 4$), except when $q = 7$, in which case we obtain the projective plane of order 2.

(ii) Certain residues modulo a prime of the form $p = 4x^2+27$.

(iii) Biquadratic residues, and zero, modulo primes of the form $4x^2+9$, where x is odd, except $x = 1$, in which case we obtain the projective plane of order 3.

(iv) Octic residues of primes $p = 8a^2+1 = 64b^2+9$, with a and b odd, except when $a = 3$ and $b = 1$, in which case we obtain the projective plane of order 8.

(v) Octic residues, and zero, modulo $p = 8a^2+49 = 64b^2+441$, where a is odd and b is even.

In the following cases $k-\lambda$ is a square, and so determination of all polarities is rather difficult. However, it is easy to show that the polarity directly associated with the difference set is never planar.

(vi) Twin prime difference sets.

(vii) Whiteman's generalizations of the twin prime difference sets.

(viii) The Gordon–Mills–Welch multiply-inequivalent difference sets, in the case of $k-\lambda$ being a square. If $k-\lambda$ is non-square then none of the polarities are planar.

Finally, the polarities of the block designs derived from the other known family of cyclic difference sets, namely the Singer difference sets, have already been discussed in Theorem 1.

5. Planar polarities with the maximum number of absolute points. Clearly, if we have a (v, k, λ)-design **B** admitting a planar polarity ρ, then the most interesting case is when $a(\rho) = \dfrac{v-k}{(k-\lambda)^{\frac{1}{2}}}+1$ (see Result 3), as in this case the absolute points and non-absolute blocks of ρ themselves form a block design, say $\mathscr{U}$, having parameters $\left(\dfrac{v-k}{(k-\lambda)^{\frac{1}{2}}}+1, \quad (k-\lambda)^{\frac{1}{2}}+1, \quad \lambda\right)$. Note that $\mathscr{U}$ is necessarily non-symmetric provided that $v > 4$.

By Result 1, if this maximum number of absolute points is to be attained, we must have

$$\frac{v-k}{(k-\lambda)^{\frac{1}{2}}}+1 = k+\alpha(k-\lambda)^{\frac{1}{2}},$$

where α is an integer having opposite parity to v.

Thus $$(k-1)(k-\lambda)^{\frac{1}{2}}+\alpha(k-\lambda) = v-k,$$

i.e. $$\lambda(k-1)(k-\lambda)^{\frac{1}{2}}+\alpha\lambda(k-\lambda) = \lambda(v-k) = (k-1)(k-\lambda);$$

so $$(k-\lambda)^{\frac{1}{2}} \mid \lambda(k-1),$$

i.e. $$(k-\lambda)^{\frac{1}{2}} \mid \lambda(\lambda-1). \tag{i}$$

Write $(k-\lambda)^{\frac{1}{2}} = m$, and let

$$\lambda(\lambda-1) = mu. \tag{ii}$$

From above

$$\alpha\lambda m = (m-\lambda)(k-1) \tag{iii}$$

and so

$$\alpha\lambda = k-1-u-\lambda m. \tag{iv}$$

Thus $$\lambda \mid (k-1-u) \quad \text{or} \quad \lambda \mid (m^2-1-u). \tag{v}$$

Since $\lambda(v-1)=k(k-1)$, and so $\lambda \mid k(k-1)$, then (v) gives

$$\lambda \mid u(u+1). \tag{vi}$$

These equations are very restrictive on the parameters (v, k, λ) for which the maximum number of absolute points can be achieved. In some cases we can say more:

LEMMA 9. *If $m > 1$ and $\lambda = p^r$, where p is a prime and $r > 0$, then if $a(\rho) = \dfrac{v-k}{(k-\lambda)^{\frac{1}{2}}} + 1$, we must have either*

(a) *p is odd, $\alpha = 0$ and $(v, k, \lambda) = (\lambda^3+2\lambda^2, \lambda^2+\lambda, \lambda)$, or*
(b) *$p = 2$, $\alpha = -1$ and $(v, k, \lambda) = (\lambda^3-2\lambda^2+2\lambda, \lambda^2-\lambda+1, \lambda)$.*

https://doi.org/10.1017/S0017089500002263 Published online by Cambridge University Press

Proof. Suppose that $p^s \| u$. From (vi), one possibility is that $s = 0$ and $\lambda | (u+1)$. In this case, (ii) gives that $u | (\lambda - 1)$; so we must have $\lambda = u+1$, and hence $\lambda = m$. So $k = \lambda^2 + \lambda$, $v = \lambda^3 + 2\lambda^2$ and $\alpha = 0$. Thus v, and hence λ, are odd and we are in case (a).

The other possibility from (vi) is that $s > 0$, and so $s \geqq r$. From (ii), $s = r$ and so $m | (\lambda - 1)$. From (v) $\lambda | (m-1)(m+1)$ and so either $\lambda | (m \pm 1)$ or else $\frac{1}{2}\lambda | (m \pm 1)$, in which case $p = 2$. Using also the fact that $m | (\lambda - 1)$, we see that the first of these possibilities gives $\lambda = m+1$ and we are in case (b). Otherwise, if $\frac{1}{2}\lambda | m-1$, we have that $m = 3$ and $\lambda = 4$, which has already been covered, whereas, if $\frac{1}{2}\lambda | (m+1)$, we again have $\lambda = m+1$.

Using Lemma 9, together with equations (i)–(vi), we can quickly obtain the following list as the only possibilities for nontrivial (v, k, λ)-designs **B** with $\lambda < 10$ that can admit a planar polarity having the maximum number of absolute points.

λ	**B**	$\mathcal{U}$
(i) $\lambda = 1$	$(s^4 + s^2 + 1, s^2 + 1, 1)$	$(s^3 + 1, s + 1, 1)$
(ii) $\lambda = 3$	(45, 12, 3)	(12, 4, 3)
(iii) $\lambda = 4$	(40, 13, 4)	(10, 4, 4)
(iv) $\lambda = 5$	(175, 30, 5)	(30, 6, 5)
(v) $\lambda = 6$	(16, 10, 6)	(4, 3, 6)
(vi) $\lambda = 6$	(156, 31, 6)	(26, 6, 6)
(vii) $\lambda = 6$	(1856, 106, 6)	(176, 11, 6)
(viii) $\lambda = 6$	(8856, 231, 6)	(576, 16, 6)
(ix) $\lambda = 7$	(441, 56, 7)	(56, 8, 7)
(x) $\lambda = 8$	(400, 57, 8)	(50, 8, 8)
(xi) $\lambda = 9$	(891, 90, 9)	(90, 10, 9)

Concerning this list of possibilities we make the following remarks.

(a) Case (i) occurs in desarguesian, and certain non-desarguesian, projective planes of order s^2. Block designs with parameters $(s^3+1, s+1, 1)$ are known as *unitals*. (See, for instance, [**4**].)

(b) Cases (iii), (vi) and (x) occur in $PG(3, 3)$, $PG(3, 5)$ and $PG(3, 7)$, respectively (Theorem 1), and the corresponding $\mathcal{U}$ are the classical miquelian inversive planes. (See Dembowski [**2**, Chapter 6].)

(c) For cases (ii), (iv), (ix) and (xi), there do not exist cyclic difference sets with parameters (v, k, λ, n) (see, e.g., [**1**]), although they can occur in the abelian case (McFarland [**6**]), though it is easy to prove that none of the abelian difference sets described in [**6**] can satisfy condition P.

(d) There does not appear to be anything in the literature concerning cases (vii) and (viii), although no cyclic difference set with parameters (1856, 106, 6, 100) exists, from Baumert [**1**, Theorem 2.17]. However, R. L. McFarland (in a private communication) has shown, by considering the homomorphic image in the cyclic group C_{29}, of order 29, that there is no abelian difference set with these parameters. Similarly, by considering C_{41}, no abelian difference set with parameters (8856, 231, 6225) can exist.

(e) Finally, case (v) cannot occur. We outline the proof below; we attempt to construct

an incidence matrix. Let $p_1, \ldots, p_{16}$ be the points of **B**, and let $b_i = p_i\rho$ $(i = 1, \ldots, 16)$ be the blocks of **B**. The required matrix is then symmetric. Let $p_1, \ldots, p_4$ be the absolute points of ρ; then, by Result 3, the points $p_1, \ldots, p_4$ and the blocks $b_5, \ldots, b_{16}$ form a design with parameters (4, 3, 6). Using this fact, and also the fact that ρ is planar, we are able to fill in the first 4 rows and the first 4 columns of the matrix as shown below.

	b_1	b_2	b_3	b_4	b_5	b_6	b_7	b_8	b_9	b_{10}	b_{11}	b_{12}	b_{13}	b_{14}	b_{15}	b_{16}
p_1	1	0	0	0	1	1	1	1	1	1	1	1	1	0	0	0
p_2	0	1	0	0	1	1	1	1	1	1	0	0	0	1	1	1
p_3	0	0	1	0	1	1	1	0	0	0	1	1	1	1	1	1
p_4	0	0	0	1	0	0	0	1	1	1	1	1	1	1	1	1
p_5	1	1	1	0	0	1	0	1	1	0	1	1	0	1	1	0
p_6	1	1	1	0	1	0	0	1	0	1	1	0	1	1	0	1
p_7	1	1	1	0	0	0										
p_8	1	1	0	1	1	1										
p_9	1	1	0	1	1	0										
p_{10}	1	1	0	1	0	1										
p_{11}	1	0	1	1	1	1										
p_{12}	1	0	1	1	1	0										
p_{13}	1	0	1	1	0	1										
p_{14}	0	1	1	1	1	1										
p_{15}	0	1	1	1	1	0										
p_{16}	0	1	1	1	0	1										

Next, column 5 can be completed, by using the fact that b_5 is non-absolute and has precisely 6 points in common with each of the blocks b_1, b_2, b_3 and b_4. This enables us to complete column 5 in an essentially unique manner, as shown. Row 5 follows by symmetry. Similarly, row 6 and column 6 can be completed as shown and we can then check that it is impossible to complete column 7 subject to the required conditions.

REFERENCES

1. L. D. Baumert, *Cyclic difference sets*, Lecture Notes in Mathematics (Springer, Berlin–Heidelberg, 1971).

2. P. Dembowski, *Finite geometries* (Springer, Berlin–Heidelberg, 1968).

3. M. J. Ganley, Polarities of designs, *Bull. London Math. Soc.* **4** (1972), 20–22.

4. M. J. Ganley, A class of unitary block designs, *Math. Zeit.* **128** (1972), 34–42.

5. M. Hall, *Combinatorial theory* (Waltham, Mass., 1967).

6. R. L. McFarland, A family of difference sets in non-cyclic groups, *J. Combinatorial Theory* **15** (1973), 1–10.

7. H. B. Mann, *Addition theorems* (New York, 1965).

8. M. Seib, Unitäre Polaritäten endlicher projektiver Ebenen, *Arch. Math.* **21** (1970), 103–112.

UNIVERSITY OF GLASGOW
GLASGOW G12 8QW