ON RELATIVE DIFFERENCE SETS AND PROJECTIVE PLANES

by FRED PIPER

(Received 23 August, 1973)

1. Introduction. A permutation group is *quasiregular* if it acts regularly on each of its orbits (i.e. the stabiliser of an element fixes every other element in its orbit). So, in particular, any permutation representation of an abelian or hamiltonian group must be quasiregular.

If P is a finite projective plane of order n with a quasiregular collineation group G then, since G must act faithfully on at least one orbit [2, p. 181], $|G| \leqq n^2+n+1$. In [3] quasiregular collineation groups G with $|G| > \frac{1}{2}(n^2+n+1)$ were studied and the following theorem was proved.

THEOREM 1. *Let G be a quasiregular collineation group of a projective plane P of order n. Denote by t the number of point (or line; see* [6, p. 257]*) orbits of G and by F the substructure of the elements fixed by G. If $|G| > \frac{1}{2}(n^2+n+1)$, then there are only the following possibilities:*

(a) $|G| = n^2+n+1$, $t = 1$ *and* $F = \phi$.

(b) $|G| = n^2$, $t = 3$ *and F is a flag.*

(c) $|G| = n^2$, $t = n+2$ *and F is either a line with all its incident points or its dual.*

(d) $|G| = n^2-1$, $t = 3$ *and F is a non-incident point-line pair.*

(e) $|G| = n^2-\sqrt{n}$, $t = 2$ *and* $F = \phi$.

(f) $|G| = n(n-1)$, $t = 5$ *and F consists of two points, the line joining them and a second line through one of the points.*

(g) $|G| = (n-1)^2$, $t = 7$ *and F consists of the vertices and sides of a triangle.*

(h) $|G| = (n-\sqrt{n}+1)^2$, $t = 2\sqrt{n}+1$ *and* $F = \phi$.

Examples of quasiregular groups of each type are known in finite desarguesian planes. However the only known cases of type (e) or type (h) occur when $n = 4$ and it is possible that there are no others. Certainly if there are other examples then the groups must act on non-desarguesian planes; in fact the planes must be new as it is easy to check that no known plane with $n \neq 4$ can admit a group of type (e) or (h).

In this note we discuss planes that admit quasiregular groups of type (e) and show that such planes of order q^2 exist if and only if there is a group G of order q^4-q with a relative difference set with respect to a normal subgroup H of order q^2-q. This is a natural analogue to the theorem that says that a plane P admits a group G of type (a) (i.e. a Singer group) if and only if G has a difference set.

For the standard definitions and basic results on projective planes see [6].

2. Relative difference sets. Let G be a finite group with a normal subgroup H. A subset S of G is called a *relative λ-difference set* of G with respect to H if, for every g in $G\backslash H$, there

https://doi.org/10.1017/S0017089500002329 Published online by Cambridge University Press

exist exactly λ pairs s_1, s_2 in S with $g = s_1 s_2^{-1}$ and exactly λ pairs s_3, s_4 in S with $g = s_3^{-1} s_4$. If $|G| = mn$, $|H| = n$ and $|S| = k$, then we say that S has parameters (m, n, k, λ). Thus a λ-difference set is a special case of a relative λ-difference set with $H = 1$, i.e. one with parameters $(m, 1, k, \lambda)$ (see [1] or [5]). If $\lambda = 1$, then we shall call S a *relative difference set* of G with respect to H. We now establish two lemmas which are simple extensions of well-known results on difference sets. (Note that Lemmas 1 and 2 have obvious generalisations to relative λ-difference sets.)

LEMMA 1. *Let G be a finite group with a normal subgroup H and let S be a subset of G. The following three statements are equivalent:*

(a) *S is a relative difference set of G with respect to H.*
(b) *For any g in $G\backslash H$ there exist unique s_1, s_2 in S with $g = s_1 s_2^{-1}$.*
(c) *For any g in $G\backslash H$ there exist unique s_3, s_4 in S with $g = s_3^{-1} s_4$.*

Proof. By definition, (a) implies (b) and (c). Thus we have only to show that (b) and (c) are equivalent.

Assume (b), i.e. that $G\backslash H = \{s_i s_j^{-1} \mid s_i, s_j \in S, s_i \neq s_j\}$, and put $L = \{s_l^{-1} s_m \mid s_l, s_m \in S, s_l \neq s_m\}$. If $s_i^{-1} s_j = s_l^{-1} s_m$ then $s_i s_l^{-1} = s_m s_j^{-1}$, which, since (b) holds, implies that $s_i = s_m$ and $s_l = s_j$. Thus the elements of L are all distinct and $|L| = |G\backslash H|$. In order to prove that $L = G\backslash H$ it is now sufficient to show that $L \cap H = \phi$. If $s_i^{-1} s_j = h \in H$ then $s_j = s_i h$, so that s_i and $s_i h$ are in S. So, by (b), $s_i h s_i^{-1} \in G\backslash H$. But, since H is normal in G, there exists an element h' in H with $s_i h = h' s_i$ and thus $h' = s_i h s_i^{-1}$ is in $G\backslash H$. This contradiction shows that $L \cap H = \phi$ and proves that (b) implies (c).

Similarly (c) implies (b) and the lemma is established.

LEMMA 2. *Let S be a relative difference set for a finite group G with respect to a normal subgroup H and let α be a homomorphism from G on to $K \cong G/H$ with kernel H. Then*

(a) *for any g in G, Sg (gS) is a relative difference set for G with respect to H.*
(b) *$S^{-1} = \{s^{-1} \mid s \text{ in } S\}$ is a relative difference set for G with respect to H.*
(c) *S^α is a λ-difference set of K with $\lambda = |H|$.*

Proof. (a) If g_1 is any element of $G\backslash H$, then there exist unique s_1, s_2 in S with $g_1 = s_1 s_2^{-1}$. Thus there exist unique $s_1 g, s_2 g$ in Sg with $g_1 = (s_1 g)(s_2 g)^{-1}$ and so, by Lemma 1, Sg is a relative difference set for G with respect to H. Similarly gS is a relative difference set.

(b) If g_2 is any element of $G\backslash H$ then there exist unique s_3, s_4 in S with $g_2 = s_3^{-1} s_4$. Thus there exist unique $s_1 = s_3^{-1}$, $s_2 = s_4^{-1}$ in S^{-1} such that $g_2 = s_1 s_2^{-1}$ and, by Lemma 1, S^{-1} is a relative difference set for G with respect to H.

(c) For any $k \neq 1$ in K, $k = (Hg)^\alpha$ for some g in $G\backslash H$. Thus, since k has exactly $|H|$ preimages in $G\backslash H$, there are exactly $|H|$ pairs s_1, s_2 in S such that $(s_1 s_2^{-1})^\alpha = k$. Hence there are exactly $|H|$ pairs s_1^α, s_2^α in S^α such that $k = s_1^\alpha (s_2^\alpha)^{-1}$, i.e. S^α is a $|H|$-difference set of K [4, p. 122].

Finally we state a well-known result about λ-difference sets (see, for example, [1, p. 3]).

LEMMA 3. *If D is a $(v, 1, k, \lambda)$ difference set for a finite group G then the complement of D in G is a $(v, 1, v-k, v-2k+\lambda)$ difference set for G.*

3. Planes with quasiregular groups of type (e). Let G be a quasiregular collineation group of type (e) of a finite projective plane P of order q^2. Then, from [3], one point and line orbit form a Baer subplane P_0 and G acts faithfully on the remaining points and lines. If H is the subgroup fixing P_0 pointwise then, since H is an orbit stabiliser, H is a normal subgroup of G.

We now show that if X and l are any point and line of $P\backslash P_0$ then $S = \{g \in G \mid Xg \text{ is on } l\}$ is a relative difference set of G with respect to H. This gives us a geometric definition for a relative difference set of quasiregular collineation group of type (e). We call X and l the *base elements* of S.

LEMMA 4. *Let G be a quasiregular collineation group of type (e) acting on a finite projective plane P of order q^2. Let P_0 be the Baer subplane formed by the non-faithful point and line orbits and let H be the subgroup fixing P_0 pointwise. If X and l are any point and line of $P\backslash P_0$ then $S = \{g$ in $G \mid Xg$ is on $l\}$ is a relative difference set of G with respect to H, having parameters $(q^2+q+1, q^2-q, q^2, 1)$.*

Proof. Since G is regular on the orbit of X, the points X and Xg are distinct. As X is not in P_0, there is a unique line x of P_0 such that X is on x (see [6, p. 82]). This line x is also the only line through X which is not in the orbit of l. Since g is not in H, $xg \neq x$ and consequently Xg is not on x. Thus the line joining X to Xg is la for some a in $G\backslash H$. But now Xa^{-1} and Xga^{-1} are both on l so that $a^{-1} = s_2$ and $ga^{-1} = s_1$ are in S; solving gives $g = s_1 s_2^{-1}$. Conversely, if $g = s_1' s_2'^{-1}$, where s_1', s_2' are in S, then $gs_2' = s_1'$ and so $Xgs_2' = Xs_1'$ is on l. Thus Xg is on $ls_2'^{-1}$ and clearly, since s_2' is in S, X is also on $ls_2'^{-1}$. Hence $ls_2'^{-1}$ is the line joining X and Xg. But this means that $ls_2'^{-1} = la$ and so, by the regularity of G on the orbit of l, $a = s_2'^{-1}$. It is now easy to see that $s_1 = s_1'$ and $s_2 = s_2'$ so that s_1 and s_2 are unique.

Similarly, by considering the lines l and lg, we find there is a unique pair s_3, s_4 in S with $g = s_3^{-1} s_4$. This shows that S is a relative difference set of G with respect to H and simple counting now gives its parameters.

4. The converse of Lemma 4.

THEOREM 2. *Let G be a finite group of order q^4-q with a relative difference set S with respect to a normal subgroup H of order q^2-q. Then there is a unique (up to isomorphism) projective plane P admitting G as a quasiregular collineation group of type (e) with relative difference set S.*

Proof. Let K be a group isomorphic to G/H, let α be a homomorphism from G on to K with kernel H and let t be any element of $K\backslash S^\alpha$. Put $D = K\backslash t(S^\alpha)^{-1}$. By Lemma 2(c), S^α is a (q^2-q)-difference set of K. Thus $t(S^\alpha)^{-1}$ is a (q^2-q)-difference set of K. Clearly $|K| = q^2+q+1$ and, since $|S| \cdot (|S|-1) = |G|-|H|$, $|S| = q^2$. Hence, by Lemma 3, D is a $(q^2+q+1-2q^2+q^2-q)$-difference set for K; i.e. D is a difference set for K.

https://doi.org/10.1017/S0017089500002329 Published online by Cambridge University Press

We now use the elements of G and K to construct P.

For each g in G and k in K let (g) and (k) be points of P. For any k in K let the line $[k]$ be the point set $Dk \cup \{g \text{ in } G \mid g^\alpha = k\}$ and for any g in G define the line $[g]$ to be the point set $Sg \cup \{tg^\alpha\}$. Clearly P has q^4+q^2+1 points and lines and each line of P contains exactly q^2+1 points. Thus in order to show that P is a projective plane it is sufficient to show that any two distinct points are on a unique common line [6, p. 86]. There are three cases to consider; (i) (k_1) and (k_2), (ii) (g_1) and (g_2), (iii) (g_1) and (k_1).

Case (i). Since D is a difference set for K there is a unique line $[k]$ with $(k_1) \in [k]$ and $(k_2) \in [k]$. Furthermore, since the only point (k') on the line $[g]$ is (tg^α), there is no line (g) containing both (k_1) and (k_2). Thus $[k]$ is the unique line of P containing (k_1) and (k_2).

Case (ii). If $g_1^\alpha = g_2^\alpha = k$, then (g_1) and (g_2) are both on $[k]$ and there is no other line $[k]$ containing either of these points. Suppose that there is also a line $[g]$ containing them. Then $g_1 \in Sg$ and $g_2 \in Sg$. But, by Lemma 2, Sg is a relative difference set for G with respect to H which implies that $g_1 g_2^{-1} \in G \backslash H$. However, $g_1^\alpha = g_2^\alpha$ implies that $g_1 \in Hg_2$; i.e. $g_1 g_2^{-1} \in H$. This contradiction shows that there is no such line $[g]$ and that $[k]$ is the unique line of P containing (g_1) and (g_2).

If $g_1^\alpha \neq g_2^\alpha$ then, clearly, there is no line $[k]$ containing (g_1) and (g_2). The points (g_1) and (g_2) are on $[g]$ if and only if $g_1 g^{-1} \in S$ and $g_2 g^{-1} \in S$. Since $g_1^\alpha \neq g_2^\alpha$, $g_1 g_2^{-1} \notin H$ and there exist unique s_1, s_2 in S with $g_1 g_2^{-1} = s_1 s_2^{-1}$. Thus (g_1) and (g_2) are on $[s_2^{-1} g_2]$ and this is the only line of P containing both points.

Case (iii). If $g_1^\alpha = k_1$, then clearly, since $1 \in D$, both points are on $[k_1]$ and on no other line $[k]$. Suppose $(g_1) \in [g]$ and $(k_1) \in [g]$ then $g_1 \in Sg$ and $k_1 = tg^\alpha \notin (Sg)^\alpha$. This contradicts $g_1^\alpha = k_1$ and shows that $[k_1]$ is the unique line of P containing (g_1) and (k_1).

If $g_1^\alpha = k_2 \neq k_1$, then there exists a line $[k]$ containing (g_1) and (k_1) if and only if $k_1 \in Dk_2$. Similarly there exists a line $[g]$ containing both points if and only if $k_1 = t(s^\alpha)^{-1} k_2$ for some s in S, i.e. if and only if $k_1 \in t(S^\alpha)^{-1} k_2$. But, by the choice of D, $K = D \cup t(S^\alpha)^{-1}$ and $D \cap t(S^\alpha)^{-1} = \phi$. Thus $K = Dk_2 \cup t(S^\alpha)^{-1} k_2$ and either $k_1 \in Dk_2$ or $k_1 \in t(S^\alpha)^{-1} k_2$, which means there is a unique line of P containing (g_1) and (k_1).

Thus we have shown that P is a finite projective plane of order q^2.

If $g_1 \in G$, then the mapping θ_{g_1} given by $(g)^{\theta_{g_1}} = (gg_1)$ and $(k)^{\theta_{g_1}} = (kg_1^\alpha)$ is a collineation of G and it is easily seen that the group of all such θ_g is isomorphic to G and is a quasiregular collineation group of type (e). If we choose $X = (1)$ and $l = [1]$, then the relative difference set for the collineation group with these base elements is

$$\{\theta_g \mid (1)^{\theta_g} \in [1]\} = \{\theta_g \mid (g) \in [1]\} = \{\theta_g \mid g \in S\}.$$

Now suppose that P_1 and P_2 are two planes admitting G as a quasiregular collineation group of type (e) with relative difference set S. Let X_i, l_i $(i = 1, 2)$ be the base elements of G acting on P_i and let P_i' be the Baer subplane of P_i consisting of the non-faithful orbits of G.

If θ is the mapping given by $(X_1 g)\theta = X_2 g$ and $(l_1 g)\theta = l_2 g$ for all $g \in G$ then θ is a one-to-one mapping from the points and lines of $P_1 \backslash P_1'$ on to the points and lines of $P_2 \backslash P_2'$. But $X_1 g$ is on $l_1 h$ if and only if $gh^{-1} \in S$ which is also the condition for $X_2 g$ to be on $l_2 h$. Thus

θ is an isomorphism between the incidence structures consisting of the points and lines of $P_1 \backslash P_1'$ and $P_2 \backslash P_2'$. Since $P_i \backslash P_i'$ uniquely determines P_i, the theorem is proved.

It would be very interesting to find examples of planes with groups of type (e), as there are only two known families of planes (desarguesian and Hughes planes) for which the full collineation group fixes no point or line. The simplest groups to consider are the cyclic or, slightly more generally, the abelian ones. (The cyclic case is considered in [4].) If any relative difference sets exist then these results show how to construct them. Namely, choose a difference set for K, take its complement and then consider subsets of G which consist of one element from each preimage of this complement under all homomorphisms from G on to K with kernel H.

As a simple illustration, we consider the case $q = 2$ where, of course, we know an example exists. Here we write the groups additively, take $G = Z_{14}$, $K = Z_7$ and consider the natural homomorphism. In this case the preimage of any $k \in K$ is $\{k, k+7\}$. Thus we must find a_1, a_2, a_3, a_4 such that the twelve differences formed from $\{2+a_1 7, 4+a_2 7, 5+a_3 7, 6+a_4 7\}$ (where $a_i = 0$ or 1, $i = 1, 2, 3, 4$) take all possible values modulo 14 except 0 or 7. Straightforward checking of all possibilities give $\{2, 4, 12, 13\}$ and $\{5, 6, 9, 11\}$ as the only solutions. In view of the results in [4] it seems likely that $q = 2$ is the only value for which such planes exist.

REFERENCES

1. L. Baumert, *Cyclic difference sets*, Lecture Notes in Mathematics 182 (Springer-Verlag, 1971).

2. H. P. Dembowski, *Finite geometries*, Ergebnisse der Mathematik (Springer-Verlag, 1968).

3. H. P. Dembowski and F. C. Piper, Quasiregular collineation groups of finite projective planes, *Math. Z.* **99** (1967), 53–75.

4. M. J. Ganley and E. Spence, Relative difference sets and quasiregular collineation groups; to appear.

5. M. Hall, Jr., *Combinatorial theory* (Blaisdell, 1967).

6. D. R. Hughes and F. C. Piper, *Projective planes*, Graduate Texts in Mathematics 6 (Springer-Verlag, 1973).

DEPARTMENT OF MATHEMATICS
WESTFIELD COLLEGE
UNIVERSITY OF LONDON
HAMPSTEAD
LONDON NW5 3ST