Symmetric Designs With $\lambda = 2$ Admitting PSL(2,q) fixing a block

J.D. Fanning

Department of Mathematics
University College
Galway, Republic of Ireland.

Abstract. It is shown that a symmetric design with $\lambda = 2$ can admit PSL(2,q) for q odd and q greater than 3 as an automorphism group fixing a block and acting in its usual permutation representation on the points of the block only if q is congruent to 5 (mod 8). A consequence for more general automorphism groups is also described.

The question of symmetric designs admitting PSL(2,q) as an automorphism group fixing a block and acting (not necessarily faithfully) in its usual permutation representation on the points of the block was considered in [6]. All examples were determined except for $\lambda = 2$ and q odd, when the representation is necessarily faithful. Our purpose is to show that no new examples can occur here if q is congruent to 1, 3 or 7 modulo 8, apart from the known example with $q = 3$. Section 1 contains a statement of this result (Theorem 1) and some lemmas. Section 2 contains a proof of Theorem 1. A consequence of this result is described in Section 3.

We do not give detailed background either for the designs or for the groups. This can be found in [6] and the references therein.

We will sometimes use the term biplane for a symmetric design with $\lambda = 2$.

1. Statement of Theorem 1 and some lemmas.

Our main result is the following theorem.

Theorem 1. *Let $\mathcal{D}$ denote a symmetric design with $\lambda = 2$ and G an automorphism group of $\mathcal{D}$ isomorphic to PSL(2,q) for q odd and $q > 3$ such that G fixes a block B and acts on the points of B in the usual permutation representation of G of degree $q + 1$. Then q is congruent to 5 (mod 8) and $q - 1$ is square.*

The proof of Theorem 1 will require the following series of lemmas. The hypotheses of Theorem 1 are assumed in the following discussion and for Lemmal and Lemma 2.

Throughout F will denote the field of q elements and the points of B will be identified with the elements of F and the special symbol ∞. The elements of G can be written as linear fractional transformations $\frac{ex+f}{gx+h}$ for $eh - fg$ a non-zero square in F. The elements of G which fix ∞ may alternatively be written $ex + f$.

The involutions in G will usually be written as $\frac{ex+f}{x-e}$ and this representation of any involution is unique; conversely, every involution has this form if $q \equiv 3(\mod 4)$.

G will be transitive on the blocks different from B and on the points off B of which there are, respectively, $q(q+1)/2$ and $q(q-1)/2$. If C is any block different from B and p is any point off B then G_C has order $q-1$ and G_p has order $q+1$. As described in [6] we may use the classification of the subgroups of PSL(2,q) due to Dickson [5] to show that G_p may be assumed to be dihedral, and a similar argument shows that G_C may be assumed to be dihedral also; the exceptional occurences of subgroups of PSL(2,q) of order $q-1$ which are not dihedral are ruled out here because for each the non-existence of $\mathcal{D}$ is shown by the Bruck-Ryser-Chowla conditions ([4] pp 61, 63). Thus we may state:-

Lemma 1. (*a*) *If C is a block different from B then G_C is dihedral of order $q-1$.*

(*b*) *If p is a point not on B then G_p is dihedral of order $q+1$.*

The Hussain chains for biplanes of this type, and the group action on them, were partially determined in [6]. From there we may extract the information contained in the following lemma.

Lemma 2. *If q is congruent to 3 (mod 4) and p is a point not on B then the involution h in the centre of G_p fixes no block through p. Any other invovution in G_p fixes exactly two blocks through p which are interchanged by h.*

The following lemma is a special case of Lemma 2.6 of [1].

Lemma 3. *If H is an automorphism group of a biplane which fixes at least two points and has odd order then the fixed points and blocks of H form a subbiplane. In particular, H fixes equally many points on any two fixed blocks.*

We will also require the following two lemmas.

Lemma 4. *If C is a block of a biplane and g is an involutory automorphism which does not fix C then g fixes either 0 or 2 points of C.*

Proof: Clearly the only points of C which g can fix are the two points of $C \cap C^g$. Since g either fixes or interchanges these points, g fixes either 0 or 2 points of C.

Lemma 5. *In a symmetric Hadamard 2-$(4\lambda+3, 2\lambda+1, \lambda)$ design $\mathcal{H}$, for any three distinct blocks X, Y, Z we have $X \cap Y^c \cap Z^c \neq \emptyset$.*

Proof: Let $\mathcal{H}_Z$ denote the residual of $\mathcal{H}$ at Z. Then $\mathcal{H}_Z$ cannot contain a repeated block since it contains less that twice as many blocks as points (see, for example, [7]). It follows that X intersects Y^c in $\mathcal{H}_Z$, that is $X \cap Y^c \cap Z^c \neq \emptyset$.

2. Proof of Theorem 1

Under the hypotheses of Theorem 1 the number of points in $\mathcal{D}$ is $(q+1)q/2+1$. This is even if $q \equiv 5(\bmod 8)$ and so by the theorem of Bruck ([4] page 61) the order of $\mathcal{D}$, that is $q-1$, is square, whence the last condition of the theorem. The rest of the proof consists of showing the impossibility of an example with $q \equiv 1,3,7 \ (\bmod 8)$. We take the three cases separately.

Case 1. $q \equiv 1(\bmod 8)$. This case can be dismissed easily. When $q \equiv 1(\bmod 8)$ G contains the permutations $-x, 1/x$ and $\frac{x+1}{x-1}$. These generate a subgroup K of of order 8 each element of which either fixes or interchanges the pairs $\{\infty, 0\}$ and $\{1, -1\}$. Let C and D be the blocks intersecting B in these pairs and let C and D intersect in points a and b which necessarily lie off B. Then every element of K either fixes or interchanges C and D and so either fixes or interchanges a and b. A subgroup of order 4 (at least) therefore fixes a and b. But G_a has order $q+1$ which is not divisible by 4, a contradiction.

Case 2. $q \equiv 7(\bmod 8)$. Assume $q \equiv 7(\bmod 8)$. If a is a point on B then G_a has order $q(q-1)/2$, which is odd. Therefore any 2-subgroup of G is semi-regular on the points of B.

For a point b off B, G_b has order $q+1$ which is divisible by 8; thus G_b contains a subgroup K of order 8. Suppose first that K fixes a second point c off B. Then K fixes or interchanges the two blocks through b and c and so permutes among themselves the four points in which these blocks intersect B. Since K is semi-regular on B of order 8, this is a contradiction. The same argument shows that K has no orbits of length 2 on the points off B. Thus all orbits of K on the points off B, other that b, have length 4 or 8. We can conclude from this that any subgroup of G_b of order 4 fixes no point off B other than b. By Lemma 2 G_b is dihedral having a unique involution h in its centre which fixes no block through b. If g is any other involution in G_b then g fixes two blocks through b which are interchanged by h. If c is the second point in which these blocks intersect then c is fixed by g and h and so by the subgroup of order 4 which they generate. This contradiction concludes the argument for $q \equiv 7(\bmod 8)$.

Case 3. $q \equiv 3(\bmod 8)$. When q is congruent to 3 or 5 $(\bmod 8)$ the Sylow 2-subgroups of G have order 4, and so arguments like those above are not available. For $q \equiv 3(\bmod 8)$ a straightforward analysis of the possible Hussain chains as determined in [6] immediately leads to conditions which are very unlikely-looking but from which a contradiction cannot easily be deduced. Our approach is to establish a one-to-one correspondence between the points off B and the involutions in G. In fact, for every point a off B, G_a is dihedral of order $q+1$ so that $Z(G_a)$, the centre of G_a, has order 2. It is not difficult to establish that for different points a and b off B the involutions in $Z(G_a)$ and $Z(G_b)$ are different, and simply because there are equally many involutions in G as points off b, the correspondence thus established is one-to-one. So we identify each point a off B with the involution in $Z(G_a)$ and the permutation action of any element of G on these "points" is given by conjugation.

Next we consider the permutation action of G_C on $C\backslash B$ for any block C different from B. By Lemma 1, G_C is dihedral of order $q-1$ and will contain a cyclic subgroup H of order $(q-1)/2$, which is odd. H must fix the two points of $B \cap C$. Each non-identity element of H fixes no other point on B, since the stabilizer in G of three points of B is the identity. By Lemma 3, no non-identity element of H fixes a point of $C\backslash B$. Thus H has two orbits of length $(q-1)/2$ on $C\backslash B$. Then G_C either has two orbits on $C\backslash B$ and induces the usual dihedral permutation on each, or G_C is regular on $C\backslash B$. In the respective cases any involution in G_C fixes 2 or 0 points on C. Since G is transitive on the blocks different from B, the stabilizers of any two such blocks are conjugate in G. Thus if G_C is regular on $C\backslash B$ no involution in G fixes a block different from B and a point on that block. But Lemma 2 shows that involutions in G do fix such point-block pairs. Thus for any C different from B, G_C has two orbits on $C\backslash B$ and each involution in G_C fixes two points on C.

Now let C be the block intersecting B in $\{\infty, 0\}$. We ask which involutions (that is, points under the above correspondence) lie on C. The involution $-1/x$ fixes C and so fixes two points a and b of $C\backslash B$. Let D be the second block through a and b. Then $-1/x$ fixes D also. Thus D intersects B in $\{w, -1/w\}$ for some w in F. The involutions in $Z(G_a)$ and $Z(G_b)$ fix no block through a or b but interchange C and D and so interchange the pairs $\{\infty, 0\}$ and $\{w, -1/w\}$. It follows that they equal $\frac{wx+1}{x-w}$ and $\frac{-w^{-1}x+1}{x+w^{-1}}$ in some order. The condition that these be in PSL(2,q) is that w^2+1 be a non-square in F. The mappings tx, for t a square in F, fix C; conjugating the above involutions by these mappings we get all q involutions corresponding to points on $C\backslash B$. They are

$$\frac{twx+t^2}{x-tw} \qquad \text{for } t \text{ a square in } F \tag{1}$$

and

$$\frac{-tw^{-1}+t^2}{x+tw^{-1}} \qquad \text{for } t \text{ a square in } F \tag{2}$$

Our purpose is to show the existence of an involution in G not fixing C which commutes with exactly one of the involutions in (1) and (2) above. It will then fix exactly one point on C in contradiction to Lemma 4.

Let h_1 be any involtuion of Type (1) above and let g be the arbitrary involution $\frac{ex+f}{x+c}$. Then

$$h_1 g = \frac{(ewt+t^2)x + fwt - et^2}{(e-wt)x + f + ewt}$$

and

$$gh_1 = \frac{(ewt + f)x + et^2 - fwt}{(wt - e)x + t^2 + ewt}$$

These are equal if $e = wt$ and $f = t^2$ when g is of the form (1); otherwise they are equal if and only if

$$t^2 + 2ewt + f = 0 \qquad (3)$$

Similarly, if h_2 is of the form (2) then

$$h_2 g = \frac{(t^2 - etw^{-1})x - et^2 - ftw^{-1}}{(e + tw^{-1})x + f - etw^{-1}}$$

and

$$gh_2 = \frac{(f - etw^{-1})x + et^2 + ftw^{-1}}{-(e + tw^{-1})x + t^2 - etw^{-1}}$$

These are equal if $e = -t/w$ and $f = t^2$ when g is of the form (2) and otherwise if and only if

$$t^2 - 2ew^{-1}t + f = 0 \qquad (4)$$

Thus if g is not of the form (1) or (2) then the fixed points of g on C correspond to those roots of (3) and (4) which are squares in F. We will assume now that f is a non-square in F. Then g is not of the form (1) or (2) and each of the quadratics (3) and (4) either has no roots in F or has distinct roots exactly one of which is square.

Assume $e = 1$. Then (3) and (4) have the respective discriminants $4(w^2 - f)$ and $4(w^{-2} - f)$. Let T denote the set of non-zero squares in F. The sets $T + u$ for u in F form a Hadamard design ([4] page 97). By Lemma 5 the sets $T + w^{-2}, T^c$ and $(T + w^2)^c$ have non-empty intersection. Let f be in this intersection. Then f is non-zero since it is the sum of two squares in F and -1 is a non-square in F; also f is non-square. Since f is in $T + w^{-2}$, $f = s + w^{-2}$ for some square s, so $w^{-2} - f = -s$ is a non-square, that is the discriminant of (4) is non-square. Also, since f is not in $T + w^2$, f is not of the form $s + w^2$ for s a non-zero square in F, nor is f equal to w^2; thus $f - w^2$ is a non-square in F and $w^2 - f$ is a square, that is the discriminant of (3) is a square in F. Thus this g fixes exactly one point on C, and g does not fix C since it maps ∞ to 1. This is a contradiction to Lemma 4 and concludes the proof for $q \equiv 3(\bmod 8)$.

3. A Consequence

In this section we state a theorem for any biplane admitting an automorphism group G fixing a block B and acting transitively on the remaining blocks. The theorem was proved in [2] under the hypothesis that G is a block stabilizer in a doubly-transitive automorphism group. An examination of the proof of Theorem 2 of [2] will show that the doubly transitive group is invoked there only to reject the possibility of a group in which the block stabilizer contains PSL(2,q) with $q \equiv 3 \pmod 4$. As we have shown such a group to be impossible, the proof of Theorem 2 of [2] now shows the following:

Theorem 2. *Let G be an automorphism group of a symmetric design with $\lambda = 2$ fixing a block B and transitive on the remaining blocks. Let k be the number of points in a block and let k be greater than 4. Then*

(a) *G is doubly transitive on the points of B of order divisible by $k(k-1)(k-2)/4$;*

(b) *if $k \not\equiv 2 \pmod 4$ then G is triply transitive on the points of B.*

In view of the classification of the finite simple groups, the groups satisfying the conclusions of Theorem 2 are known (see [3]). Since any doubly-transitive subgroup of G will be transitive on the blocks different from B and so must also satisfy the conclusions of the theorem, it is trivial to show that any new example will contain PSL(2,q) and so any example of a group satisfying the hypotheses of Theorem 2 which is not already known will belong to the outstanding case of Theorem 1 with $q \equiv 5 \pmod 8$.

References

1. M. Aschbacher, *On collineation groups of synetric block designs*, J. Combin. Theory **11** (1971), 272–281.
2. P.J. Cameron, *Biplanes*, Math Z, **131** (1973), 85–101.
3. P.J. Cameron, *Finite permutation groups and finite simple groups*, Bull. London Math. Soc. **13** (1981), 1–22.
4. P. Dembowski, "Finite geometries", Springer–Verlag, Berlin-Heidelberg-New York, 1968.
5. L.E. Dickson, *Linear groups with an exposition of the Galois field theory*, Reprint, Dover Publications, New York, 1958.
6. G. Kelly, *Symmetric 2-designs admitting PSL(2,q) fixing a block*, Ars Corbinatoria **12** (1981), 269–293.
7. H.B. Mann, *A note on balanced incomplete block designs*, Ann. Math Statist **40** (1969), 679–680.