Half-regular symmetric designs

Alan Rahilly

Cheryl E. Praeger
Department of Mathematics
University of Western Australia, Nedlands, WA 6009, Australia

Anne Penfold Street
Centre for Combinatorics, Department of Mathematics
The University of Queensland, QLD 4072, Australia

Darryn E. Bryant
Centre for Combinatorics, Department of Mathematics
The University of Queensland, QLD 4072, Australia

Abstract.

This paper is part of an investigation of symmetric $2-(v,k,\lambda)$ designs such that the point set and the block set can each be halved to give a tactical decomposition. We assume that there is a group of automorphisms of the design of order $v/2$ which has two orbits of points, each of length $v/2$. Only the identity fixes a point, and we say that such a group acts half-regularly on the design. The design itself is also said to be half-regular.

The existence of a group acting regularly on the set of points of a design is equivalent to the existence of a difference set in the group. We present a variant of this construction, which gives a family of four subsets of the group, leading to difference sets for the half-regular design. We show that several of the known biplanes may be constructed in this way, and we believe that this method provides a reasonable framework for conducting a computer search for new half-regular symmetric designs, possibly including further biplanes.

1. Introduction.

This paper is part of an investigation of symmetric $2-(v,k,\lambda)$ designs such that the point set and the block set can each be halved to give a tactical decomposition. Earlier papers on this topic were [**9**] and [**10**]. The present paper is based on an incomplete manuscript left by Alan Rahilly, which the other authors felt contained ideas too interesting to be overlooked.

Australasian Journal of Combinatorics 8(1993), pp.1-26

A *symmetric* $2-(v,k,\lambda)$ *design*, or more precisely a $2-(v,k,\lambda)$ *design* $\mathcal{D} = (\mathcal{P},\mathcal{B})$, consists of a set $\mathcal{P}$ of v points, and a set $\mathcal{B}$ of k-element subsets of $\mathcal{P}$, called blocks, such that each pair of points lies in λ blocks, and $|\mathcal{B}| = v$. Thus the designs which we will consider have no repeated blocks; that is, they are all *simple designs.* This paper is part of an investigation of symmetric designs such that the point set $\mathcal{P} = \mathcal{P}_1 \cup \mathcal{P}_2$ and block set $\mathcal{B} = \mathcal{B}_1 \cup \mathcal{B}_2$ can be partitioned in such a way that $(\mathcal{P}_i, \mathcal{B}_i)$ is a tactical decomposition, for $i = 1,2$; see [4,p7 and p17] for the definition of a tactical decomposition, and [9,10] for papers reporting on other aspects of this investigation. Here we assume that there is a group G of automorphisms of $\mathcal{D}$ which has order $v/2$ and has two orbits $\mathcal{P}_1$ and $\mathcal{P}_2$ on points (each necessarily of length $v/2$). In such a group of automorphisms only the identity element fixes a point of $\mathcal{P}$; that is, such a group acts *semi-regularly* on $\mathcal{P}$ and we call such a group a *half-regular group* acting on $\mathcal{D}$. A symmetric design $\mathcal{D}$ admitting a half-regular group of automorphisms will be called a *half-regular symmetric design.*

A group G is said to act *regularly* on $\mathcal{P}$ if G is semi-regular and transitive on $\mathcal{P}$. Symmetric designs $\mathcal{D} = (\mathcal{P},\mathcal{B})$ which admit a group G of automorphisms acting regularly on the point set $\mathcal{P}$ have received much attention. For a symmetric design $\mathcal{D} = (\mathcal{P},\mathcal{B})$ admitting a regular group G, and for $p \in \mathcal{P}$, and $b \in \mathcal{B}$, the subset Δ of G of elements g such that $p^g \in b$ is a λ-difference set for G with parameters v,k,λ, and $\mathcal{D}$ can be reconstructed from Δ (see Section 7 or [6, pp60-62]). Thus the existence of a symmetric design admitting a group G acting regularly on points is equivalent to the existence of a λ-difference set in G. This paper presents a variant of the construction of symmetric designs from difference sets, giving instead a construction of symmetric designs from a family of four subsets of a group G with properties similar to those of a difference set for G. Such a family will be called a *Rahilly family of pre-difference sets* and the precise definition and properties will be discussed in Section 2. Each Rahilly family has associated with it several other Rahilly families leading to the original design or to its dual; these are discussed in Section 3. Restrictions on the parameters of the designs are found in Section 4. Equivalence and multipliers of half-regular symmetric designs are dealt with in Sections 5 and 6.

If $\mathcal{D} = \mathcal{D}(\Delta)$ is a symmetric design with half-regular group G and Rahilly family Δ of pre-difference sets, then we can find necessary and sufficient conditions, in terms of Δ, for G to have a regular extension. Properties of regular extensions and of multipliers of associated difference sets are discussed in Sections 7 and 8.

We show that several of the known biplanes may be constructed by these methods, and we believe that the construction of Rahilly families of pre-difference sets provides a reasonable framework for conducting a computer search for new half-regular symmetric designs, possibly including further biplanes. Earlier constructions of difference sets for each of the $(16,6,2)$ biplanes were given by Kibler [7]; they will be derived here in a uniform manner.

2. Half-regular designs and Rahilly families of pre-difference sets.

Let $\mathcal{D} = (\mathcal{P}, \mathcal{B})$ be a symmetric $2-(v,k,\lambda)$ design with a half-regular group G of automorphisms. By definition, automorphisms g of $\mathcal{D}$ are permutations of $\mathcal{P}$ which map blocks to blocks; that is, $b^g \in \mathcal{B}$ for each $b \in \mathcal{B}$. Hence, the automorphism group $\mathrm{Aut}\,\mathcal{D}$ of $\mathcal{D}$ is a subgroup of the symmetric group $\mathrm{Sym}\,\mathcal{P}$ of all permutations of $\mathcal{P}$. Thus $G \leq \mathrm{Aut}\,\mathcal{D} \leq \mathrm{Sym}\,\mathcal{P}$. By definition, G has two orbits in $\mathcal{P}$, say $\mathcal{P}_1$ and $\mathcal{P}_2$, where $|G| = |\mathcal{P}_1| = |\mathcal{P}_2| = v/2$, and G acts semi-regularly on $\mathcal{P}$. By [6, p46], an automorphism of a symmetric design fixes equally many points as blocks, and hence a subgroup of automorphisms of $\mathcal{D}$ acts semi-regularly on $\mathcal{P}$ if and only if it is semi-regular on $\mathcal{B}$. It follows that our group G is semi-regular on $\mathcal{B}$ with two block orbits, $\mathcal{B}_1$ and $\mathcal{B}_2$, each of length $v/2$.

We shall construct a family of "pre-difference sets" in G essentially by identifying each of $\mathcal{P}_1, \mathcal{P}_2, \mathcal{B}_1$ and $\mathcal{B}_2$ with G in a standard way. First we review the way in which regular groups are identified with the sets on which they act.

Suppose that a group H of permutations of a set X is regular on X; that is, H is transitive on X and only the identity of H fixes a point of X. Choose a point $x \in X$. We shall refer to x as the *base point* in this identification. Define the map $\varphi : H \to X$ by $(h)\varphi := x^h$ for each $h \in H$, where x^h denotes the image of x under h. Since H is regular, φ is a bijection. Moreover, it is straightforward to check that, for all $h, h' \in H$, $(h)\varphi^{h'} = (hh')\varphi$; that is, the action of H on X is equivalent to its action on itself by right multiplication. Thus, by identifying X with H in this manner, we may assume that H acts by right multiplication. (Note that in making this identification we may make a free choice of the base point, but once this choice is made the identification is completely determined.)

Since the group G is regular on each of $\mathcal{P}_1, \mathcal{P}_2, \mathcal{B}_1$ and $\mathcal{B}_2$, we can identify G with each of these sets. In order to avoid confusing elements of G with their corresponding points in $\mathcal{P}_1$, $\mathcal{P}_2$, etc, we shall identify $\mathcal{P} = \mathcal{P}_1 \cup \mathcal{P}_2$ with $G \times \{1,2\} = \{\ (g,i) \mid g \in G,\ i \in \{1,2\}\ \}$. We choose base points $p_1 \in \mathcal{P}_1$ and $p_2 \in \mathcal{P}_2$, and define the mapping φ analogously to the way we defined it on the group H in the previous paragraph. Thus

$$(g,i)\varphi = p_i^g$$

for all (g,i). Then φ is a bijection, and if we in fact identify $\mathcal{P}$ with $G \times \{1,2\}$ in this way, then an element $g' \in G$ maps a point (g,i) to (gg',i). We could identify $\mathcal{B}$ with $G \times \{1,2\}$ in a similar way, but it will be more convenient to refrain from a formal identification in this case (as we are regarding blocks as subsets of $\mathcal{P}$).

Choose *base blocks* $b_1 \in \mathcal{B}_1$ and $b_2 \in \mathcal{B}_2$, and for $i,j \in \{1,2\}$, define a subset Δ_{ij} of G by

$$\mathcal{P}_i \cap b_j = \Delta_{ij} \times \{i\}.$$

Set

$$k_{ij} = |\Delta_{ij}| = |\mathcal{P}_i \cap b_j|.$$

Then $k_{1j} + k_{2j} = |b_j| = k$ for $j = 1,2$. We shall show that the subsets Δ_{ij} provide a variant of a difference set for G, which is defined as follows.

Definition 2.1. Let v, k, λ be positive integers with $k < v$ and v even, let G be a finite group of order $v/2$, and, for $i, j \in \{1,2\}$, let Δ_{ij} be a subset of G of size k_{ij}, where $k_{1j} + k_{2j} = k$. Then the collection $\Delta := \{\Delta_{ij} \mid i, j \in \{1,2\}\ \}$ is called a *Rahilly family of pre-difference sets* for G with parameters v, k, λ if the following conditions hold.

(a) For each non-identity element g of G, and for $i = 1,2$, there is a non-negative integer $\lambda_i(g) \leq \lambda$ such that g can be represented exactly $\lambda_i(g)$ times as cd^{-1} with $c, d \in \Delta_{ii}$, and exactly $\lambda - \lambda_i(g)$ times as ef^{-1}, with $e, f \in \Delta_{ij}$ where $\{i,j\} = \{1,2\}$

(b) For each element g of G, and for $\{i,j\} = \{1,2\}$, there is a non-negative integer $\lambda_{ij}(g) \leq \lambda$, such that g can be represented exactly $\lambda_{ij}(g)$ times as cd^{-1} with $c \in \Delta_{ii}$, $d \in \Delta_{ji}$, and exactly $\lambda - \lambda_{ij}(g)$ times as ef^{-1}, with $e \in \Delta_{ij}$ and $f \in \Delta_{jj}$.

There are not many obvious restrictions on the integers $\lambda_i(g)$ and $\lambda_{ij}(g)$, but it follows from the definition that

$$\lambda_{ij}(g^{-1}) = \lambda - \lambda_{ji}(g) \tag{1}$$

for all $g \in G$. Our first task is to show that the sets Δ_{ij} defined earlier form a Rahilly family of pre-difference sets for G.

Proposition 2.2 *Let $\mathcal{D} = (\mathcal{P}, \mathcal{B})$ be a symmetric $2-(v,k,\lambda)$ design with a half-regular group G of automorphisms. Suppose that $\mathcal{P} = \mathcal{P}_1 \cup \mathcal{P}_2$ is identified with $G \times \{1,2\}$ such that $p_1 = (1,1)$ and $p_2 = (1,2)$, and that $\mathcal{B}_j$, b_j, and the Δ_{ij} and k_{ij} are defined as above. Then $\Delta := \{\Delta_{ij} \mid i,j \in \{1,2\}\ \}$ is a Rahilly family of pre-difference sets for G with parameters v, k, λ.*

Proof. Certainly $k_{1j} + k_{2j} = k$ for $j = 1,2$. Let $g \in G$ and $l, m \in \{1,2\}$. Then the points $(1,l), (g,m)$ are distinct provided that if $l = m$ then $g \neq 1$. We shall assume that these two points are distinct. Then, by the definition of $\mathcal{D}$, they lie together in precisely λ blocks, say $\sigma := \sigma_{lm}(g)$ blocks $b_1^{x_1}, \ldots, b_1^{x_\sigma} \in \mathcal{B}_1$ and $\lambda - \sigma$ blocks $b_2^{y_1}, \ldots, b_2^{y_{\lambda-\sigma}} \in \mathcal{B}_2$. The points $(1,l)$ and (g,m) lie in this collection of blocks if and only if $\{(x_n^{-1}, l) | 1 \leq n \leq \sigma\} \cup \{(gx_n^{-1}, m) | 1 \leq n \leq \sigma\} \subseteq b_1$ and $\{(y_n^{-1}, l) | 1 \leq n \leq \lambda - \sigma\} \cup \{(gy_n^{-1}, m) | 1 \leq n \leq \lambda - \sigma\} \subseteq b_2$. This in turn is true if and only if $x_n^{-1} \in \Delta_{l1}$ and $gx_n^{-1} \in \Delta_{m1}$ for $1 \leq n \leq \sigma$, and $y_n^{-1} \in \Delta_{l2}$ and $gy_n^{-1} \in \Delta_{m2}$ for $1 \leq n \leq \lambda - \sigma$. Part (a) of the definition follows on taking $l = m$ and setting $\lambda_1(g) := \sigma_{11}(g)$ and $\lambda_2(g) := \lambda - \sigma_{22}(g)$. Part (b) follows on taking $l \neq m$ and setting $\lambda_{12}(g) := \sigma_{21}(g)$ and $\lambda_{21}(g) := \lambda - \sigma_{12}(g)$.

Next we observe that the symmetric design $\mathcal{D}$ can be reconstructed from the Δ_{ij}.

Proposition 2.3 *Let v, k, λ be positive integers with $k < v$ and v even, let G be a finite group of order $v/2$, and, for $i, j \in \{1,2\}$, let Δ_{ij} be a subset of G of size*

k_{ij} such that $k_{1j} + k_{2j} = k$ for $j = 1, 2$, and such that $\Delta := \{\Delta_{ij} \mid i, j \in \{1, 2\}\ \}$ is a Rahilly family of pre-difference sets for G.

Set $\mathcal{P} := G \times \{1, 2\}$, $b_1 := \{(g, 1) | g \in \Delta_{11}\} \cup \{(g, 2) | g \in \Delta_{21}\}$ and $b_2 := \{(g, 1) | g \in \Delta_{12}\} \cup \{(g, 2) | g \in \Delta_{22}\}$. Then $\mathcal{B} := \{b_1^g \mid g \in G\} \cup \{b_2^g \mid g \in G\}$ is the block set of a symmetric $2-(v, k, \lambda)$ design $\mathcal{D}(\Delta) = (\mathcal{P}, \mathcal{B})$. Moreover,

$$(x, i)^g := (xg, i)$$

for all $g \in G$ and $(x, i) \in \mathcal{P}$, defines an action of G as a half-regular group of automorphisms of $\mathcal{D}(\Delta)$.

Proof. Since $k_{1j} + k_{2j} = k$ for $j = 1, 2$, each block has size k; there are v points and v blocks, and the properties of a Rahilly family of pre-difference sets imply that each pair of distinct points lies in precisely λ blocks. Thus $\mathcal{D}(\Delta)$ is a symmetric $2-(v, k, \lambda)$ design. Finally it is easily checked that $(x, i)^g := (xg, i)$ defines an action of G as a group of automorphisms of $\mathcal{D}(\Delta)$ which is half-regular on $\mathcal{D}(\Delta)$.

It is clear from the proof that, if Δ is the Rahilly family obtained from a symmetric design $\mathcal{D}$ as in Proposition 2.2, then the design $\mathcal{D}(\Delta)$ constructed in Proposition 2.3 is equal to $\mathcal{D}$.

We illustrate the construction, described in Proposition 2.3, of a half-regular symmetric biplane, namely, the one denoted by $\mathcal{B}_7$ in Assmus and Salwach [1].

Corollary 2.4 *Let Δ be the Rahilly family corresponding to the symmetric design $\mathcal{D}$, as defined in Proposition 2.2. Then the symmetric design $\mathcal{D}(\Delta)$ defined in Proposition 2.3 is equal to $\mathcal{D}$.*

Example 2.5 The biplane $\mathcal{B}_7$ can be developed as follows. Let $v = 16, k = 6, \lambda = 2$ and let $G = (\{0, 1, 2, 3\} \times \{0, 2\}, +_{(\text{mod } 4)})$; so $G \cong Z_4 \times Z_2$. For brevity, we will denote elements $(i, j) \in G$ by ij. Let $\Delta_{11} = \Delta_{22} = \{00, 12, 22, 32\}$, let $\Delta_{12} = \{10, 12\}$ and let $\Delta_{21} = \{00, 02\}$. It is straightforward to verify that $\Delta := \{\Delta_{ij} \mid i, j \in \{1, 2\}\ \}$ is a Rahilly family for G. Then according to Proposition 2.3 we obtain a half-regular symmetric design $\mathcal{D}(\Delta) = (\mathcal{P}, \mathcal{B})$, with base blocks b_1 and b_2, where

$$\begin{aligned}
\mathcal{P} = \{&(00,1),(02,1),(10,1),(12,1),(20,1),(22,1),(30,1),(32,1),\\
&(00,2),(02,2),(10,2),(12,2),(20,2),(22,2),(30,2),(32,2)\},\\
b_1 = \{&(00,1),(12,1),(22,1),(32,1),(00,2),(02,2)\},\\
b_2 = \{&(10,1),(12,1),(00,2),(12,2),(22,2),(32,2)\}
\end{aligned}$$

and

$$\begin{array}{ll}\mathcal{B} = \{ & \{(00,1),(12,1),(22,1),(32,1),(00,2),(02,2)\},\\ & \{(10,1),(22,1),(32,1),(02,1),(10,2),(12,2)\},\\ & \{(20,1),(32,1),(02,1),(12,1),(20,2),(22,2)\},\\ & \{(30,1),(02,1),(12,1),(22,1),(30,2),(32,2)\},\\ & \{(02,1),(10,1),(20,1),(30,1),(02,2),(00,2)\},\\ & \{(12,1),(20,1),(30,1),(00,1),(12,2),(10,2)\},\\ & \{(22,1),(30,1),(00,1),(10,1),(22,2),(20,2)\},\\ & \{(32,1),(00,1),(10,1),(20,1),(32,2),(30,2)\},\\ & \{(10,1),(12,1),(00,2),(12,2),(22,2),(32,2)\},\\ & \{(20,1),(22,1),(10,2),(22,2),(32,2),(02,2)\},\\ & \{(30,1),(32,1),(20,2),(32,2),(02,2),(12,2)\},\\ & \{(00,1),(02,1),(30,2),(02,2),(12,2),(22,2)\},\\ & \{(12,1),(10,1),(02,2),(10,2),(20,2),(30,2)\},\\ & \{(22,1),(20,1),(12,2),(20,2),(30,2),(00,2)\},\\ & \{(32,1),(30,1),(22,2),(30,2),(00,2),(10,2)\},\\ & \{(02,1),(00,1),(32,2),(00,2),(10,2),(20,2)\} \quad \}.\end{array}$$

This construction of a half-regular symmetric design from a Rahilly family of pre-difference sets is a special case of the method of symmetrically repeated differences introduced by Bose in [2, p366]. We note that we do not require the group G to be abelian. In the next section we introduce several Rahilly families of pre-difference sets associated with a given Rahilly family Δ.

3. Rahilly families related to Δ.

Let $\mathcal{D} = (\mathcal{P}, \mathcal{B})$ be a half-regular symmetric $2-(v,k,\lambda)$ design with a half-regular group G of automorphisms. Suppose that $\mathcal{P}$ is identified with $G \times \{1,2\}$, that base points $p_i = (1,i)$ and base blocks $b_i \in \mathcal{B}_i$ are chosen as before, and that $\Delta = \{\Delta_{ij} \mid i,j \in \{1,2\}\ \}$ is the associated Rahilly family of pre-difference sets as defined in Section 2. In this section we obtain some restrictions on the $k_{ij} := |\Delta_{ij}|$ which depend only on the combinatorial properties of a symmetric design. Then we introduce several Rahilly families related to Δ.

Proposition 3.1

(a) *For all $i,j \in \{1,2\}$, each point of $\mathcal{P}_i$ lies in precisely k_{ij} blocks in $\mathcal{B}_j$.*
(b) *$k_{11} = k_{22}$, and $k_{12} = k_{21}$.*

Proof. Part (a) follows on counting the number of pairs (p, b), where $p \in \mathcal{P}_i$, $b \in \mathcal{B}_j$, and $p \in b$.

Since $\mathcal{D}$ is symmetric, each point lies in exactly k blocks, and so, by part (a), we have $k_{i1} + k_{i2} = k$, for $i = 1, 2$. We also have $k_{1j} + k_{2j} = k$, for $j = 1, 2$, and so $k_{11} = k_{22}, k_{12} = k_{21}$, proving part (b).

In the proof of part (b) we used one simple aspect of duality of a symmetric design, namely that the number of points in a block is equal to the number of blocks on a point. A simple counting argument also shows that each pair of distinct blocks intersects in precisely λ points. Thus if $\mathcal{D} = (\mathcal{P}, \mathcal{B})$ is a symmetric $2-(v, k, \lambda)$ design, so also is $\mathcal{D}^* = (\mathcal{P}^*, \mathcal{B}^*)$, where $\mathcal{P}^* := \mathcal{B}$ and $\mathcal{B}^* := \{p^* \mid p \in \mathcal{P}\}$ where we define $p^* := \{b \in \mathcal{B} \mid p \in b\}$. The design $\mathcal{D}^*$ is called the *dual design* of $\mathcal{D}$.

There is a close connection between Rahilly families for $\mathcal{D}^*$ and those for $\mathcal{D}$. For a subset X of a group G, X^{-1} denotes the set $\{x^{-1} \mid x \in X\}$ of inverses of the elements of X.

Proposition 3.2 *The collection $\Delta^* := \{\Delta^*_{ij} := \Delta^{-1}_{ji} \mid i, j \in \{1, 2\}\ \}$ is a Rahilly family of pre-difference sets for G with parameters v, k, λ, and the corresponding design $\mathcal{D}(\Delta^*)$ is isomorphic to the dual design $\mathcal{D}^*$ of $\mathcal{D}$.*

Proof. Let $g \in G$ and $l, m \in \{1, 2\}$. Then the blocks b_l, b^g_m are distinct provided that, if $l = m$, then $g \neq 1$. Assume that these blocks are distinct. Then they intersect in precisely λ points, say $\sigma := \sigma_{lm}(g)$ points $(x_1, 1), \dots, (x_\sigma, 1) \in \mathcal{P}_1$ and $\lambda - \sigma$ points $(y_1, 2), \dots, (y_{\lambda-\sigma}, 2) \in \mathcal{P}_2$. The blocks b_l, b^g_m contain this collection of points if and only if b_l contains $\{(x_1, 1), \dots, (x_\sigma, 1)\} \cup \{(y_1, 2), \dots, (y_{\lambda-\sigma}, 2)\}$, and b_m contains $\{(x_1 g^{-1}, 1), \dots, (x_\sigma g^{-1}, 1)\} \cup \{(y_1 g^{-1}, 2), \dots, (y_{\lambda-\sigma} g^{-1}, 2)\}$. This in turn is true if and only if $x_i \in \Delta_{1l}$ and $x_i g^{-1} \in \Delta_{1m}$ for $i = 1, \dots, \sigma$, and $y_i \in \Delta_{2l}$ and $y_i g^{-1} \in \Delta_{2m}$ for $i = 1, \dots, \lambda - \sigma$. Since $g = (x_i g^{-1})^{-1} x_i^{-1} = (y_i g^{-1})^{-1} y_i^{-1}$ for all i, we obtain the Rahilly family Δ^* as in the proof of Proposition 2.2.

It is clear from the previous paragraph that Δ^* is the Rahilly family corresponding to the dual design $\mathcal{D}^*$ of $\mathcal{D}$. Thus by Corollary 2.4 it follows that $\mathcal{D}^*$ is isomorphic to $\mathcal{D}(\Delta^*)$.

Remark 3.3 The Rahilly family Δ^* is called the *dual Rahilly family* of Δ. The construction of $\mathcal{D}(\Delta^*)$ given by Proposition 2.3 is such that the base blocks are $b^*_1 = \{(g, 1) \mid g \in \Delta^*_{11}\} \cup \{(g, 2) \mid g \in \Delta^*_{21}\} = \{(g^{-1}, 1) \mid g \in \Delta_{11}\} \cup \{(g^{-1}, 2) \mid g \in \Delta_{12}\}$, and $b^*_2 = \{(g^{-1}, 1) \mid g \in \Delta_{21}\} \cup \{(g^{-1}, 2) \mid g \in \Delta_{22}\}$. The standard identification of points of $\mathcal{D}^*$ with $G \times \{1, 2\}$ described in Section 2 is such that the point $b^g_i \in \mathcal{B} = \mathcal{P}^*$ is identified with (g, i). It follows that the map κ which takes each point $b^g_i \in \mathcal{B} = \mathcal{P}^*$ of $\mathcal{D}^*$ to the point (g, i) of $\mathcal{D}(\Delta^*)$,

$$\kappa : b^g_i \mapsto (g, i),$$

is an isomorphism from the dual $\mathcal{D}^*$ of $\mathcal{D}$ to the design $\mathcal{D}(\Delta^*)$.

Remark 3.4 The Rahilly family Δ for $\mathcal{D}$ can be modified in several trivial ways to produce other Rahilly families with the same parameters. Interchanging the roles of the base blocks b_1 and b_2 gives the Rahilly family Δ' where

$$\Delta'_{i1} := \Delta_{i2} \quad \text{and} \quad \Delta'_{i2} := \Delta_{i1} \quad \text{and} \quad i \in \{1,2\}.$$

Interchanging the roles of the base points p_1 and p_2 gives the Rahilly family Δ'' defined by

$$\Delta''_{1j} := \Delta_{2j} \quad \text{and} \quad \Delta''_{2j} := \Delta_{1j} \quad \text{and} \quad j \in \{1,2\}.$$

Finally interchanging the roles of both the base points p_1 and p_2 and the base blocks b_1 and b_2 gives the Rahilly family $\bar{\Delta}$ defined by

$$\bar{\Delta}_{11} := \Delta_{22},\ \bar{\Delta}_{22} := \Delta_{11},\ \bar{\Delta}_{12} := \Delta_{21},\ \bar{\Delta}_{21} := \Delta_{12}.$$

This last family $\bar{\Delta}$ is called the *Rahilly family conjugate to* Δ, and the corresponding design $\mathcal{D}(\bar{\Delta})$ is called the *conjugate symmetric design* to $\mathcal{D}$. The relation between Δ and $\bar{\Delta}$ will be important in our investigations of multipliers and regular extensions in Sections 6 and 7. Clearly all the designs $\mathcal{D}(\Delta')$, $\mathcal{D}(\Delta'')$, $\mathcal{D}(\bar{\Delta})$ are isomorphic to $\mathcal{D}$ as we are merely relabeling points and blocks in some way. A natural isomorphism ρ from $\mathcal{D}$ to its conjugate design $\mathcal{D}(\bar{\Delta})$ is given by

$$\rho : (g,1) \mapsto (g,2), \quad (g,2) \mapsto (g,1),$$

for all $g \in G$.

To see that this so, note that the base blocks for $\mathcal{D}(\bar{\Delta})$ using our notation are $\bar{b}_j := (\bar{\Delta}_{1j} \times \{1\}) \cup (\bar{\Delta}_{2j} \times \{2\})$, for $j = 1,2$. It is straightforward to check that ρ is a permutation of $\mathcal{P}$ which maps the blocks b_1^g and b_2^g of $\mathcal{D}$ to $\bar{b}_2^g$ and $\bar{b}_1^g$ respectively, for all $g \in G$. Hence ρ is an isomorphism from $\mathcal{D}$ to $\mathcal{D}(\bar{\Delta})$.

4. Parameters of the designs.

The point set $\mathcal{P} = \mathcal{P}_1 \cup \mathcal{P}_2$ and block set $\mathcal{B} = \mathcal{B}_1 \cup \mathcal{B}_2$ have been partitioned in such a way that $(\mathcal{P}_i, \mathcal{B}_i)$ is a tactical decomposition, for $i = 1,2$. Let $C = [c_{ij}]$ and $D = [d_{ij}]$ be the incidence matrices of this tactical decomposition (see [4, p7 and p17]), let I_2 be the 2×2 identity matrix and let

$$P = \operatorname{diag}(|\mathcal{P}_i|) = \frac{v}{2} I_2 = \operatorname{diag}(|\mathcal{B}_i|) = B.$$

Then $BC^T = DP$ [4, p17], implying that $C^T = D$.

We know that $c_{1j} + c_{2j} = d_{1j} + d_{2j} = k$, for $j = 1,2$ and hence that $c_{ii} = d_{ii} = k'$, say, for $i = 1,2$, and that $c_{ij} = d_{ij} = k - k' = k''$, say, for $i \neq j, \{i,j\} = \{1,2\}$. (From Proposition 3.1, this means that $k_{11} = k_{22} = k'$ and $k_{12} = k_{21} = k''$.) If J_2 is the 2×2 matrix with each entry equal to 1, then [4, p60] $CD = (k - \lambda)I_2 + \lambda P J_2$. This means that

$$(k')^2 + (k'')^2 = k - \lambda + \frac{\lambda v}{2} \qquad (2)$$

and

$$2k'k'' = \frac{\lambda v}{2}. \tag{3}$$

By (2) and (3), $(k' - k'')^2 = k - \lambda$. Without loss of generality, we assume $k' \geq k''$, and let $s = k' - k'' \geq 0$. Then $k = s^2 + \lambda$ and, since $k' + k'' = k$, we have

$$2k' = s^2 + s + \lambda \quad \text{and} \quad 2k'' = s^2 - s + \lambda. \tag{4}$$

By (3) and (4), we find

$$v = (s^2 + s + \lambda)(s^2 - s + \lambda)/\lambda. \tag{5}$$

Since $k(k-1) = \lambda(v-1)$, and v is even, we see that λ must be even. Also λ must divide $s^2(s^2-1)/2$, since $v/2$ is an integer.

Summarising, we obtain

Lemma 4.1 *A half-regular group must have order $(s^2+s+\lambda)(s^2-s+\lambda)/2\lambda$, for some positive integers s, λ such that $s \geq 2$, λ is even, and λ divides $s^2(s^2-1)/2$. Further $k' = (s^2+s+\lambda)/2$ and $k'' = (s^2-s+\lambda)/2$ are non-negative integers. (Note that we have assumed $k' \geq k''$, and that in fact $k' > k''$.)*

This leads us to

Lemma 4.2 *None of $\Delta_{11}, \Delta_{12}, \Delta_{21}, \Delta_{22}$ is a perfect difference set in G.*

Proof We prove this statement for Δ_{11}; the other cases are similar. If Δ_{11} is a $(v/2, k', \lambda')$ difference set in G, then

$$\lambda'(\frac{v}{2} - 1) = k'(k'-1). \tag{6}$$

From equations (4), (5) and (6), we find that[1]

$$\lambda' = \frac{\lambda}{2} + s - w,$$

$$\text{where} \qquad \begin{aligned} w &= s(s^2-1)(s^2+\lambda)/d, \\ d &= (s^2+\lambda-1)(s^2+\lambda) - \lambda. \end{aligned}$$

It was shown [9, p71] that d cannot be a divisor of $s(s^2-1)(s^2+\lambda)$ and hence that λ' is not an integer. We outline the proof.

[1] Alan Rahilly did this calculation by hand; it was checked by the other authors using Maple V.2. [3]

Suppose that w (and hence λ') is an integer; that is, suppose that

$$d \mid s(s^2-1)(s^2+\lambda). \tag{a}$$

We note a result quoted, for example, in Knuth [8, p336]: if $u \mid v_1 v_2 \ldots v_n$, then

$$u \mid \gcd(u,v_1)\gcd(u,v_2)\ldots\gcd(u,v_n). \tag{b}$$

Since

$$d = (s^2+\lambda-1)(s^2+\lambda)-\lambda, \tag{c}$$

we know that for any integer h, if $h \mid d$ and $h \mid (s^2+\lambda)$, then $h \mid \lambda$ and thus $h \mid s^2$. Hence, provided $h > 1$, we have $h \nmid (s^2-1)$. This means that $h_1 \mid d$, $h_1 \mid (s^2+\lambda)$, $h_2 \mid d$, $h_2 \mid (s^2-1)$ together imply that

$$\gcd(h_1,h_2) = 1. \tag{d}$$

Now let $\alpha = \gcd(d, s^2+\lambda)$, and let $\alpha\alpha' = d$. Then $\alpha\alpha' \mid s(s^2-1)(s^2+\lambda)$, and by (b), $\alpha' \mid s(s^2-1)$. Let $\beta = \gcd(\alpha', s^2-1) = \gcd(d, s^2-1)$. Since $\beta \mid (s^2-1)$, we have $\sqrt{\beta} < s$. By rearranging (c), we obtain

$$d = \lambda^2 + 2(s^2-1)\lambda = s^2(s^2-1), \tag{e}$$

and from (e) we see that $\beta \mid (s^2-1)$ and $\beta \mid d$ together imply that $\beta \mid \lambda^2$.

Let $\gamma = \gcd(\beta,\lambda)$ and let $\gamma\delta = \beta$. We check that $\delta \leq \gamma$. Suppose that $p_1,\ldots,p_r$ are distinct primes such that $\lambda = \prod_{i=1}^{r} p_i^{e_i}$, for some integers $e_1,\ldots,e_r > 0$. Since $\beta \mid \lambda^2$,we must have $\beta = \prod_{i=1}^{r} p_i^{f_i}$ where $0 \leq f_i \leq 2e_i$. Then $\gamma = \prod_{i=1}^{r} p_i^{m_i}$ where $m_i = \min(e_i,f_i)$ and $\delta = \prod_{i=1}^{r} p_i^{(f_i-m_i)}$. Since all these exponents are non-negative, $f_i \leq \min(2e_i, 2f_i) = 2\min(e_i,f_i)$. This implies that $f_i - \min(e_i,f_i) \leq \min(e_i,f_i)$ and hence that $\delta \leq \gamma$. But now $\delta \leq \sqrt{\beta} < s$.

Since $\gcd(\alpha,\gamma) = 1$ by equation (d), and since $\alpha \mid \lambda$ and $\gamma \mid \lambda$, we have $\alpha\gamma \leq \lambda$. Hence $\alpha\beta = \alpha\gamma\delta \leq \lambda\delta < \lambda s$. But $\alpha\beta = \gcd(d,(s^2-1)(s^2+\lambda))$ and hence, by equation (a), $d \mid \alpha\beta s$. That means $d \leq \alpha\beta s < \lambda s^2$, which contradicts equation (e) since $s \geq 2$, $\lambda \geq 2$. This is the contradiction we need: $d \nmid s(s^2-1)(s^2+\lambda)$.

5. Equivalence of half-regular symmetric designs.

Let Δ and $\tilde{\Delta}$ be Rahilly families of pre-difference sets in a group G with the same parameters v, k, λ. In this section we investigate certain relationships which the corresponding symmetric designs $\mathcal{D}(\Delta) = (\mathcal{P},\mathcal{B})$ and $\mathcal{D}(\tilde{\Delta}) = (\tilde{\mathcal{P}},\tilde{\mathcal{B}})$ may have. Each of these designs has point set $\mathcal{P} = \tilde{\mathcal{P}} = G \times \{1,2\}$. An element $\pi \in \operatorname{Sym}\mathcal{P}$

which fixes $G \times \{i\}$ setwise for $i = 1, 2$, will induce two bijections from G to itself, namely π_1 and π_2 where

$$(g^{\pi_i}, i) := (g, i)^\pi$$

for all $g \in G$, and π will induce an isomorphism from $\mathcal{D}(\Delta)$ to some other symmetric design with point set $\mathcal{P}$. We first obtain necessary and sufficient conditions for π to induce an automorphism of G and an isomorphism from $\mathcal{D}(\Delta)$ to $\mathcal{D}(\tilde{\Delta})$. The matter of inducing an automorphism of G requires a little explanation. Since automorphisms necessarily preserve the identity element of G, and since the elements $a_i := 1^{\pi_i}$ will not usually be the identity, we shall say that π *induces an automorphism* of G if, for some $\varphi \in \operatorname{Aut} G$,

$$g^{\pi_i} = a_i \cdot g^\varphi$$

for all $g \in G$, and $i = 1, 2$. Let $\mathcal{B}_1$ and $\mathcal{B}_2$ be the block orbits for G in $\mathcal{B}$, and $\tilde{\mathcal{B}}_1$ and $\tilde{\mathcal{B}}_2$ be the block orbits for G in $\tilde{\mathcal{B}}$.

Theorem 5.1 *Let Δ and $\tilde{\Delta}$ be two Rahilly families of pre-difference sets in a group G with parameters v, k, λ. Suppose that the permutation π of $G \times \{1,2\}$ fixes $G \times \{i\}$ setwise, for $i = 1, 2$. Then π induces an automorphism of G, and an isomorphism from $\mathcal{D}(\Delta)$ to $\mathcal{D}(\tilde{\Delta})$ which maps $\mathcal{B}_1$ to $\tilde{\mathcal{B}}_1$ and $\mathcal{B}_2$ to $\tilde{\mathcal{B}}_2$, if and only if, for some $\varphi \in Aut G$ and some elements $a_1, a_2, c_1, c_2 \in G$,*

$$g^{\pi_i} = a_i \cdot g^\varphi \quad \text{and} \quad a_i \cdot \Delta_{ij}^\varphi = \tilde{\Delta}_{ij} \cdot c_j \tag{7}$$

for all $g \in G$, and $i, j \in \{1, 2\}$.

Proof. Suppose first that π induces an automorphism φ of G and an isomorphism from $\mathcal{D}(\Delta)$ to $\mathcal{D}(\tilde{\Delta})$ which maps $\mathcal{B}_1$ to $\tilde{\mathcal{B}}_1$ and $\mathcal{B}_2$ to $\tilde{\mathcal{B}}_2$. Thus we have $(g, i)^\pi = (a_i \cdot g^\varphi, i)$ for all $g \in G, i = 1, 2$. Since π maps $\mathcal{B}_j = \{b_j^g | g \in G\}$ onto $\tilde{\mathcal{B}}_j = \{\tilde{b}_j^g | g \in G\}$, where the b_j and $\tilde{b}_j$ are the base blocks, π induces further permutations of G, namely σ_j where $(b_j^g)^\pi = \tilde{b}_j^{g^{\sigma_j}}$, for $j = 1, 2$. In particular $b_j^\pi = \tilde{b}_j^{c_j}$ where $c_j := 1^{\sigma_j}$. However $b_j = (\Delta_{1j} \times \{1\}) \cup (\Delta_{2j} \times \{2\})$ and $\tilde{b}_j = (\tilde{\Delta}_{1j} \times \{1\}) \cup (\tilde{\Delta}_{2j} \times \{2\})$, and from our knowledge of how π acts on points we therefore have

$$b_j^\pi = (a_1 \cdot \Delta_{1j}^\varphi \times \{1\}) \cup (a_2 \cdot \Delta_{2j}^\varphi \times \{2\}) = (\tilde{\Delta}_{1j} \cdot c_j \times \{1\}) \cup (\tilde{\Delta}_{2j} \cdot c_j \times \{2\}).$$

Hence, $a_i \cdot \Delta_{ij}^\varphi = \tilde{\Delta}_{ij} \cdot c_j$ for $i, j \in \{1, 2\}$.

Conversely, suppose that (7) holds. Then, by definition, π induces the automorphism φ of G. Further, each block in $\mathcal{B}_j$ is of the form $b_j^g = (\Delta_{1j} \cdot g \times \{1\}) \cup (\Delta_{2j} \cdot g \times \{2\})$, and its image under π is $(a_1 \cdot \Delta_{1j}^\varphi \cdot g^\varphi \times \{1\}) \cup (a_2 \cdot \Delta_{2j}^\varphi \cdot g^\varphi \times \{2\})$ which equals $(\tilde{\Delta}_{1j} \cdot c_j \cdot g^\varphi \times \{1\}) \cup (\tilde{\Delta}_{2j} \cdot c_j \cdot g^\varphi \times \{2\})$, and this is just $\tilde{b}_j^{c_j \cdot g^\varphi}$ which lies in $\tilde{\mathcal{B}}_j$. Thus π maps $\mathcal{B}$ onto $\tilde{\mathcal{B}}$ and hence is an isomorphism from $\mathcal{D}(\Delta)$ to $\mathcal{D}(\tilde{\Delta})$ which maps $\mathcal{B}_1$ to $\tilde{\mathcal{B}}_1$ and $\mathcal{B}_2$ to $\tilde{\mathcal{B}}_2$.

An isomorphism π with the properties of Theorem 5.1 is strongly linked to the structure of the corresponding Rahilly families of the designs. Designs which are isomorphic via such a map π will be called equivalent, and we show by example that two half-regular symmetric designs may be isomorphic, but not equivalent.

Definition 5.2 Let Δ and $\tilde{\Delta}$ be two Rahilly families of pre-difference sets in a group G with the same parameters v, k, λ. Then Δ and $\tilde{\Delta}$ are said to be *equivalent* if and only if, for some $\varphi \in \operatorname{Aut} G$, and some elements $a_1, a_2, c_1, c_2 \in G$,

$$a_i \cdot \Delta_{ij}^{\varphi} = \tilde{\Delta}_{ij} \cdot c_j \tag{8}$$

for all $g \in G$, and $i, j \in \{1,2\}$. If this is the case, then the corresponding symmetric designs, $\mathcal{D}(\Delta)$ and $\mathcal{D}(\tilde{\Delta})$, are also said to be *equivalent*. By Theorem 5.1, equivalent designs are isomorphic via the map π given by

$$\pi : (g, i) \mapsto (a_i \cdot g^{\varphi}, i) \tag{9}$$

for all $g \in G, i = 1, 2$. An isomorphism π from $\mathcal{D}(D)$ to $\mathcal{D}(\tilde{D})$ which satisfies (9), for some $a_1, a_2 \in G$ and some $\varphi \in \operatorname{Aut} G$ such that (8) holds for some $c_1, c_2 \in G$, is called an *equivalence*. The automorphism φ is called the *associated automorphism* of π, and the 4-tuple (a_1, a_2, c_1, c_2) is called the 4-tuple of *associated translations* of π.

Remark 5.3 Note that, if a permutation π of $G \times \{1,2\}$ satisfies the conclusions of Theorem 5.1, then π is determined completely by its associated translations $a_1, a_2, c_1, c_2 \in G$ and associated automorphism $\varphi \in \operatorname{Aut} G$. Thus $\pi \in \operatorname{Sym}(G \times \{1,2\})$ is an equivalence from $\mathcal{D}$ to $\tilde{\mathcal{D}}$ if and only if, for some $\varphi \in \operatorname{Aut} G$, and some $a_1, a_2 \in G$, π is given by

$$(g, i)^{\pi} = (a_i \cdot g^{\varphi}, i)$$

for all $g \in G,\ i = 1, 2$, such that for some $c_1, c_2 \in G$,

$$\tilde{\Delta}_{ij} = a_i \cdot \Delta_{ij}^{\varphi} \cdot c_j^{-1}$$

for all $i, j \in \{1,2\}$.

It follows that two Rahilly families Δ and $\tilde{\Delta}$ of pre-difference sets for G are inequivalent if and only if there are no elements $a_1, a_2, c_1, c_2 \in G$ and no $\varphi \in \operatorname{Aut} G$ such that

$$\tilde{\Delta}_{ij} = a_i \cdot \Delta_{ij}^{\varphi} \cdot c_j^{-1}$$

for $i, j \in \{1,2\}$.

Example 5.4 The biplane $\mathcal{B}_6$ of order four (see [1]) can be represented as a half-regular design for at least two inequivalent Rahilly families of pre-difference sets in the group $G = Z_4 \times Z_2$:

(1) $\Delta_{11} = \Delta_{22} = \{00, 12, 22, 32\}, \Delta_{12} = \Delta_{21} = \{00, 02\}$;
(2) $\Delta_{11} = \Delta_{22} = \{00, 10, 02, 32\}, \Delta_{12} = \{10, 30\}, \Delta_{21} = \{00, 20\}$;

Just as some, but not all, isomorphisms of half-regular symmetric designs are equivalences, so also some, but not all, automorphisms of such designs will be equivalences. The following corollary of Theorem 5.1 gives some information about this.

Corollary 5.5 *Let Δ be a Rahilly family of pre-difference sets in a group G, let $\mathcal{D} := \mathcal{D}(\Delta)$ be the corresponding half-regular design, and let $\pi \in Aut\mathcal{D}$ be an equivalence with associated translations $a_1, a_2, c_1, c_2 \in G$ and associated automorphism $\varphi \in AutG$. Then:*

- (a) *for $i = 1, 2$, π fixes the base point p_i if and only if $a_i = 1$;*
- (b) *the equivalence π lies in the normaliser $N_{\mathrm{Aut}\,\mathcal{D}}(G)$ of G in $Aut\mathcal{D}$, and π fixes each of $\mathcal{P}_1, \mathcal{P}_2, \mathcal{B}_1, \mathcal{B}_2$ setwise;*
- (c) *the set of all equivalences in $Aut\mathcal{D}$ forms a subgroup of $N_{\mathrm{Aut}\,\mathcal{D}}(G)$ which fixes $\mathcal{P}_1$ and $\mathcal{P}_2$ setwise.*

In part (b) we show, in fact, that regarding π as an element of $N_{\mathrm{Aut}\,\mathcal{D}}(G)$, the automorphism of G induced by π by conjugation is equal to the associated automorphism φ of π. In Section 6 we obtain a more precise characterisation of the subgroup of equivalences in $\mathrm{Aut}\,\mathcal{D}$.

Proof. Part (a) is an immediate consequence of Theorem 5.1. To prove part (b), let $h \in G < \mathrm{Aut}\,\mathcal{D}$. Then, for all $(g, i) \in \mathcal{P}$,

$$(g,i)^{\pi^{-1}h\pi} = ((a_i^{-1} \cdot g)^{\varphi^{-1}}, i)^{h\pi} = ((a_i^{-1} \cdot g)^{\varphi^{-1}} \cdot h, i)^{\pi} = (g \cdot h^{\varphi}, i)$$

whence $\pi^{-1}h\pi = h^{\varphi}$, so $\pi \in N_{\mathrm{Aut}\,\mathcal{D}}(G)$. Finally, π fixes $\mathcal{P}_1$ and $\mathcal{P}_2$ setwise, and hence $< G, \pi >$ has two orbits in $\mathcal{P}$ and hence two orbits in $\mathcal{B}$. Thus π also fixes $\mathcal{B}_1$ and $\mathcal{B}_2$ setwise. So (b) is proved. Part (c) is now an immediate corollary of Theorem 5.1 and part (b).

6. Multipliers of half-regular symmetric designs.

Let G be a half-regular group of automorphisms of a symmetric design $\mathcal{D}$, the points of which are identified with $G \times \{1, 2\}$, and let Δ be the corresponding Rahilly family of pre-difference sets. Thus $G \leq \mathrm{Aut}\,\mathcal{D} \leq \mathrm{Sym}\,\mathcal{P}$. Let

$$N := N_{\mathrm{Aut}\,\mathcal{D}}(G)$$

be the normaliser of G in $\mathrm{Aut}\,\mathcal{D}$. Then G is a normal subgroup of N, and so N either interchanges the point orbits $\mathcal{P}_1$ and $\mathcal{P}_2$ of G or fixes $\mathcal{P}_1$ and $\mathcal{P}_2$ setwise.

Similarly, N interchanges $\mathcal{B}_1$ and $\mathcal{B}_2$ or fixes them setwise, and N has equally many orbits on points as on blocks. Let $E(G)$ denote the subgroup of N which fixes $\mathcal{P}_1$ and $\mathcal{P}_2$ setwise. Then $[N : E(G)]$ is 1 or 2, and $E(G)$ fixes $\mathcal{B}_1$ and $\mathcal{B}_2$ setwise also.

For $p \in \mathcal{P}$ let N_p denote the stabiliser of p in N; similarly for $b \in \mathcal{B}$ let N_b denote the stabiliser of b. Note that $N_p = E(G)_p$ and $N_b = E(G)_b$ for all p and b whether or not $N = E(G)$. Then, since G and $E(G)$ have the same orbits on points and blocks, $E(G) = G.E(G)_p = G.E(G)_b$ for any p and b. For any two points or blocks in the same $E(G)$-orbit, the corresponding stabilisers are conjugate in $E(G)$. However it may or may not be the case that $E(G)_{p_1}$ and $E(G)_{p_2}$ are conjugate in $E(G)$, or that $E(G)_{b_1}$ and $E(G)_{b_2}$ are conjugate in $E(G)$.

Now it is straightforward to show that, for $(g,i) \in \mathcal{P}$ and $x \in E(G)$ fixing the base point $p_i = (1,i)$,

$$x : (g,i) \mapsto (x^{-1} \cdot g \cdot x, i).$$

Thus, the action of $E(G)_{p_i}$ on $\mathcal{P}_i$ is equivalent to its action by conjugation on G, for $i = 1,2$. This means in particular that, under the natural homomorphism $\psi : N \rightarrow \operatorname{Aut} G$ defined by $(x)\psi : g \mapsto x^{-1} \cdot g \cdot x$, for $x \in N$, $g \in G$, we have two subgroups of $\operatorname{Aut} G$, namely $(E(G)_{p_1})\psi$ and $(E(G)_{p_2})\psi$, corresponding to point stabilisers in $E(G)$. Although $E(G)_{p_1} \cong E(G)/G \cong E(G)_{p_2}$, it is not clear that the images of $E(G)_{p_1}$ and $E(G)_{p_2}$ under ψ will be the same. In fact, for each $x \in E(G)_{p_2}$, there is a unique $g \in G$ such that $g \cdot x \in E(G)_{p_1}$. So the subgroups of $\operatorname{Aut} G$ induced by $E(G)_{p_1}$ and $E(G)_{p_2}$ will be 'equal modulo inner automorphisms' of G. In the special case when G is abelian the two subgroups of $\operatorname{Aut} G$ coincide, but this will not be the case in general. Thus we take some care in defining the multipliers of G.

Definition 6.1 For $i = 1,2$, a *(point) multiplier of type i* of G is an element of $E(G)_{p_i}$. The subgroup $E(G)_{p_i}$ is called the *(point) multiplier group of type i* of G. In particular, a multiplier $x \in E(G)_{p_i}$ is said to be *simple* if it fixes at least one point in each of $\mathcal{P}_1$ and $\mathcal{P}_2$, and x is said to be *numerical* if, for some positive integer m, $(x)\psi : (g,i) \mapsto (g^m, i)$ for all $g \in G$; the smallest such m is called the *degree* of x.

Remark 6.2 Block multipliers of types 1 and 2 could be defined similarly. By [6, p46], each automorphism of $\mathcal{D}$ fixes equally many points and blocks. Thus each point multiplier of type i is a block multiplier of type 1 or 2. However the multiplier group of type i need not be equal to the subgroup of block multipliers of a given type.

Our use of the term 'multiplier' is consistent with the definition of a multiplier of a difference set, see [6, Section 2.4] or the next section. We note that, in the case where G is abelian, the set of automorphisms of G induced by the multiplier groups of types 1 and 2 are the same, and so we need not make the distinction on type.

Further, if $E(G)_{p_1}$ is conjugate to $E(G)_{p_2}$ by an element of N, then applying ψ we see that the subgroups of $\operatorname{Aut} G$ induced by these two groups are conjugate in Aut G. Since conjugation by elements of N, considered as elements of Aut G by applying ψ, preserves the set of simple multipliers and the set of numerical multipliers, we shall again in this case not bother to distinguish multipliers by type. This is the case in particular when N is transitive on $\mathcal{P}$.

Thus it is of interest to have some criterion for deciding when N is transitive on $\mathcal{P}$. It turns out that there is such a criterion in terms of equivalences from $\mathcal{D}$ to its conjugate design, and this will be obtained in Theorem 6.5 below. First we explore the relationship between equivalences in Aut $\mathcal{D}$ and multipliers of G.

Lemma 6.3 *Let $\mathcal{D} = (\mathcal{P}, \mathcal{B})$ be a symmetric design with half-regular group G of automorphisms and corresponding Rahilly family Δ of pre-difference sets, and let $i = 1$ or 2. If $\pi \in Aut\mathcal{D}$ is a (point) multiplier of type i, then π is an equivalence with associated automorphism equal to the automorphism φ induced by π by conjugation on G, and with associated translations (a_1, a_2, c_1, c_2) such that $a_i = 1$.*

Proof. Suppose that $\pi \in E(G)_{p_i}$; that is, π is a multiplier of type i, and suppose that π induces $\varphi \in$ Aut G by conjugation. We showed above that, for all g, $(g,i)^\pi = (g^\varphi, i)$. Let $j \in \{1,2\}$, $j \neq i$. Since $E(G) = G.E(G)_{p_j}$, there is a unique $\pi' \in E(G)_{p_j}$, and a unique $h \in G$ such that $\pi = h \cdot \pi'$. Now the automorphism φ' of G induced by π' is the composition of the inner automorphism of G induced by h^{-1} and φ. Hence, for all $g \in G$, $(g,j)^{\pi'} = ((h \cdot g \cdot h^{-1})^\varphi, j)$. It follows that $(g,j)^\pi = (g,j)^{h\pi'} = (g \cdot h, j)^{\pi'} = (h^\varphi \cdot g^\varphi, j)$, which equals $(a_j \cdot g^\varphi, j)$ on setting $a_j := h^\varphi$. Similarly, for $m = 1,2$, there are unique $x_m \in G$ and $\tau_m \in E(G)_{b_m}$ such that $\pi = x_m \cdot \tau_m$. Since τ_m fixes $\mathcal{P}_1$ and $\mathcal{P}_2$ setwise we have, for $l = 1,2$,

$$\Delta_{lm} = \Delta_{lm}^{\tau_m} = \Delta_{lm}^{x_m^{-1} \cdot \pi} = (\Delta_{lm} \cdot x_m^{-1})^\pi$$

which is equal to $a_l \cdot \Delta_{lm}^\varphi \cdot (x_m^{-1})^\varphi$, and, on setting $c_m = x_m^\varphi$, we see that π is an equivalence as required.

Now we show that the subgroup of equivalences in Aut $\mathcal{D}$ is equal to $E(G)$.

Theorem 6.4 *Let $\mathcal{D} = (\mathcal{P}, \mathcal{B})$ be a symmetric design with half-regular group G of automorphisms and corresponding Rahilly family Δ of pre-difference sets. Then, the subgroup of equivalences in $AutG$ is equal to $E(G)$.*

Proof. By Corollary 5.5(c), the subgroup of equivalences in Aut $\mathcal{D}$ is contained in $E(G)$. By Lemma 6.3, every element of $E(G)_{p_1}$ is an equivalence. For $g \in G$, taking φ to be the inner automorphism of G induced by g, and $a_1 = a_2 = c_1 = c_2 = g$, it follows from Remark 5.3 that g is an equivalence. Thus by Corollary 5.5(c), each element of $E(G) = G.E(G)_{p_1}$ is an equivalence. We therefore deduce that the subgroup of equivalences is equal to $E(G)$.

Putting together the conclusions of Corollary 5.5 and Theorem 6.4, we see that the subgroup of equivalences of Aut $\mathcal{D}$ can be computed within the group G once we know a Rahilly family of pre-difference sets for $\mathcal{D}$. Note in particular that $E(G)$ depends only on G; that is, it is independent of Δ. Now we deduce a criterion for determining whether or not N is transitive on $\mathcal{P}$, that is whether or not $N \neq E(G)$. This criterion will also be easy to verify within the group G. By Remark 3.4, $\mathcal{D}$ is always isomorphic to its conjugate design $\bar{\mathcal{D}}$; it turns out that N is transitive on $\mathcal{P}$ if and only if $\mathcal{D}$ and $\bar{\mathcal{D}}$ are equivalent.

Theorem 6.5 *Let $\mathcal{D} = (\mathcal{P}, \mathcal{B})$ be a symmetric design with half-regular group G of automorphisms and corresponding Rahilly family Δ of pre-difference sets. Then $N := N_{\mathrm{Aut}\,\mathcal{D}}(G)$ is transitive on $\mathcal{P}$ if and only if Δ is equivalent to its conjugate family $\bar{\Delta}$.*

Proof. Let $\bar{\mathcal{D}} := \mathcal{D}(\bar{\Delta})$. Suppose that $N \neq E(G)$ and let $\tau \in N \setminus E(G)$. Then τ interchanges $\mathcal{P}_1$ and $\mathcal{P}_2$ and so induces two permutations τ_1 and τ_2 of G defined by

$$(g^{\tau_1}, 1) := (g, 2)^\tau, \quad \text{and} \quad (g^{\tau_2}, 2) := (g, 1)^\tau$$

for all $g \in G$. Let $\rho \in \mathrm{Sym}\,\mathcal{P}$ be the permutation defined in Remark 3.4, that is

$$\rho : (g, 1) \mapsto (g, 2), \quad (g, 2) \mapsto (g, 1)$$

for all $g \in G$, and set $\pi = \tau \cdot \rho$. Then π is a permutation of $\mathcal{P}$ which fixes $\mathcal{P}_1$ and $\mathcal{P}_2$ setwise, and the two permutations π_1 and π_2 of G defined as in the paragraph preceeding Theorem 5.1 are $\pi_1 = \tau_2$, $\pi_2 = \tau_1$. By Remark 3.4, ρ is an isomorphism from $\mathcal{D}$ to $\bar{\mathcal{D}}$ which maps $\mathcal{B}_1$ to $\bar{\mathcal{B}}_2$ and $\mathcal{B}_2$ to $\bar{\mathcal{B}}_1$, and hence π is an isomorphism from $\mathcal{D}$ to $\bar{\mathcal{D}}$ which maps $\mathcal{B}_1$ to $\bar{\mathcal{B}}_1$ and $\mathcal{B}_2$ to $\bar{\mathcal{B}}_2$. Further, the permutation ρ centralises the subgroup G of $\mathrm{Sym}\,\mathcal{P}$, and hence $\pi \in N_{\mathrm{Sym}\,\mathcal{P}}(G)$ and π and τ, acting by conjugation on G, induce the same automorphism, say φ, of G. Thus, for all $g \in G$, $\pi^{-1} \cdot g \cdot \pi = g^\varphi$. For $j = 1, 2$, let a_j be the image of the identity element $1 \in G$ under π_j. Then

$$(g^{\pi_j}, j) = (g, j)^\pi = (1, j)^{g \cdot \pi} = (1, j)^{\pi \cdot g^\varphi} = (1^{\pi_j}, j)^{g^\varphi} = (a_j, j)^{g^\varphi} = (a_j \cdot g^\varphi, j)$$

whence $g^{\pi_j} = a_j \cdot g^\varphi$ for all $g \in G$. This proves that π induces an automorphism of G in the technical sense defined before Theorem 5.1. It now follows from Theorem 5.1 that there exist $c_1, c_2 \in G$ such that

$$a_i \cdot \Delta_{ij}^\varphi = \bar{\Delta}_{ij} \cdot c_j$$

for $i, j \in \{1, 2\}$, and hence that $\mathcal{D}$ and $\bar{\mathcal{D}}$ are equivalent, and Δ and $\bar{\Delta}$ are equivalent.

Conversely suppose that $\mathcal{D}$ and $\bar{\mathcal{D}}$ are equivalent and let π be an equivalence mapping $\mathcal{D}$ to $\bar{\mathcal{D}}$. So there are $a_1, a_2, c_1, c_2 \in G$ and $\varphi \in \mathrm{Aut}\, G$ such that

$$(g, i)^\pi = (a_i \cdot g^\varphi, i) \quad \text{and} \quad a_i \cdot \Delta_{ij}^\varphi = \bar{\Delta}_{ij} \cdot c_j$$

for all $g \in G$, $i, j \in \{1,2\}$. Then, by Remark 3.4, since $\rho^2 = 1$ so that ρ is also an isomorphism from $\bar{\mathcal{D}}$ to $\mathcal{D}$, the permutation $\tau := \pi \cdot \rho$ is an automorphism of $\mathcal{D}$. Let $g, h \in G$. Then

$$(h,i)^{g \cdot \pi} = (h \cdot g, i)^{\pi} = (a_i \cdot (h \cdot g)^{\varphi}, i) = (a_i \cdot h^{\varphi} \cdot g^{\varphi}, i) = (a_i \cdot h^{\varphi}, i)^{g^{\varphi}} = (h,i)^{\pi \cdot g^{\varphi}}$$

whence $\pi^{-1} \cdot g \cdot \pi = g^{\varphi}$; that is, π lies in the normaliser of the subgroup G of $\mathrm{Sym}\,\mathcal{P}$. Since ρ centralises G, it follows that $\tau \in N$. Finally, since π fixes $\mathcal{P}_1$ and $\mathcal{P}_2$, τ interchanges $\mathcal{P}_1$ and $\mathcal{P}_2$, and hence $\tau \in N \setminus E(G)$.

The proof actually establishes the following technical result which is sometimes useful in its own right.

Corollary 6.6 (a) *Suppose that $N \neq E(G)$ and let $\tau \in N \setminus E(G)$. Let ρ be the permutation of $\mathcal{P}$ which interchanges $(g,1)$ and $(g,2)$ for all $g \in G$. Then $\tau \cdot \rho$ is an equivalence from $\mathcal{D}$ to its conjugate design $\bar{\mathcal{D}}$.*

(b) *Conversely, if $\mathcal{D}$ and $\bar{\mathcal{D}}$ are equivalent and π is an equivalence from $\mathcal{D}$ to $\bar{\mathcal{D}}$, then $\pi \cdot \rho$ is an automorphism of $\mathcal{D}$, and $\pi \cdot \rho \in N \setminus E(G)$.*

7. Regular extensions.

As usual let $\mathcal{D} = \mathcal{D}(\Delta)$ be a symmetric design with half-regular group G and Rahilly family Δ of pre-difference sets, relative to base points $p_i = (1,i)$ and base blocks b_i, $i = 1,2$. If $G < R < \mathrm{Aut}\,\mathcal{D}$ and R is regular on $\mathcal{P}$, then R is called a *regular extension* of G. In this section we find necessary and sufficient conditions, in terms of the Rahilly family Δ, for G to have a regular extension.

Theorem 7.1 *Let $\mathcal{D} = \mathcal{D}(\Delta)$ be a symmetric design with half-regular group G and Rahilly family Δ of pre-difference sets. Then G has a regular extension if and only if there exists an equivalence π from $\mathcal{D}$ to its conjugate design $\mathcal{D}(\bar{\Delta})$ with associated automorphism $\theta \in \mathit{Aut} G$ and associated translations $(1, z, u^{-1}, u^{\theta^{-1}} \cdot z)$ such that $z^{\theta} = z$ and θ^2 is the inner automorphism of G induced by z.*

Remark 7.2 If π is as in Theorem 7.1, then

$$\Delta_{22} = \Delta_{11}^{\theta} \cdot u \quad \text{and} \quad \Delta_{12} = z \cdot \Delta_{21}^{\theta} \cdot u.$$

In the proof we show that, for such a π, if we set $\tau := \pi \cdot \rho$ where ρ interchanges $(g,1)$ and $(g,2)$ for all $g \in G$, then the subgroup $R := < G, \tau >$ is a regular extension of G, $\tau^2 = z$, and $g^{\tau} = g^{\theta}$ for all $g \in G$.

Proof. Suppose that there is a regular extension R of G. Then, as R normalises G and R is transitive on $\mathcal{P}$, we have $N = RE(G) \neq E(G)$. By Corollary 6.6, for any $\tau \in R \setminus E(G)$, $\pi := \tau \cdot \rho$ is an equivalence from $\mathcal{D}$ to $\mathcal{D}(\bar{\Delta})$, where ρ is the permutation which interchanges $(g,1)$ and $(g,2)$ for all $g \in G$. In the coset $G \cdot \tau$

in R there is a unique element such that $(1,1)^\tau = (1,2)$ since G is regular on $\mathcal{P}_1$. Let us assume that τ is chosen to be this element. It follows that π has associated translations (a_1, a_2, c_1, c_2) with $a_1 = 1$. Also the automorphism θ associated with π is the automorphism of G induced by conjugation by τ. It follows that, for all $g \in G$ and for $i = 1, 2$,

$$(g,i)^\tau = (g,i)^{\pi \cdot \rho} = (a_i \cdot g^\theta, i)^\rho = (a_i \cdot g^\theta, j)$$

where $j \in \{1,2\}$, $j \neq i$. Now $z := \tau^2 \in G$ since $|R : G| = 2$, and it follows that θ^2 is the inner automorphism of G induced by z. Considering the action of $z = \tau^2$ on $\mathcal{P}$, we have, for $i, j \in \{1,2\}$, $i \neq j$,

$$(z,i) = (1,i)^{\tau^2} = (a_i, j)^\tau = (a_j \cdot a_i^\theta, i)$$

whence $z = a_j \cdot a_i^\theta$. Taking $i = 1$ we get $a_2 = z$, and taking $i = 2$ we see that $z^\theta = z$. Set $u := c_1^{-1}$. Then $\Delta_{12} = \bar{\Delta}_{21} = a_2 \cdot \Delta_{21}^\theta \cdot c_1^{-1} = z \cdot (\bar{\Delta}_{12})^\theta \cdot u = z \cdot (a_1 \cdot \Delta_{12}^\theta \cdot c_2^{-1})^\theta \cdot u = z \cdot \Delta_{12}^{\theta^2} \cdot (c_2^{-1})^\theta \cdot u = \Delta_{12} \cdot z \cdot (c_2^{-1})^\theta \cdot u$. Also $\Delta_{22} = \bar{\Delta}_{11} = a_1 \cdot \Delta_{11}^\theta \cdot c_1^{-1} = (\bar{\Delta}_{22})^\theta \cdot u = (a_2 \cdot \Delta_{22}^\theta \cdot c_2^{-1})^\theta \cdot u = z^\theta \cdot \Delta_{22}^{\theta^2} \cdot (c_2^{-1})^\theta \cdot u = \Delta_{22} \cdot z \cdot (c_2^{-1})^\theta \cdot u$. It follows that $z \cdot (c_2^{-1})^\theta \cdot u$ fixes the block b_2 and hence is the identity element; that is, $c_2 = u^{\theta^{-1}} \cdot z$ since $z = z^\theta$.

To prove the converse, suppose that there is an equivalence π from $\mathcal{D}$ to $\mathcal{D}(\bar{\Delta})$ with associated automorphisms and translations as in the statement of the theorem. Set $\tau := \pi \cdot \rho$. Then by Corollary 6.6, τ is an automorphism of $\mathcal{D}$ and $\tau \in N \setminus E(G)$. Now, for all $g \in G$, and for $i, j \in \{1,2\}$ with $i \neq j$, we have

$$(1,i)^{\tau \cdot g^\theta} = (a_i \cdot g^\theta, j) = (g,i)^\tau = (1,i)^{g \cdot \tau},$$

so, since $\tau^{-1} \cdot g \cdot \tau \in G$ and G is semi-regular on $\mathcal{P}_i$, we have $\tau^{-1} \cdot g \cdot \tau = g^\theta$. Also

$$(g,i)^{\tau^2} = (a_i \cdot g^\theta, j)^\tau = (a_j \cdot a_i^\theta \cdot g^{\theta^2}, i) = (a_j \cdot a_i^\theta \cdot z^{-1} \cdot g \cdot z, i).$$

This is equal to $(g \cdot z, i) = (g,i)^z$ for both $i = 1$ and $i = 2$. Thus $\tau^2 = z$ and it follows that the subgroup $R =< G, \tau >$ of Aut $\mathcal{D}$ is a regular extension of G.

As we mentioned before, there is a standard construction of a symmetric design from a λ-difference set in a group such that the group is admitted as a group of automorphisms acting regularly on the points of the design. Whenever there is a regular extension of a half-regular group of a symmetric design $\mathcal{D}$, the design can be obtained by this method. We review this construction, and show how to obtain a λ-difference set for a regular extension R of G from a Rahilly family for G.

Let R be a finite group and λ a positive integer. A subset Σ of R of size $1 < |\Sigma| < |R|$ is said to be a *λ-difference set* for R if every element $g \neq 1$ of R may be represented exactly λ times as $g = x \cdot y^{-1}$ with $x, y \in \Sigma$.

If Σ is a λ-difference set of size k in a group R of order v, then the design $\mathcal{D} := (R, \mathcal{B})$ with $\mathcal{B} := \{\Sigma \cdot g \mid g \in R\}$ is a symmetric $2-(v,k,\lambda)$ design admitting R as a group of automorphisms acting regularly on the point set R. Conversely, if $\mathcal{D}$ is a symmetric $2-(v,k,\lambda)$ design with a subgroup R of automorphisms acting regularly on points, then we may identify the point set with R in such a way that R acts by right multiplication, and, hence, that the block set is $\{\Sigma \cdot g \mid g \in R\}$ where $\Sigma \subseteq R$ is any one of the blocks; it is easily checked from the properties of the design that Σ is a λ-difference set for R.

Theorem 7.3 *Let $\mathcal{D} = \mathcal{D}(\Delta)$ be a symmetric design with half-regular group G and Rahilly family Δ of pre-difference sets. If G has a regular extension R in $Aut\mathcal{D}$, and $R =< G, \tau >$ with τ as in Remark 7.2, then $\Sigma := \Delta_{11} \cup \tau \cdot \Delta_{21}$ is a λ-difference set in R, and its corresponding symmetric design is isomorphic to $\mathcal{D}$.*

Proof. By Remark 7.2, $\Delta_{22} = \Delta_{11}^{\theta} \cdot u, \Delta_{12} = z \cdot \Delta_{21}^{\theta} \cdot u$, and $\tau^{-1} = z^{-1} \cdot \tau = \tau \cdot z^{-1}$.

Let $x_i = \tau \cdot d_i \in \tau \cdot \Delta_{21}$ for $i = 1, 2$. Then $x_1 \cdot x_2^{-1} = (d_1 \cdot d_2^{-1})^{\tau^{-1}} = (d_1 \cdot d_2^{-1})^{\tau \cdot z^{-1}} = (z \cdot d_1^{\theta} \cdot u) \cdot (u^{-1} \cdot (d_2^{\theta})^{-1} \cdot z^{-1}) = w_1 \cdot w_2^{-1}$ with $w_i := z \cdot d_i^{\theta} \cdot u \in \Delta_{12}$. Using this, it now follows from Definition 2.1(a) that each non-identity element of G can be represented exactly λ times as $w \cdot y^{-1}$, where either both $w, y \in \Delta_{11}$ or both $w, y \in \tau \cdot \Delta_{21}$.

Next let $x = \tau \cdot d \in \tau \cdot \Delta_{21}$, and $c \in \Delta_{11}$. Then $x \cdot c^{-1} = (d \cdot c^{-1})^{\tau^{-1}} \cdot \tau = (d \cdot c^{-1})^{\tau \cdot z^{-1}} \cdot \tau = z \cdot d^{\theta} \cdot (c^{-1})^{\theta} \cdot z^{-1} \cdot \tau = (z \cdot d^{\theta} \cdot u) \cdot (u^{-1} \cdot (c^{-1})^{\theta}) \cdot \tau^{-1} = w \cdot y^{-1} \cdot \tau^{-1}$ where $w \in \Delta_{12}$ and $y \in \Delta_{22}$. Also $c \cdot x^{-1} = c \cdot d^{-1} \cdot \tau^{-1}$, and it follows from Definition 2.1(b) that each element of $R \setminus G = G \cdot \tau^{-1}$ can be represented exactly λ times as $w \cdot y^{-1}$ where either $w \in \Delta_{11}, y \in \tau \cdot \Delta_{21}$ or $y \in \Delta_{11}, w \in \tau \cdot \Delta_{21}$. Hence Σ is a λ-difference set in R.

The map which sends $(g, 1)$ to g, and $(g, 2)$ to $\tau \cdot g$, for all $g \in G$, is an isomorphism from $\mathcal{D}$ to the symmetric design corresponding to Σ defined above.

Remark 7.4

(a) The λ-difference sets most frequently investigated in the literature are those which arise in abelian groups. We note that the group R is abelian if and only if G is abelian and $\theta = 1$.

(b) The information in the proof of Theorem 7.3 provides a means of constructing symmetric $2-(v,k,\lambda)$ designs from λ-difference sets in groups of order v in the following way. We consider a group G of order $v/2$ which admits an automorphism θ such that θ^2 is the inner automorphism of G induced by some element $z \in G$ such that $z^{\theta} = z$; see [5, p225]. Given such G, z, and θ, we seek subsets Δ_{11} and Δ_{21} of G such that:

(i) $|\Delta_{11}| + |\Delta_{21}| = k$;

(ii) each non-identity element of G occurs exactly λ times in the multiset $\{w \cdot y^{-1} | \; w, y \in \Delta_{11}\} \cup \{(w \cdot y^{-1})^{\theta^{-1}} | w, y \in \Delta_{21}\}$;

(iii) each element of G occurs exactly λ times in the multiset

$$\{w \cdot y^{-1} | \; w \in \Delta_{11}, y \in \Delta_{21}\} \cup \{(w \cdot y^{-1} \cdot z)^{\theta^{-1}} | w \in \Delta_{21}, y \in \Delta_{11}\}.$$

It follows from the proof of Theorem 7.3 that these conditions lead to the construction of a λ-difference set in the group $R =< G, \tau >$ of order v where $\tau^2 = z$ and $g^\tau = g^\theta$ for all $g \in G$.

We believe that this may be especially fruitful in the case where G is cyclic and θ inverts every element of G, for example, the case where R is a dihedral or generalised quaternion group. We make further comments about searching for symmetric designs at the end of the next section.

Example 7.5 The biplane $\mathcal{B}_8$ of order four (see [1]) can be developed from the following Rahilly family of pre-difference sets in $G = Z_4 \times Z_2$:

$$\Delta_{11} = \{00, 20, 22, 32\}, \Delta_{22} = \{00, 20, 02, 32\}, \Delta_{12} = \{00, 10\}, \Delta_{21} = \{00, 30\}.$$

Let $\theta, \theta' \in \operatorname{Aut} G$, where θ, θ' are given by

$$10^\theta := 30 \text{ and } 02^\theta := 02,$$
$$10^{\theta'} := 30 \text{ and } 02^{\theta'} := 22.$$

Then the equivalences π, π' with associated automorphisms θ, θ' and associated translations

$$\begin{array}{ll} (00, 20, 20, 00) & (u = z = 20), \\ (00, 00, 00, 00) & (u' = z' = 00) \end{array}$$

define regular extensions $R = \langle G, \tau \rangle$ and $R' = \langle G, \tau' \rangle$ of G (where $\tau = \pi \cdot \rho, \tau' = \pi' \cdot \rho$). The extension $R \cong 16/7$ of [11] and the extension $R' \cong 16/8$ of [11]. These extensions give rise to λ-difference sets

$$\begin{array}{ll} \Sigma := \Delta_{11} \cup \tau \cdot \Delta_{21} \subseteq R & \text{and} \\ \Sigma' := \Delta_{11} \cup \tau' \cdot \Delta_{21} \subseteq R' & \end{array}$$

whose corresponding symmetric designs are isomorphic to $\mathcal{B}_8$.

8. Regular extensions and multipliers.

In this section we assume that $\mathcal{D}$ is a symmetric design with a half-regular subgroup G of automorphisms and corresponding Rahilly family Δ of pre-difference sets, and we assume moreover that there exists some regular extension for G in $\operatorname{Aut} \mathcal{D}$. Then by Theorem 7.3, there is a regular extension of the form $R =< G, \tau >$ where τ induces an automorphism θ of G, $\tau^2 = z \in G$ is such that $z^\theta = z$, and $\tau \cdot \rho$ is an equivalence from $\mathcal{D}$ to $\mathcal{D}(\bar{\Delta})$ with associated automorphism θ and associated translations $(1, z, u^{-1}, u^{\theta^{-1}} \cdot z)$. Here, as usual, ρ is the map which interchanges $(g, 1)$ and $(g, 2)$ for each $g \in G$. It follows from the results of the previous section that the set $\Sigma := \Delta_{11} \cup \tau \cdot \Delta_{21}$ is a λ-difference set in R.

Suppose that μ is a multiplier of type 1 for G as defined in Definition 6.1, that is $\mu \in E(G)_{p_1}$ where $p_1 = (1,1)$. By Lemma 6.3, μ is an equivalence of $\mathcal{D}$ with associated automorphism φ say, and associated translations $a_1 = 1, a_2, c_1, c_2 \in G$.

In [5,p67], a *multiplier of a λ-difference set for R* is defined to be an element of $N_{\mathrm{Aut}\,\mathcal{D}}(R)$ which fixes some chosen base point. Suppose that the base point with respect to which multipliers for R are defined is p_1. Then our multiplier μ of type 1 for G will be a multiplier for R if and only if μ normalises R. This is the case if and only if

$$[\mu, \tau] := \mu^{-1} \cdot \tau^{-1} \cdot \mu \cdot \tau \in G.$$

We obtain necessary and sufficient conditions for this in terms of the associated automorphisms and translations of μ and τ, or more correctly of μ and $\tau \cdot \rho$.

Theorem 8.1 *Let μ, τ, and R be as above. Then μ is a multiplier for R if and only if:*

(a) $\theta \cdot \varphi = \varphi \cdot \theta \cdot \alpha$, *where α is the inner automorphism of G induced by a_2;*
(b) $a_2^\theta \cdot a_2 = z^{-1} \cdot z^\theta$.

Remark 8.2 The proof of this result shows that, if u is a multiplier for R, then $[\mu, \tau] = a_2^{-1}$.

Proof. Suppose that μ is a multiplier for R. Then $\mu \cdot \tau = \tau \cdot \mu \cdot g$, for some $g \in G$. Then, for all $x \in G$, we have

$$(x^{\varphi \cdot \theta}, 2) = (x^\varphi, 1)^\tau = (x, 1)^{\mu \cdot \tau} = (x, 1)^{\tau \cdot \mu \cdot g} = (x^\theta, 2)^{\mu \cdot g} = (a_2 \cdot x^{\theta \cdot \varphi} \cdot g, 2).$$

Setting $x = 1$ we have $g = a_2^{-1}$, and then, considering the displayed equation for arbitrary x, we have $\theta \cdot \varphi = \varphi \cdot \theta \cdot \alpha$, where α is the automorphism of G induced by conjugation by a_2. Further, we have

$$(z \cdot a_2^\theta, 1) = (a_2, 2)^\tau = (1, 2)^{\mu \cdot \tau} = (1, 2)^{\tau \cdot \mu \cdot a_2^{-1}} = (z, 1)^{\mu \cdot a_2^{-1}} = (z^\varphi \cdot a_2^{-1}, 1),$$

and it follows that $z \cdot a_2^\theta = z^\varphi \cdot a_2^{-1}$, whence (b) follows.

Conversely, suppose that (a) and (b) are true. Then, for all $x \in G$,

$$(x, 1)^{\mu \cdot \tau} = (x^\varphi, 1)^\tau = (x^{\varphi \cdot \theta}, 2) = (a_2 \cdot x^{\theta \cdot \varphi} \cdot a_2^{-1}, 2) = (x^\theta, 2)^{\mu \cdot a_2^{-1}} = (x, 1)^{\tau \cdot \mu \cdot a_2^{-1}},$$

and

$$\begin{aligned}(x, 2)^{\mu \cdot \tau} &= (a_2 \cdot x^\varphi, 2)^\tau = (z \cdot a_2^\theta \cdot x^{\varphi \cdot \theta}, 1) \\ &= (z^\varphi \cdot x^{\theta \cdot \varphi} \cdot a_2^{-1}, 1) = (z \cdot x^\theta, 1)^{\mu \cdot a_2^{-1}} = (x, 2)^{\tau \cdot \mu \cdot a_2^{-1}}.\end{aligned}$$

Hence $\mu \cdot \tau = \tau \cdot \mu \cdot a_2^{-1}$, and so μ is a multiplier for R.

If μ is a multiplier for R as in Theorem 8.1, then, in addition to the conditions in Theorem 8.1 on a_2 and φ, there is an extra condition on the associated translations of μ which must be satisfied.

Proposition 8.3 *If μ is a multiplier for R, then*

$$c_2 = u^{-1} \cdot c_1^\theta \cdot a_2 \cdot u^\varphi .$$

Remark 8.4 The proof also shows how the images of the base blocks $b_j = (\Delta_{1j} \times \{1\}) \cup (\Delta_{2j} \times \{2\})$ under $\mu \cdot \tau$ may be computed. The image of b_1 is computed in full detail; that of b_2 may be obtained similarly. The answers are:

$$b_1^{\mu\cdot\tau} = b_2^{u^{-1}\cdot c_1^\theta} \quad \text{and} \quad b_2^{\mu\cdot\tau} = b_1^{z\cdot u^\theta \cdot c_2^\theta} .$$

Proof. By Remark 7.2, $\Delta_{22} = \Delta_{11}^\theta \cdot u$, and $\Delta_{12} = z \cdot \Delta_{21}^\theta \cdot u$. Applying θ to these equations, we have also

$$\Delta_{22}^\theta = z^{-1} \cdot \Delta_{11} \cdot z \cdot u^\theta \quad \text{and} \quad \Delta_{12}^\theta = \Delta_{12} \cdot z \cdot u^\theta$$

noting that θ^2 is the inner automorphism induced by $z = z^\theta$.

Now we compute:

$$\begin{aligned} b_1^{\mu\cdot\tau} &= ((\Delta_{11} \times \{1\}) \cup (\Delta_{21} \times \{2\}))^{\mu\cdot\tau} = (\Delta_{11}^\varphi \times \{1\})^\tau \cup (a_2 \cdot \Delta_{21}^\varphi \times \{2\})^\tau \\ &= (\Delta_{11} \cdot c_1 \times \{1\})^\tau \cup (\Delta_{21} \cdot c_1 \times \{2\})^\tau = (\Delta_{11}^\theta \cdot c_1^\theta \times \{2\}) \cup (z \cdot \Delta_{21}^\theta \cdot c_1^\theta \times \{1\}) \\ &= (\Delta_{22} \cdot u^{-1} \cdot c_1^\theta \times \{2\}) \cup (\Delta_{12} \cdot u^{-1} \cdot c_1^\theta \times \{1\}) = b_2^{u^{-1}\cdot c_1^\theta} \end{aligned}$$

and similarly

$$\begin{aligned} b_1^{\tau\cdot\mu\cdot a_2^{-1}} &= (\Delta_{11}^\theta \times \{2\})^{\mu\cdot a_2^{-1}} \cup (z \cdot \Delta_{21}^\theta \times \{1\})^{\mu\cdot a_2^{-1}} \\ &= (\Delta_{22} \cdot u^{-1} \times \{2\})^{\mu\cdot a_2^{-1}} \cup (\Delta_{12} \cdot u^{-1} \times \{1\})^{\mu\cdot a_2^{-1}} \\ &= (a_2 \cdot \Delta_{22}^\varphi \cdot (u^{-1})^\varphi \cdot a_2^{-1} \times \{2\}) \cup (\Delta_{12}^\varphi \cdot (u^{-1})^\varphi \cdot a_2^{-1} \times \{1\}) \\ &= (\Delta_{22} \cdot c_2 \cdot (u^{-1})^\varphi \cdot a_2^{-1} \times \{2\}) \cup (\Delta_{12} \cdot c_2 \cdot (u^{-1})^\varphi \cdot a_2^{-1} \times \{1\}) \\ &= b_2^{c_2\cdot(u^{-1})^\varphi\cdot a_2^{-1}} . \end{aligned}$$

It follows, since G acts regularly on $\mathcal{B}_2$, that $u^{-1} \cdot c_1^\theta = c_2 \cdot (u^{-1})^\varphi \cdot a_2^{-1}$, whence $c_2 = u^{-1} \cdot c_1^\theta \cdot a_2 \cdot u^\varphi$.

In the remainder of this section we shall assume that μ is a multiplier for R, and also that μ is a *numerical* multiplier for G of type 1 of degree m.

When is μ a numerical multiplier for R, and, if it is, what is its degree?

Recall that μ is numerical for G if $g^\varphi = g^m$ for all $g \in G$, where φ is its associated automorphism, and the least positive integer m is called the degree of μ. Let $\varphi' \in \operatorname{Aut} R$ be the automorphism induced by μ. Then φ' restricted to G is

φ, and $\tau^{\varphi'} = \mu^{-1} \cdot \tau \cdot \mu = \tau \cdot a_2$ by Remark 8.2. Then μ would be numerical for R, if there is some integer m' such that $x^{\varphi'} = x^{m'}$ for all $x \in R$. Of course we would have to have $g^{m'} = g^m$ for all $g \in G$, and in this case the degree of μ as a numerical multiplier for R would be the smallest positive such integer m'. Clearly $m' \geq m$, and as $g^{m'-m} = 1$ for all $g \in G$ it follows that $m' - m$ is divisible by the *exponent* $e(G)$ of G, that is the least common multiple of the orders of all the elements of G.

Question 8.5 *If μ is a numerical multiplier for G of degree m, and a numerical multiplier for R of degree m', is it possible for m' to be greater than m?*

We have some partial answers to this question.

Lemma 8.6 *If μ is a numerical multiplier for R of degree m', then:*

(a) *m' must be odd;*

(b) $a_2 = z^{(m'-1)/2}$.

Proof. We must have $\mu^{-1} \cdot \tau \cdot \mu = \tau^{m'}$. Since $\mu^{-1} \cdot \tau \cdot \mu \in R \backslash G$ and since $\tau^2 = z \in G$, m' must be odd. Also we have $\mu^{-1} \cdot \tau^{-1} \cdot \mu = \tau^{-m'}$ and so $a_2^{-1} = [\mu, \tau] = \tau^{-m'} \cdot \tau$, so $a_2 = \tau^{m'-1} = z^{(m'-1)/2}$.

If τ centralises G, in particular if R is abelian, and if $m' = m$, the converse of this lemma is true.

Lemma 8.7 *Suppose that τ centralises G. Then μ is a numerical multiplier for R of degree m if and only if:*

(a) *m is odd;*

(b) $a_2 = z^{(m-1)/2}$.

Proof. Suppose that τ centralises G and that (a) and (b) hold. Each element of R is of the form $\tau^d \cdot g$ where d is 0 or 1 and $g \in G$. We have $\mu^{-1} \cdot g \cdot \mu = g^m$ since μ is numerical of degree m for G. Further, since $\mu^{-1} \cdot \tau \cdot \mu = \tau \cdot a_2 = \tau \cdot z^{(m-1)/2} = \tau^m$, we also have $\mu^{-1} \cdot \tau \cdot g \cdot \mu = \tau^m \cdot g^m$, which equals $(\tau \cdot g)^m$ since τ centralises g.

However, we would like a sufficient condition for μ to be numerical for R in the case where R is non-abelian. While this seems difficult in general, we do have such a condition when G is abelian.

Proposition 8.8 *Suppose that G is abelian. Then μ is a numerical multiplier for R of degree m if and only if:*

(a) *m is odd;*

(b) $a_2 = z^{(m-1)/2}$;

(c) *for each $(m-1)/2$-th power $x = g^{(m-1)/2} \in G$, $x^\theta = x$.*

Proof. Suppose that μ is numerical for R of degree m. Then by Lemma 8.6, (a) and (b) hold. Let $g \in G$. Note that $(\tau \cdot g)^2 = \tau^2 \cdot (\tau^{-1} \cdot g \cdot \tau) \cdot g = z \cdot g^\theta \cdot g$. Then

$$(\tau \cdot g)^\mu = \tau^\mu \cdot g^\mu = \tau^m \cdot g^m,$$

and, using the fact that G is abelian,

$$\begin{aligned}(\tau \cdot g)^m &= \tau \cdot g \cdot (z \cdot g^\theta \cdot g)^{(m-1)/2} \\ &= \tau \cdot z^{(m-1)/2} \cdot (g^{(m-1)/2})^\theta \cdot g^{(m+1)/2} \\ &= \tau^m \cdot (g^{(m-1)/2})^\theta \cdot g^{(m+1)/2}.\end{aligned}$$

Since these two expressions are equal, it follows that θ fixes $g^{(m-1)/2}$ for each $g \in G$. Conversely, if (a), (b), and (c) all hold, then the above equations show that $(\tau \cdot g)^\mu = (\tau \cdot g)^m$ for all $g \in G$, and we know already that $g^\mu = g^m$ for all $g \in G$. Thus μ is numerical for R of degree m.

Remark 8.9

(a) We mentioned earlier the possibility of using the information in these latter sections for searching for symmetric designs which possess a non-abelian regular subgroup of automorphisms R having an abelian subgroup G of index 2. There are infinitely many known examples of such designs for which the group G is cyclic, namely in the class of symmetric designs formed from the points and hyperplanes of the d-dimensional projective geometry PG(d, p^n), when d and the prime p are both odd. The half-regular groups $G =< y >$ in question have an extension $R =< G, \tau >$ such that

$$\tau^2 = z = y^w, \text{ and } g \cdot \tau = \tau \cdot g^l$$

where $w = (p^{n(d+1)/2} + 1)/2$ and $l = p^{n(d+1)/2}$. For further details, see [3, pp33-34].

Symmetric designs of this type admitting a nontrivial numerical multiplier for R, that is, of degree $m > 1$, are of particular interest, and Proposition 8.8 gives restrictions on the group G which would aid in the search for such designs. Firstly, given G, the assumption of the existence of the multiplier μ helps us to decide upon the extension R. Secondly, it limits the search for Δ_{11} and Δ_{21} in G, or equivalently, for $\Sigma = \Delta_{11} \cup (\tau \cdot \Delta_{21})$ in R, for we must have, by Remark 7.4(b),

$$\Delta_{11}^m = \Delta_{11} \cdot c_1, \text{ and } z^{(m-1)/2} \cdot \Delta_{21}^m = \Delta_{21} \cdot c_1$$

where $\Delta_{ij}^m = \{g^m | g \in \Delta_{ij}\}$, in order that $\Sigma^\varphi = \Sigma \cdot \boldsymbol{c}_1$.

(b) We comment further on the case in which G is cyclic of order $v/2$. By Lemma 4.1,

$$v/2 = (s^2 + s + \lambda)(s^2 - s + \lambda)/2\lambda,$$

for some positive integers s and λ, such that λ is even and λ divides $s^2(s^2 - 1)/2$. Suppose that G has a Rahilly family Δ of pre-difference sets such that in the corresponding design $\mathcal{D}(\Delta)$, G has a regular extension R. By Remark 7.2, we may assume that $R =< G, \tau >$ where τ induces an automorphism θ of G, and $\tau^2 = z \in G$ such that $z^\theta = z$. Since G is cyclic, there is an integer l, with $1 \leq l \leq v/2 - 1$ and $(l, v/2) = 1$, such that

$$g^\theta = g^l,$$

for all $g \in G$. If we are interested in non-abelian groups R, then we want $2 \leq l \leq v/2 - 1$. In order that $\mathcal{D}(\Delta)$ admit a numerical multiplier μ for R of degree m, we must have, by Proposition 8.8, the following conditions on m:

(i) $(m, v/2) = 1$, so that $g \rightarrow g^m$ is an automorphism of G;

(ii) $((m-1)/2, v/2) = 1$, so that the subgroup consisting of the $(m-1)/2$-th powers of elements of G is not equal to G.

Then, given such an m, the integer l must satisfy the following conditions:

(iii) $(l, v/2) = 1$, so that θ is an automorphism of G;

(iv) $l^2 \equiv 1 (\text{mod } v/2)$, for the facts that G is abelian and $\tau^2 = z$ imply that θ^2 is the identity;

(v) $(l-1)(m-1)/2 \equiv 1 (\text{mod } v/2)$, so that θ fixes each of the $(m-1)/2$-th powers of elements of G.

(c) These conditions on m and l are not unduly restrictive. For example, with $s = \lambda = 4$, and hence with $v/2 = 48$, there are 19 pairs of values of m, l between 2 and 47 satisfying them. An infinite class of parameters satisfying conditions (i)-(v), with λ even and λ dividing $s^2(s^2 - 1)/2$, is given by:

$$\lambda = s = 2x, \; v/2 = 4x^2(x+1), \; l = 2x^2(x+1) + 1, \; m = 5,$$

where $x \equiv 1, 2, \text{or } 3 (\text{mod } 5)$.

On the other hand, when $s = \lambda = 2$, so that we may take G to be the group of integers modulo 8, there is a unique solution for m, l satisfying conditions (i)-(v), namely $m = l = 5$. A search based upon Theorems 7.1 and 8.1, and Propositions 8.3 and 8.8 led quickly to the 2-difference set

$$\Sigma = \{0, 1, 2, 5, \tau, \tau \cdot 6\},$$

which satisfies $5\Sigma = \Sigma$ in the non-abelian extension $R =< G, \tau >$ of G such that τ induces the automorphism $g \rightarrow 5g$ of G. Here we write G additively as integers modulo 8, and we write the elements of the non-trivial coset of G in R as $\tau \cdot i$ for $i \in G$.

(d) The latitude we have in choosing base blocks affords some simplification to our search. By [6, p46], since the multiplier μ fixes a point, it also fixes a block. By interchanging the roles of the base blocks b_1 and b_2, if necessary, we may assume that μ fixes a block in $\mathcal{B}_1$. Of course this means that we may no longer assume that $|\Delta_{11}| \geq |\Delta_{21}|$. Then, by changing our choice of base block $b_1 \in \mathcal{B}_1$, if necessary, we may assume that μ fixes b_1, and hence that $c_1 = 1$.

Further, the element z can be taken to be any element of G fixed by θ. Then, since $a_2 = z^{(m-1)/2}$, and since θ fixes the $(m-1)/2$-th power of each element of G, it follows that condition (b) of Theorem 7.5, that is, $a_2^{\theta} \cdot a_2 = z^{-1} \cdot z^{\varphi}$, is automatically satisfied.

Acknowledgements. We thank Peter Adams, Adelle Howse and Keith Matthews for assistance with calculations.

This work was sponsored by ARC grants A69031285, A49130102 and A68931532. One of us (CEP) held a Raybould Visiting Fellowship at the University of Queensland during the time when most of this work was carried out, and another (APS) is supported by an Australian Senior Research Fellowship.

REFERENCES

1. E. F. Assmus, Jr. and C. J. Salwach, *The* (16, 6, 2)*-designs*, International Journal of Mathematics and Mathematical Sciences **2** (1979), 261-281.
2. R. C. Bose, *On the construction of balanced incomplete block designs*, Annals of Eugenics **9** (1939), 353-399.
3. B. W. Char, K. O. Geddes, G. H. Gonnet, B. L. Leong, M. B. Monagan, S. M. Watt, *Maple V Language Reference Manual*, Springer-Verlag, New York, 1991.
4. P. Dembowski, *Finite Geometries*, Springer, Berlin, Heidelberg, New York, 1968.
5. Marshall Hall, Jr., *The Theory of Groups*, The Macmillan Company, New York, 1959.
6. D. R. Hughes and F. C. Piper, *Design Theory*, Cambridge University Press, Cambridge, 1985.
7. R. E. Kibler, *A summary of non-cyclic difference sets, $k \leq 20$*, Journal of Combinatorial Theory (A) **25** (1978), 62-67.
8. D. E. Knuth, *The Art of Computer Programming. 2d ed*, Addison-Wesley Publishing Company, Philippines, 1981.
9. Alan Rahilly, *Divisions of symmetric designs into two parts*, Graphs and Combinatorics **4** (1988), 67-73.
10. Alan Rahilly, *On a class of symmetric designs*, Note di Matematica **9** (1989), 241-248.
11. A. D. Thomas and G. V. Wood, *Group Tables*, Shiva Publishing Limited, 1980.

(Received 22/3/93)