J. Austral. Math. Soc. (*Series A*) **58** (1995), 210–218

BALANCED DIRECTED CYCLE DESIGNS BASED ON CYCLIC GROUPS

CHAUFAH NILRAT and CHERYL E. PRAEGER

(Received 29 January 1991; revised 27 August 1992)

Communicated by L. Caccetta

Abstract

A balanced directed cycle design with parameters $(v, k, 1)$, sometimes called a $(v, k, 1)C_k^{\rightarrow}$*-design*, is a decomposition of the complete directed graph $K_v^{\rightarrow}$ into edge disjoint directed cycles of length k. A complete classification is given of $(v, k, 1)C_k^{\rightarrow}$-designs admitting the holomorph $\{\phi_{a,b} : x \mapsto ax + b \mid a, b \in \mathbb{Z}_v, (a, v) = 1\}$ of the cyclic group $\mathbb{Z}_v$ as a group of automorphisms. In particular it is shown that such a design exists if and only if one of (a) $k = 2$, (b) $p \equiv 1(\text{mod}\, k)$ for each prime p dividing v, or (c) k is the least prime dividing v, k^2 does not divide v, and $p \equiv 1(\text{mod}\, k)$ for each prime $p > k$ dividing v.

1991 *Mathematics subject classification* (*Amer. Math. Soc.*): 05B30, 20B25.

In 1987, Brand and Huffman [2] showed that there were essentially two types of balanced directed cycle designs, sometimes called Mendelsohn designs, admitting a one-dimensional affine group $AGL(1, q)$ over a field as a group of automorphisms. The two types of examples correspond roughly to the additive and multiplicative structure of the field $GF(q)$. This paper was motivated by their result. We classify all balanced directed cycle designs on v points admitting the holomorph $\{\phi_{a,b} : x \mapsto ax + b \mid a, b \in \mathbb{Z}_v, (a, v) = 1\}$ of $\mathbb{Z}_v$ as automorphisms. Again there are two basic types of designs, based on the additive and multiplicative structure, and these basic designs are combined in a well-defined manner to give the complete class of examples.

We shall be concerned with *balanced directed cycle designs* with parameters $(v, k, 1)$. Such designs have been called in the literature $(v, k, 1)C_k^{\rightarrow}$-designs and 2-$(v, k, 1)$ Mendelsohn designs, (see [2, 3, 4]). We shall use the former notation. A $(v, k, 1)C_k^{\rightarrow}$*-design* is a decomposition of the complete directed graph $K_v^{\rightarrow}$ into edge

https://doi.org/10.1017/S1446788700038246 Published online by Cambridge University Press

disjoint directed cycles of length k. The automorphism group Aut $\mathcal{D}$ of such a design $\mathcal{D}$ is the subgroup of permutations of the points of $K_v^{\rightarrow}$ which permute the cycles in the decomposition among themselves. If $H \leq \operatorname{Aut}\mathcal{D}$ we shall say that $\mathcal{D}$ *admits* H as a group of automorphisms. A method often used for constructing these cycle designs is the so-called *difference method* in which the set of v points of the design is identified with a group G of order v in such a way that G, acting by right multiplication, is admitted as a group of automorphisms. We shall say that such a design is *based* on G. This difference method of construction was discussed in [1] , and the designs described in [2] and [4] arise in this way. The normalizer of the group G (acting by right multiplication) in the symmetric group of all permutations of a set of v points is called the *holomorph* Hol (G) of G and is the group generated by G and by Aut G (acting naturally on the set of v points still identified with G). Our aim is to classify all $(v, k, 1)C_k^{\rightarrow}$ designs based on $\mathbb{Z}_v$ and admitting the full holomorph Hol $(\mathbb{Z}_v)$ as automorphisms. For cyclic groups $G = \mathbb{Z}_v$ the holomorph comprises simply the maps $\phi_{a,b} : x \mapsto ax + b$ where $a, b \in \mathbb{Z}_v$ and $(a, v) = 1$. As $G = \mathbb{Z}_v$ is abelian we use addition as the group operation, so G acting by addition is the subgroup $\{\phi_{1,b} \mid b \in \mathbb{Z}_v\}$ of Hol $(\mathbb{Z}_v)$, and Aut $\mathbb{Z}_v = \{\phi_{a,0} \mid (a, v) = 1\}$ consists of the multiplication maps by integers relatively prime to v.

As described in [2], $(v, k, 1)C_k^{\rightarrow}$ designs $\mathcal{D}$ based on a group G may be described quite compactly by the corresponding *difference family* $\hat{\mathcal{D}}$ which consists of one k-tuple $m(\mathcal{O})$ of non-identity elements of G corresponding to each orbit $\mathcal{O}$ of G on the cycles of $\mathcal{D}$. We define $\hat{\mathcal{D}}$ for additive abelian groups. (The definition for general groups is given in [4].) For a G-orbit $\mathcal{O}$ and cycle $\mathbf{x} = (x_1, \ldots, x_k)$ in $\mathcal{O}$, the k-tuple $m(\mathcal{O})$ is defined as

$$m(\mathcal{O}) = (x_2 - x_1, x_3 - x_2, \ldots, x_k - x_{k-1}, x_1 - x_k).$$

Clearly $m(\mathcal{O})$ is independent of the cycle $\mathbf{x}$ in $\mathcal{O}$ as any other member of $\mathcal{O}$ is of the form $\mathbf{x} + b = (x_1 + b, x_2 + b, \ldots, x_k + b)$ for some $b \in G$. Note that $\mathbf{x}$, and hence $m(\mathcal{O})$, are given only up to a cyclic shift, for example $(x_2, \ldots, x_k, x_1)$ denotes the same cycle and we write $\mathbf{x} \equiv \mathbf{y}$ to mean that the k-tuple $\mathbf{y}$ may be obtained from $\mathbf{x}$ by some cyclic shift. The design $\mathcal{D}$ is easily recovered from $\hat{\mathcal{D}}$ since if $m(\mathcal{O}) = (x_1, \ldots, x_k)$ then

$$\mathcal{O} = \{(x, x + x_2, x + x_2 + x_3, \ldots, x + x_2 + \ldots + x_k) \mid x \in G\}.$$

We shall usually describe such a design $\mathcal{D}$ by giving its difference family $\hat{\mathcal{D}}$. Moreover [2] and [1] give a criterion for deciding when a collection of k-tuples of elements of a group G of order v is the difference family of a $(v, k, 1)C_k^{\rightarrow}$ design based on G. We quote their result here as it will be used very often in the paper. If $m = (x_1, \ldots, x_k)$ and if c is the least positive integer such that $x_i = x_{i+c}$ for all i, (reading subscripts modulo k), we shall refer to the c-tuple $(x_1, \ldots, x_c)$ as the *first period* of m. Note

https://doi.org/10.1017/S1446788700038246 Published online by Cambridge University Press

that, since m is defined up to a cyclic shift, the first period of m is also defined up to a cyclic shift.

DIFFERENCE FAMILY CRITERION. *Let G be a group of order v, let $k \geq 2$, and let $\hat{\mathcal{D}}$ be a set of k-tuples of elements of G (where we take each k-tuple to be identified with all its cyclic shifts). Then $\hat{\mathcal{D}}$ is the difference family of a $(v, k, 1)C_k^{\to}$ design based on G if and only if the following both hold.*

(a) *$\hat{\mathcal{D}}$ is contained in*

$$\begin{aligned} \mathcal{S}_k(G) = \{(x_1, \dots, x_k) \mid x_i \in G, \quad & \textit{and for all} \quad i, j = 1, \dots, k, \\ x_{i+1} + \cdots + x_{i+j} = 0 \quad & \textit{if and only if} \quad j = k\} \end{aligned}$$

(The subscripts are to be taken modulo k.)

(b) *Each non-identity element of G occurs exactly once in the first period of exactly one k-tuple of $\hat{\mathcal{D}}$.*

If v is prime then Brand and Huffman [2] have classified all $(v, k, 1)C_k^{\to}$ designs admitting Hol $(\mathbb{Z}_v)$, while if v is square free such designs were shown in [4, Theorem 5.10] to be obtainable by a generalized product construction from the Brand and Huffman designs for the prime factors of v. We treat the general case here. Our result is stated below, (where $y(x_1, x_2, \dots, x_k)$ denotes $(yx_1, yx_2, \dots, yx_k)$).

THEOREM 1. *Let $v = p_1^{e_1} \dots p_r^{e_r}$ where the p_i are primes, the e_i are positive integers, $r \geq 1$, and if $r > 1$ then $p_1 < p_2 < \cdots < p_r$. Let $\hat{\mathcal{D}}$ be the difference family of a $(v, k, 1)C_k^{\to}$ design based on $\mathbb{Z}_v$ and admitting* Hol $(\mathbb{Z}_v)$, *where $k > 1$.*

(a) *Then one of the following holds.*

(i) $k = 2$.

(ii) $p_i \equiv 1 \pmod k$ *for each $i = 1, \dots, r$.*

(iii) *k is the least prime dividing v, k^2 does not divide v, and, $p_i \equiv 1 \pmod k$ for each $1 < i \leq r$.*

(b) *The difference family $\hat{\mathcal{D}}$ is the disjoint union of subsets $\hat{\mathcal{D}}(d)$ (where d is a divisor of v and $d < v$) defined as follows.*

(i) *If $k \neq p_1$, or if $k = p_1$ and v/d is not a power of p_1, then $\hat{\mathcal{D}}(d)$ consists of the k-tuples $dj(1, a, \dots, a^{k-1})$ where $1 \leq j < v/d$, $(jd, v) = d$, and a has multiplicative order k modulo v/d. (The element a depends only on d.)*

(ii) *If $k = p_1$ and $v/d = p_1^e$, $e \leq e_1$, then either $e_1 = e = 1$ and $\hat{\mathcal{D}}(d)$ consists of the k-tuples $dj(1, 1, \dots, 1)$ for $1 \leq j \leq p_1 - 1$, or $k = p_1 = 2$, $e_1 \geq 2$ and $\hat{\mathcal{D}}(d)$ consists of the k-tuples $dj(1, -1)$ for $1 \leq j < 2^e$.*

https://doi.org/10.1017/S1446788700038246 Published online by Cambridge University Press

Conversely, each set of k-tuples (up to cyclic shifts) $\hat{\mathcal{D}}$ defined as in (b) *is the difference family of a* $(v, k, 1)C_k^{\to}$ *design based on* $\mathbb{Z}_v$ *and admitting* $\mathrm{Hol}(\mathbb{Z}_v)$.

An immediate consequence of this classification is a classification of the set of parameters (v, k) for which designs of this type exist.

COROLLARY 2. *There exists a* $(v, k, 1)C_k^{\to}$ *design based on* $\mathbb{Z}_v$ *and admitting* $\mathrm{Hol}(\mathbb{Z}_v)$, *where* $k > 1$, *if and only if one of the following holds.*

(a) $k = 2$.

(b) $p \equiv 1 \pmod{k}$ *for each prime* p *dividing* v.

(c) k *is the least prime dividing* v, k^2 *does not divide* v, *and,* $p \equiv 1 \pmod{k}$ *for each prime* $p > k$ *dividing* v.

The cases in the corollary above may be made disjoint by requiring $k > 2$ in (b) and (c). These results will be proved in the next section.

REMARK. One general observation arising from the proof of Theorem 1 is that, whenever a $(v, k, 1)C_k^{\to}$ design based on a group G admits an automorphism $\sigma \in \mathrm{Aut}\, G$ such that the centralizer $C_G(\sigma)$ of σ in G is very small, the value of k is severely restricted.

To illustrate this point we have included, in Section 2, a classification of all such designs for which $C_G(\sigma)$ is cyclic of order 2 or 4.

1. Proof of Theorem 1

Let $\mathcal{D}$ be a $(v, k, 1)C_k^{\to}$ design based on $G = \mathbb{Z}_v$ and admitting $\mathrm{Hol}(G)$, and let $\hat{\mathcal{D}}$ be its difference family. Write $v = p_1^{e_1} \dots p_r^{e_r}$ where the p_i are primes, the e_i are positive integers, $r \geq 1$, and $p_1 < p_2 < \cdots < p_r$. If $r \geq 2$ then $G \cong G_1 \oplus \cdots \oplus G_r$, where $G_i := \mathbb{Z}_{p_i^{e_i}}$, and a convenient isomorphism is given by $x \mapsto (v_1 x, v_2 x, \dots, v_r x)$ where $v_i := v/p_i^{e_i}$ and the i-th entry $v_i x$ is taken modulo $p_i^{e_i}$. (Note that we are identifying the additive group $\mathbb{Z}_{v/d}$ with $d\mathbb{Z}_v$ for a divisor d of v.) Moreover the automorphism group of G also decomposes as $\mathrm{Aut}\, G \cong \mathrm{Aut}\, G_1 \times \cdots \times \mathrm{Aut}\, G_r$ and an isomorphism is given by $\phi \mapsto (\phi_1, \dots, \phi_r)$ where for each i, $(v_i x)\phi_i := v_i(x\phi)$, and

$$(v_1 x, \dots, v_r x)(\phi_1, \dots, \phi_r) := ((v_1 x)\phi_1, \dots, (v_r x)\phi_r).$$

Thus we have also $\mathrm{Hol}(G) \cong \mathrm{Hol}(G_1) \times \cdots \times \mathrm{Hol}(G_r)$. Let $I := \{1, \dots, r\}$ and for $x \in \mathbb{Z}_v$ define

$$I(x) := \{i \mid v_i x \not\equiv 0 \pmod{p_i^{e_i}}\},$$

https://doi.org/10.1017/S1446788700038246 Published online by Cambridge University Press

the support of x in the direct sum decomposition above, and define $d(x) = (x, v)$, the greatest common divisor of x and v. First we show that, for $m \in \hat{\mathcal{D}}$, the values of these two functions on an entry in m are independent of the entry.

LEMMA 1.1. *For $m = (g_1, \dots, g_k) \in \hat{\mathcal{D}}$ we have $I(g_1) = \cdots = I(g_k)$, which we shall denote by $I(m)$, and $d(g_1) = \cdots = d(g_k)$, which we shall denote by $d(m)$.*

PROOF. The fact that $I(g_1) = \cdots = I(g_k)$ was proved in [4, Proposition 5.6(a)]. As m is only given up to cyclic shifts we may suppose that $d(g_1) \leq d(g_i)$ for all i. Suppose that, for some i, $d(g_1) \neq d(g_i)$. Then, for some prime $p = p_j$ $(1 \leq j \leq r)$ and for some integer e, $(1 \leq e \leq e_j)$, p^e divides g_i but not g_1. Since $I(g_1) = I(g_i)$ we must have $e < e_j$, whence the integer $a := 1 + v/p^e$ is relatively prime to v. Thus $\phi_{a,0} \in \mathrm{Hol}\,(G) \subseteq \mathrm{Aut}\,\mathcal{D}$, and so fixes $\hat{\mathcal{D}}$ setwise. So $m\phi_{a,0}$ is an element of $\hat{\mathcal{D}}$ containing $g_i\phi_{a,0} = g_i$ whence $m\phi_{a,0} = m$ by the Difference Family Criterion. However this is not possible since $g_1\phi_{a,0} \neq g_1$. Thus $d(g_1) = d(g_i)$ for all i.

Thus $\hat{\mathcal{D}}$ is partitioned into disjoint subsets $\hat{\mathcal{D}}(d) = \{m \in \hat{\mathcal{D}} \mid d(m) = d\}$ for each proper divisor $d < v$ of v. Since each non-zero element of G occurs in some k-tuple of $\hat{\mathcal{D}}$, each set $\hat{\mathcal{D}}(d)$ is non-empty. Next we show that $\mathcal{D}$ has many subdesigns with similar symmetry properties to $\mathcal{D}$ itself. Note that this set of subdesigns contains all the designs given by [4, Proposition 5.6(b)].

LEMMA 1.2. *Let $d < v$ be a divisor of v. Then the union $\hat{\mathcal{D}}[d] = \bigcup_{d/b} \hat{\mathcal{D}}(b)$ is a difference family for a $(v/d, k, 1)C_k^{\rightarrow}$ design based on $\mathbb{Z}_{v/d}$ admitting* $\mathrm{Hol}\,(\mathbb{Z}_{v/d})$. *(Here we are identifying $\mathbb{Z}_{v/d}$ with $d\mathbb{Z}_v$.)*

PROOF. By the Difference Family Criterion for $\hat{\mathcal{D}}$, each element dx of $d\mathbb{Z}_v$ occurs exactly once in the first period of exactly one k-tuple m in $\hat{\mathcal{D}}$, and by Lemma 1.1, $m \in \hat{\mathcal{D}}[d]$. We identify $\mathbb{Z}_{v/d}$ with $d\mathbb{Z}_v$ as above, and with this identification it is easily checked that each element of $\hat{\mathcal{D}}[d]$ lies in $\mathscr{S}_k(\mathbb{Z}_{v/d})$. It follows that $\hat{\mathcal{D}}[d]$ is a difference family for a $(v/d, k, 1)C_k^{\rightarrow}$ design based on $\mathbb{Z}_{v/d}$. Moreover $\mathrm{Aut}\,\mathbb{Z}_v$ acting on $d\mathbb{Z}_v$ induces every automorphism of $d\mathbb{Z}_v$, and fixes $\hat{\mathcal{D}}[d]$ setwise. Thus the design corresponding to $\hat{\mathcal{D}}[d]$ admits $\mathrm{Hol}\,(\mathbb{Z}_{v/d})$.

By considering the cases where v/d is prime we obtain strong restrictions on the value of k.

COROLLARY 1.3. *Either k divides $p_i - 1$ for all $i = 1, \dots, r$, or $k = p_1$ and k divides $p_i - 1$ for all $i > 1$.*

https://doi.org/10.1017/S1446788700038246 Published online by Cambridge University Press

PROOF. Choosing $v/d = p_i$ in Lemma 1.2 we obtain a $(p_i, k, 1)C_k^{\to}$ design admitting $\mathrm{Hol}\,(\mathbb{Z}_{p_i})$, and so by [2], either $k = p_i$ or k divides $p_i - 1$. If $k = p_i$ for some i then we must have $k = p_1$, for $k = p_i$, $i \geq 2$, implies that k divides $p_1 - 1$, whereas $p_1 < p_2$.

Theorem 1 will be proved by induction on r. First we deal with the case $r = 1$, that is the case where v is a prime power.

THEOREM 1.4. *Let $\hat{\mathcal{D}}$ be the difference family of a $(p^e, k, 1)C_k^{\to}$ design based on $\mathbb{Z}_{p^e}$ and admitting* $\mathrm{Hol}\,(\mathbb{Z}_{p^e})$, *where p is a prime and e is a positive integer. Then either k divides $p - 1$ or $k = p$. Moreover*

(a) *if k divides $p-1$ then $\hat{\mathcal{D}}$ consists of the k-tuples $p^b j(1, a(b), a(b)^2, \ldots, a(b)^{k-1})$ where $1 \leq j < p^{e-b}$, j is not divisible by p, $a(b)$ has multiplicative order k modulo p^{e-b}, and $0 \leq b < e$.*

(b) *if $k = p$ then either $e = 1$ and $\hat{\mathcal{D}}$ consists of the k-tuples $j(1, 1, \ldots, 1)$ for $1 \leq j \leq p - 1$, or $k = p = 2$, $e \geq 2$ and $\hat{\mathcal{D}}$ consists of the k-tuples $2^b j(1, -1)$ for $1 \leq j < 2^{e-b}$, j odd, and $0 \leq b < e$.*

Conversely each such family of k-tuples is a difference family for a $(p^e, k, 1)C_k^{\to}$ design based on $\mathbb{Z}_{p^e}$ and admitting $\mathrm{Hol}\,(\mathbb{Z}_{p^e})$.

Note that each k-tuple in $\hat{\mathcal{D}}$ is to be identified with all of its cyclic shifts, so for example $p^b(1, a(b), \ldots, a(b)^{k-1}) \equiv p^b a(b)(1, a(b), \ldots, a(b)^{k-1})$.

PROOF. By Corollary 1.3, k either divides $p - 1$ or is equal to p. In the arguments below we shall verify that each of the k-tuples in (a) or (b) lies in $\mathcal{S}_k(\mathbb{Z}_{p^e})$. Then it follows immediately from the Difference Family Criterion that each $\hat{\mathcal{D}}$ as given in the theorem is the difference family of a $(p^e, k, 1)C_k^{\to}$ design based on $\mathbb{Z}_{p^e}$. Clearly each $\phi_{a,0} \in \mathrm{Aut}\,\mathbb{Z}_{p^e}$ fixes $\hat{\mathcal{D}}$ setwise and hence the designs admit $\mathrm{Hol}\,(\mathbb{Z}_{p^e})$. It remains to establish the form of the k-tuples in $\hat{\mathcal{D}}$. Assume first that $k = p$.

If $e = 1$ then the k-tuples in $\hat{\mathcal{D}}$ are the k-tuples $j(1, 1, \ldots, 1)$ for $1 \leq j \leq p - 1$ by [2, Theorem 2.3]. So we may assume that $e \geq 2$. By the Difference Family Criterion there is a unique k-tuple m in $\hat{\mathcal{D}}$ with p^{e-2} as an entry, and, by Lemma 1.1, each entry in m is divisible by p^{e-2} but not by p^{e-1}. Since the sum of the entries in m is zero modulo p^e, and since $k = p$, m is not a constant k-tuple. Thus $m \equiv (p^{e-2}, p^{e-2}a, \ldots)$ for some a not divisible by p, with $2 \leq a < p^2$. Then $\phi_{a,0} \in \mathrm{Aut}\,\mathbb{Z}_{p^e}$, and $m\phi_{a,0}$ has $p^{e-2}a = p^{e-2}\phi_{a,0}$ as an entry, whence $m\phi_{a,0} \equiv m$ and we have $m \equiv p^{e-2}(1, a, a^2, \ldots, a^{p-1})$ and $a^p \equiv 1 \pmod{p^2}$. However $a^p \equiv a \pmod{p}$ and so we must have $a = 1 + bp$ for some $1 \leq b \leq p - 1$. Now the sum of the entries of m is zero modulo p^e, and so $1 + a + \cdots + a^{p-1} \equiv 0 \pmod{p^2}$. However, modulo p^2, $1 + a + \cdots + a^{p-1} = \sum_{0 \leq i \leq p-1}(1 + ibp) = p + bp^2(p - 1)/2$ and this is zero

https://doi.org/10.1017/S1446788700038246 Published online by Cambridge University Press

modulo p^2 if and only if $p = 2$. It follows that every k-tuple in $\hat{\mathcal{D}}$ must be of the form $(j, -j)$ as in part (b).

Thus we may assume that k divides $p - 1$. In particular p is odd. For each $b = 0, \ldots, e - 1$ there is a unique k-tuple m_b in $\hat{\mathcal{D}}$ with p^b as an entry, and each entry of m_b is divisible by p^b but not by p^{b+1} by Lemma 1.1. Since k is not divisible by p, m_b is not a constant k-tuple, so $m_b \equiv (p^b, p^b a, \ldots)$ where a, which may depend on b, is not divisible by p, and $a \not\equiv 1 \pmod{p^{e-b}}$. Then $\phi_{a,0} \in \operatorname{Aut} \mathbb{Z}_{p^e}$ and $m\phi_{a,0} \equiv m$ since $m\phi_{a,0}$ has $p^b a = p^b \phi_{a,0}$ as an entry. It follows that $m = p^b(1, a, \ldots, a^{k-1})$ and $a^k \equiv 1 \pmod{p^{e-b}}$. Suppose that $a = 1 + cp$ for some c. Then the sum of the entries in m, modulo p^{b+1}, is $p^b k$, and this contradicts the fact that $m \in \mathscr{S}_k(\mathbb{Z}_{p^e})$. Thus $a \not\equiv 1 \pmod{p}$. Then the sum of the first t entries of m is $p^b(a^t - 1)/(a - 1)$ and this is zero modulo p^e if and only if $a^t \equiv 1 \pmod{p^{e-b}}$, since $a - 1$ is not divisible by p. Since $m \in \mathscr{S}_k(\mathbb{Z}_{p^e})$ the element a must have order k modulo p^{e-b}. Thus m_b is of the required form. Finally, since $\hat{\mathcal{D}}$ is invariant under $\operatorname{Hol}(\mathbb{Z}_{p^e})$, $\hat{\mathcal{D}}$ contains $p^b j(1, a, \ldots, a^{k-1})$ for all j not divisible by p. Thus $\hat{\mathcal{D}}$ is as in part (a), and the proof of Theorem 1.4 is complete.

Now we shall complete the proof of Theorem 1. It is easily verified that the Difference Family Criterion holds for the set of k-tuples given in (b) so that $\hat{\mathcal{D}}$, as given in (b), is the difference family for a $(v/d, k, 1)C_k^{\rightarrow}$ design based on $G = \mathbb{Z}_v$, and this design admits $\operatorname{Hol}(G)$. Also the restrictions on the values of k follow from Corollary 1.3. It remains to establish that the k-tuples in $\hat{\mathcal{D}}$ must be of the form given in (b). If $v = p_1^{e_1} \ldots p_r^{e_r}$ with $r = 1$ then part (b) follows from Theorem 1.4. So we may assume that $r \geq 2$ and that part (b) holds for integers v' with less than r distinct prime divisors. Let $m \in \hat{\mathcal{D}}$. If $I(m)$, as defined just before Lemma 1.1, is a proper subset of $\{1, \ldots, r\}$ then, by Lemma 1.2, m lies in $\hat{\mathcal{D}}[d]$, where $d = d(m)$, and $\hat{\mathcal{D}}[d]$ is a difference family for a $(v/d, k, 1)C_k^{\rightarrow}$ design based on $\mathbb{Z}_{v/d} \cong d\mathbb{Z}_v$ admitting $\operatorname{Hol}(\mathbb{Z}_{v/d})$. By induction it follows that $m \equiv dj(1, a, \ldots, a^{k-1})$ for some j such that $(dj, v) = d$ and some a with multiplicative order k modulo v/d. Moreover, since $\hat{\mathcal{D}}$ is fixed setwise by $\operatorname{Hol}(\mathbb{Z}_v)$, it follows that every $m' \in \hat{\mathcal{D}}$ with $d(m') = d$ is of the form $m' \equiv dj'(1, a, \ldots, a^{k-1})$ with the same a. Thus these k-tuples are of the required form, and so we may assume that $I(m) = \{1, \ldots, r\}$, that is, writing $d = d(m)$, that v/d is divisible by $p_1 \ldots p_r$. Consider first the k-tuple m with d as an entry. We shall show that $m = d(1, a, \ldots, a^k)$ for some a with multiplicative order k modulo v/d. Then, as $\hat{\mathcal{D}}$ is fixed setwise by $\operatorname{Hol}(\mathbb{Z}_v)$, all other $m' \in \hat{\mathcal{D}}$ with $d(m') = d$ are of the form $m' \equiv dj(1, a, \ldots, a^{k-1})$ for some j such that $1 \leq j < v/d$, $(jd, v) = d$, and with the same a. Note that m is not the constant k-tuple $(d, d, \ldots, d)$ since the sum of the entries of $(d, d, \ldots, d)$ is kd which is not zero modulo v since $k \leq p_1$ and v/d is divisible by $p_1 \ldots p_r$. Thus we have $m \equiv (d, da, \ldots)$ where $(da, v) = d$, and $a \not\equiv 1 \pmod{v/d}$. Moreover, as each p_i divides v/d, we must have $(a, v) = 1$,

https://doi.org/10.1017/S1446788700038246 Published online by Cambridge University Press

so $\phi_{a,0} \in \operatorname{Aut}(G)$ and $m\phi_{a,0} \in \hat{\mathcal{D}}$. As $da = d\phi_{a,0}$ is an entry of $m\phi_{a,0}$ we have $m\phi_{a,0} = m$ and it follows that $m = d(1, a, \ldots, a^{k-1})$ and $a^k \equiv 1 \pmod{v/d}$. Suppose that $(a-1, v) \neq 1$, so that $a = 1 + cp_i$ for some $1 \leq i \leq r$, and $c \not\equiv 0 \pmod v$. Let the power of p_i dividing d be p_i^f, so $f + 1 \leq e_i$. Then, modulo p_i^{f+1}, the sum of the entries of m is dk. Since this sum is zero modulo v it follows that p_i divides k whence $k = p_1$. In this case since k is prime and m is not a constant k-tuple, m must have period k whence a must have order k modulo v/d. On the other hand, if $(a-1, v) = 1$ then the sum of the first t entries of m, namely $d(a^t - 1)/(a-1)$, is zero modulo v if and only if $a^t \equiv 1 \pmod{v/d}$, and again a must have order k modulo v/d. Thus in this case also the k-tuples are of the required form, and the proof of Theorem 1 is complete.

2. Designs based on groups admitting an automorphism with small centralizer.

In this section we classify all balanced directed cycle designs based on a group G and admitting an automorphism σ of G such that the centralizer of σ in G is cyclic of order 2 or 4.

THEOREM 2.1. *Let G be a group of order v and σ an automorphism of G such that the centralizer in G of σ is a cyclic subgroup of order 2 or 4. If $\hat{\mathcal{D}}$ is the difference family of a $(v, k, 1)C_k^{\rightarrow}$ design based on G and admitting $\langle\sigma\rangle$, then $k = 2$ and $\hat{\mathcal{D}} = \{(g, g^{-1}) \mid g \in G \setminus \{1\}\}$.*

Before presenting the proof of this theorem we note that there are many examples of groups G admitting automorphisms of this type. Any even ordered abelian group has such an automorphism, and so do many non-abelian groups, for example dihedral or generalized quaternion groups with order divisible by 4.

PROOF. Let $H = \langle h \rangle$ be the subgroup of G centralized by σ. There is a unique element m in $\hat{\mathcal{D}}$ with h as an entry. Then, as m^σ also has $h^\sigma = h$ as an entry, $m^\sigma = m$ and all of the entries of m lie in $H \setminus \{1\}$. Suppose first that H has order 2. Then, as $m \in \mathcal{S}_k(G)$, we must have $k = 2$ and $m = (h, h)$. For any $g \in G \setminus \{1\}$ it follows that the element of $\hat{\mathcal{D}}$ with g as an entry is (g, g^{-1}) as required.

Suppose now that H has order 4. If all three elements of $H \setminus \{1\}$ are entries of m then m has period 3, but in m, cyclically ordered, there are adjacent entries h, h^3 or h^3, h with product 1 contradicting the fact that $m \in \mathcal{S}_k(G)$. Thus not all elements of $H \setminus \{1\}$ occur as entries of m. If h and h^3 occur in m then $k = 2$ and $m = (h, h^3)$. In this case $\hat{\mathcal{D}} = \{(g, g^{-1}) \mid g \in G \setminus \{1\}\}$ as in the theorem. If h and h^2 occur as entries of m then a second element m' of $\hat{\mathcal{D}}$ has all its entries equal to h^3. As $m' \in \mathcal{S}_k(G)$ we conclude that $k = 4$, while $m \in \mathcal{S}_k(G)$ implies that $k = 8$. Thus

https://doi.org/10.1017/S1446788700038246 Published online by Cambridge University Press

we may assume that $m = (h, h, h, h)$, $k = 4$, and similarly that a second element of $\hat{\mathcal{D}}$ is (h^3, h^3, h^3, h^3). But then a third element of $\hat{\mathcal{D}}$ has all entries equal to h^2, and $(h^2, h^2, h^2, h^2) \notin \mathcal{S}_k(G)$. This contradiction completes the proof of the theorem.

It is easy to get fairly strong information about the difference sets in other cases, but we do not get a complete classification. For example if the centralizer in G of σ is $Z_2 \times Z_2$ then similar arguments show that either $\hat{\mathcal{D}}$ is the difference set in Theorem 2.1, or $k = 3$. However we do not know when such difference sets with $k = 3$ exist.

References

[1] J. C. Bermond and D. Sotteau, 'Graph decompositions and G-designs', *Proceedings of the Fifth British Combinatorial Conference, Cong. Numer.* **15** (1975), 53–72.

[2] N. Brand and W. C. Huffman, 'Mendelsohn designs admitting the affine group', *Geom. Dedicata* **22** (1987), 173–196.

[3] P. Hell and A. Rosa, 'Graph decompositions, handcuffed prisoners and balanced P-designs', *Discrete Math.* **2** (1972), 229–252.

[4] C. E. Praeger, 'Balanced directed cycle designs based on groups', *Discrete Math.* **92** (1991), 275–290.

Faculty of Science
Department of Mathematics
Prince of Songkla University
Haad Yai
Thailand

Department of Mathematics
University of Western Australia
Nedlands WA 6907
Australia

https://doi.org/10.1017/S1446788700038246 Published online by Cambridge University Press