A NEW TECHNIQUE FOR CONSTRUCTING PAIRWISE BALANCED DESIGNS FROM GROUPS

A. Abdollahi*
Department of Mathematics, University of Isfahan, Isfahan, and Institute for Studies in Theoretical Physics and Mathematics (IPM), Tehran, Iran.

H. R. Maimani
Center of Excellence in Biomathematics, School of Mathematics, Statistics, and Computer Science, University of Tehran, and Institute for Studies in Theoretical Physics and Mathematics (IPM), Tehran, Iran.

ABSTRACT. We introduce a new technique for constructing pairwise balanced designs and group divisible designs from finite groups. These constructed designs do not give designs with new parameters but our construction gives rise to designs having a transitive automorphism group that also preserves the resolution classes.

1. INTRODUCTION

The purpose of this paper is to introduce a new technique for constructing pairwise balanced designs (PBDs) and group divisible designs (GDDs) from some constructions in group theory. First we state the necessary definitions.

Let K be a subset of positive integers and let λ be a positive integer. A *pairwise balanced design* ($PBD(v,K;\lambda)$ or $(K,\lambda)-PBD$) of order v with block sizes from K is a pair $(\mathcal{V},\mathcal{B})$ where $\mathcal{V}$ is a finite set (the *point set*) of cardinality v and $\mathcal{B}$ is a family of subsets (*blocks*) of $\mathcal{V}$ which satisfy the properties:
1. If $B \in \mathcal{B}$, then $|B| \in K$.
2. Every pair of distinct elements of $\mathcal{V}$ occurs in exactly λ blocks of $\mathcal{B}$.
If $\lambda = 1$, $PBD(v,K)$ is used for $PBD(v,K,1)$.

Key words and phrases. pairwise balanced design; group divisible design; partitioned groups.

Mathematics Subject Classification: 05B05.

*Corresponding author: a.abdollahi@math.ui.ac.ir.

The research of the first author was in part supported by a grant from IPM (No. 84200036). The research of the second author was in part supported by a grant from IPM (No. 84050115).

The pairwise balanced design $(\mathcal{V}, \mathcal{B})$ is called *resolvable* if the block-set $\mathcal{B}$ is partitioned into classes so that each element of $\mathcal{V}$ occurs exactly once amongst the blocks of each class. Such a partition is called a *resolution* for the PBD.

Let K and G be sets of positive integers and let λ be a positive integer. A *group divisible design of index* λ *and order* v (a $(K,\lambda)-GDD$) is a triple $(\mathcal{V}, \mathcal{G}, \mathcal{B})$, where $\mathcal{V}$ is a finite set of cardinality v, $\mathcal{G}$ is a partition of $\mathcal{V}$ into parts (*groups*) whose sizes lie in G, and $\mathcal{B}$ is a family of subsets (*blocks*) of $\mathcal{V}$ which satisfy the properties:
1. If $B \in \mathcal{B}$ then $|B| \in K$.
2. Every pair of distinct elements of $\mathcal{V}$ occurs in exactly λ blocks or one group, but not both.
3. $|\mathcal{G}| > 1$.
If $\lambda = 1$, we write $K-GDD$ simply for $(K,1)-GDD$. If $v = a_1g_1 + a_2g_2 + \cdots + a_sg_s$, and if there are a_i groups of size g_i, $i = 1, 2, \ldots, s$, then we say the $(K,\lambda) - GDD$ is of type $g_1^{a_1}g_2^{a_2}\cdots g_s^{a_s}$.

One may consult [2, Part III, pp. 185-228] for a description of known PBDs and GDDs by 1996. Also, to see some new results on this area, the following web address may be useful
`http://www.emba.uvm.edu/~dinitz/newresults.html`

Let G be a finite group. A set $\mathcal{A}$ of non-trivial subgroups of G is called a *partition* for G if $G = \bigcup \mathcal{A}$ and for every two distinct members H and K of $\mathcal{A}$ we have $H \cap K = 1$. The partition $\mathcal{A}$ is called *non-trivial* if $|\mathcal{A}| > 1$. The reader may consult [5] as a survey on partitioned groups. For further possible undefined notation we refer the reader to [2].

Our main tools for construction PBDs and GDDs are the following:

Theorem 1.1. *Suppose that G is a finite group having a non-trivial partition $\mathcal{A}$. If $\mathcal{B} = \{xH \mid H \in \mathcal{A},\ \ x \in G\}$ and $\mathcal{R} = \{\{xH \mid x \in G\} \mid H \in \mathcal{A}\}$, then $(G, \mathcal{B})$ is a resolvable $PBD(|G|, K)$, where $K = \{|H| \mid H \in \mathcal{A}\}$ and $\mathcal{R}$ is a resolution. Moreover, the automorphism group $(G, \mathcal{B})$ contains a subgroup isomorphic to G which acts transitively on both the point-set G and the block-set $\mathcal{B}$, also it preserves the resolution classes.*

Theorem 1.2. *Suppose that G is a finite group having a non-trivial partition $\mathcal{A}$. Let $\mathcal{B} = \{xH \mid xH \neq H \in \mathcal{A},\ \ x \in G\}$ and $\mathcal{V} = G\backslash\{1\}$ and $\mathcal{G} = \{H\backslash\{1\} \mid H \in \mathcal{A}\}$. Then $(\mathcal{V}, \mathcal{G}, \mathcal{B})$ is a $K - GDD$, where $K = \{|H| \mid H \in \mathcal{A}\}$.*

In the next section we prove and use these results to construct PBDs and GDDs.

2. Proofs of main tools and constructions

Proof of Theorem 1.1. Let $x, y \in G$. Since $G = \bigcup \mathcal{A}$, $x^{-1}y \in H$ for some $H \in \mathcal{A}$. It follows that $x, y \in xH$. Now assume that $H, K \in \mathcal{A}$ such that $x, y \in aH \cap bK$ for some $a, b \in G$. Then $xH = yH$ and $xK = yK$. These equalities imply that $x^{-1}y \in H \cap K$. Now if $x \neq y$, then $H = K$, since $\mathcal{A}$ is a partition for G. It follows that $aH = bK$, as required. Each member of $\mathcal{R}$ is the set of left cosets of a subgroup, so it partitions G as a set. Thus $\mathcal{R}$ is a resolution.
The last part is clear since G acts on both G and $\mathcal{B}$ by left multiplication. This completes the proof. □

Proof of Theorem 1.2. Let $x, y \in \mathcal{V}$. Since $\mathcal{A}$ is a partition for G, $\mathcal{G}$ partitions G as a set. Now let x, y be two distinct elements of $\mathcal{G}$ and assume that x, y are not both in one $H \in \mathcal{A}$. Then, as the proof of Theorem 1.1 shows, the elements x, y belong to aL for some $L \in \mathcal{A}$ and $a \in G$. But $aL \neq L$, since otherwise x, y are simultaneously in a member of $\mathcal{A}$. On the other hand, as the proof of Theorem 1.1 shows, the elements x, y cannot both belong to a member of $\mathcal{B}$ and $\mathcal{G}$. This completes the proof. □

In the following we use Theorems 1.1 and 1.2 to construct PBDs and GDDs which are not perhaps of new parameters, but what we want to emphasis on it is that the constructed resolvable PBDs have a transitive automorphism group that also preserves the resolution classes.

Recall that a finite group G is called a *Frobenius group* if it contains a subgroup H with the property that $H^g \cap H = 1$ for all $g \in G \backslash H$. Such a subgroup H of a Frobenius group G is called a *Frobenius complement.* Also it is well-know (see e.g. [3]) that in a Frobenius group G with a Frobenius complement H, the set $N := G \backslash \left(\bigcup_{g \in G} H^g \right) \cup \{1\}$ is a normal subgroup of G, called *Frobenius kernel* of G.

Theorem 2.1. *Let n and t be two positive integers such that there is a Frobenius group G with Frobenius kernel F and complement K with $|F| = n$ and $|K| = t$. Then there exist a resolvable PBD$(nt, \{n, t\})$ and a $\{n, t\} - GDD$ of type $(n-1)^1(t-1)^n$. Moreover, the automorphism group of this resolvable PBD is transitive on both the point-set and block-set and it preserves the resolution classes.*

Proof. We know that the set of all conjugates of K in G with the subgroup F form a partition of G (see [3, Satz 8.17, p. 506]). Now Theorems 1.1 and 1.2 complete the proof. □

Remark 2.2. Note that if n and t are two positive integers having the property stated in Theorem 2.1, then t divides $n-1$ (see [3, Satz 8.3, p. 497]). For every odd prime p, $\mathrm{Hol}(C_p)$ (the holomorph of the cyclic group of order p) is a Frobenius group with kernel and complement size p and $p-1$, respectively. Thus, by Theorem 2.1, there exist a resolvable $PBD(p^2-p,\{p,p-1\})$ and a $\{p,p-1\}-GDD$ of type $(p-1)^1(p-2)^p$ (of course it is well known that a $PBD(p^2-p,\{p,p-1\})$ can be obtained from a resolvable $TD(p-1,p)$, and that a $\{p,p-1\}-GDD$ of type $(p-1)^1(p-2)^p$ can be obtained by deleting one point from it and using this point to redefine groups). More generally we know for which pair of positive integers f and k there is a Frobenius group with Frobenius kernel and complement of sizes f and k, respectively. This is a result due to Boykett [1]. By definition, a pair (N,Φ) of groups is called a *Ferrero pair* if Φ is a fixed point free group of automorphisms of the group N. It follows that the semidirect product $N \rtimes \Phi$ is a Frobenius group.

Theorem 2.3. (Boykett, [1, Theorem 1]) *Let n,t be positive integers, $n=\prod p_i^{e_i}$ the prime factorization of n; then there exists a Ferrero pair (N,Φ) with $n=|N|$ and $t=|\Phi|$ iff t divides $p_i^{e_i}-1$ for all i.*

Theorem 2.4. *Let n,t be positive integers such that t divides $p_i^{e_i}-1$ for all i where $n=\prod p_i^{e_i}$ be the prime factorization of n. Then there exist a resolvable $PBD(nt,\{n,t\})$ and a $\{n,t\}-GDD$ of type $(n-1)^1(t-1)^n$. The automorphism group of this resolvable PBD is transitive on both the point-set and block-set and it preserves the resolution classes.*

Proof. It follows from Theorems 2.1 and 2.3. □

Remark 2.5. In Theorem 2.4 the condition that t divides $p_i^{e_i}-1$ for all i is weak (existence of $TD(t,n)$ is a sufficient condition, and the theorem is generally not true if we remove this condition). We again emphasize on the specific structure of automorphism groups of the constructed designs.

Let q be a prime power. We denote by $\mathrm{PGL}(2,q)$ and $\mathrm{PSL}(2,q)$ the projective general (special, respectively) linear group of degree 2 over the finite field of order q.

Theorem 2.6. *Let q be an arbitrary prime power greater than 3 and $k = \gcd(2,q-1)$. Then there exist resolvable*

$$PBD(\frac{q(q^2-1)}{k},\{\frac{q-1}{k},q,\frac{q+1}{k}\}) \text{ and } PBD(q(q^2-1),\{q-1,q,q+1\})$$

and

$$\{\frac{q-1}{k},q,\frac{q+1}{k}\}-GDD \text{ and } \{q-1,q,q+1\}-GDD$$

of type

$$(\frac{q-1-k}{k})^{\frac{(q+1)q}{2}}(q-1)^{q+1}(\frac{q+1-k}{k})^{\frac{(q-1)q^2}{2}}$$

and

$$(q-2)^{\frac{(q+1)q}{2}}(q-1)^{q+1}q^{\frac{(q-1)q^2}{2}}$$

respectively. The automorphism group of this resolvable PBD is transitive on both the point-set and block-set and it preserves the resolution classes.

Proof. Let $q = p^n$ where p is a prime number and $n > 0$. The group $\mathrm{PGL}(2,q)$ (resp. $\mathrm{PSL}(2,q)$) has a partition $\mathcal{P}$ consisting of $q+1$ Sylow p-subgroups, $\frac{(q+1)q}{2}$ cyclic subgroups of order $q-1$ (resp. $\frac{q-1}{k}$) and $\frac{(q-1)q^2}{2}$ cyclic subgroups of order $q+1$ (resp. $\frac{q+1}{k}$) (see pp. 185–187 and p. 193 of [3]). Now Theorems 1.1 and 1.2 complete the proof. □

Theorem 2.7. *Let m be an arbitrary positive integer and $q = 2^{2m+1}$ and $r = 2^m$. Then there exist a resolvable*

$$PBD(q^2(q^2+1)(q-1),\{q-2r+1,q-1,q^2,q+2r+1\})$$

and a

$$\{q-2r+1,q-1,q^2,q+2r+1\}-GDD$$

of type

$$(q-2r)^{\frac{q^2(q-1)(q+2r+1)}{4}}(q-2)^{\frac{(q^2+1)q^2}{2}}(q^2-1)^{q^2+1}(q+2r)^{\frac{q^2(q-1)(q-2r+1)}{4}}.$$

Moreover, the automorphism group of this resolvable PBD is transitive on both the point-set and block-set and it preserves the resolution classes.

Proof. Let G be the Suzuki group $Sz(q)$. By [4, Theorems 3.10 and 3.11, pp. 192–193] G has a partition consisting of $\frac{q^2(q-1)(q+2r+1)}{4}$ $(\frac{(q^2+1)q^2}{2}, \frac{q^2(q-1)(q-2r+1)}{4}, q^2+1$ respectively) subgroups of orders $q-2r+1, q-1, q+2r+1, q^2$. Since $|Sz(q)| = q^2(q^2+1)(q-1)$, Theorems 1.1 and 1.2 complete the proof. □

Remark 2.8. It seems that Theorem 2.7 could possibly be a new result. We are unable to demonstrate the use of these PBDs in some problems that are of central to design theorist.

References

[1] T. Boykett, Construction of Ferrero pairs of all possible orders, SIAM J. Discrete Math. 14 (2001), 283–285.

[2] The CRC handbook of combinatorial designs. Edited by Charles J. Colbourn and Jeffrey H. Dinitz. CRC Press Series on Discrete Mathematics and its Applications. CRC Press, Boca Raton, FL, 1996.

[3] B. Huppert, *Endliche Gruppen I*, Springer-Verlag, Berlin, 1967.

[4] B. Huppert and N. Blackburn, *Finite groups III*, Springer-Verlag, Berlin, 1982.

[5] G. Zappa, Partitions and other coverings of finite groups, Illinois J. Math. 47 (2003), 571–580.