From a 1-rotational RBIBD to a Partitioned Difference Family *

Marco Buratti
Dipartimento di Matematica e Informatica
Università di Perugia, I-06123, Italy
buratti@mat.uniroma1.it

Jie Yan and Chengmin Wang
School of Science
Jiangnan University, Wuxi 214122, China
wcm@jiangnan.edu.cn

Submitted: Nov 16, 2008; Accepted: Sep 15, 2010; Published: Oct 22, 2010
Mathematics Subject Classification: 05B05, 05E18

Abstract

Generalizing the case of $\lambda = 1$ given by Buratti and Zuanni [*Bull Belg. Math. Soc.* (1998)], we characterize the 1-*rotational difference families* generating a 1-rotational (v, k, λ)-RBIBD, that is a (v, k, λ) *resolvable balanced incomplete block design* admitting an automorphism group G acting sharply transitively on all but one point ∞ and leaving invariant a resolution $\mathcal{R}$ of it. When G is transitive on $\mathcal{R}$ we prove that removing ∞ from a parallel class of $\mathcal{R}$ one gets a *partitioned difference family*, a concept recently introduced by Ding and Yin [*IEEE Trans. Inform. Theory*, 2005] and used to construct *optimal constant composition codes*. In this way, by exploiting old and new results about the existence of 1-rotational RBIBDs we are able to derive a great bulk of previously unnoticed partitioned difference families. Among our RBIBDs we construct, in particular, a $(45, 5, 2)$-RBIBD whose existence was previously in doubt.

Keywords. 1-rotational RBIBD; 1-rotational difference family; partitioned difference family; constant composition code.

1 Introduction

Throughout the paper, every union will be understood as *multiset union*. The union of μ copies of a multiset A will be denoted by ${}^{\mu}A$. Of course ${}^{\mu}A$ has a different meaning from ${}^{\mu}\{A\}$; as an example, if $A = \{a, b, c\}$, then ${}^{2}A = \{a, a, b, b, c, c\}$ while ${}^{2}\{A\} =$

*Research is supported by NSFCs under Grant No. 10801064 and 11001109, Tianyuan Mathematics Foundation of NSFC under Grant No. 10926103, Jiangnan University Foundation under Grant No. 2008LQN013 and Program for Innovative Research Team of Jiangnan University.

$\{\{a,b,c\},\{a,b,c\}\}$. Given some integers k_1, ..., k_t, sometimes we will write $[^{\mu_1}k_1, ..., {}^{\mu_t}k_t]$ instead of ${}^{\mu_1}\{k_1\} \cup ... \cup {}^{\mu_t}\{k_t\}$. As usual, the list of differences of a subset B of an additive group G will be denoted by ΔB.

A *difference family* in a group G that is *relative* to a subgroup N of G is a collection $\mathcal{F}$ of subsets of G (*base blocks*) whose lists of differences are disjoint with N and cover, altogether, every element of $G-N$ a constant number λ of times: $\bigcup_{B\in\mathcal{F}} \Delta B = {}^{\lambda}(G-N)$. If K is the multiset of block sizes of $\mathcal{F}$ one briefly says that $\mathcal{F}$ is a (G,N,K,λ)-DF. We write (G,K,λ)-DF instead of $(G,\{0\},K,\lambda)$-DF, and (G,N,k,λ)-DF instead of $(G,N,[^{\mu}k],\lambda)$-DF whatever is μ. Thus, a (G,k,λ)-DF is a collection of k-subsets of G whose differences cover every non-zero element of G exactly λ times.

Speaking of a (v,n,K,λ)-DF we mean a (G,N,K,λ)-DF where $G=\mathbf{Z}_v$ and N is the subgroup of $\mathbf{Z}_v$ of order n, namely $N=\frac{v}{n}\mathbf{Z}_v$. We recall, in particular, that a $(v,n,k,1)$-DF can be viewed as a special kind of *optical orthogonal code* that is called *n-regular* in [37] and that is *optimal* in the case that $n \leqslant k(k-1)$.

A (v,N,K,λ)-DF is said to be *disjoint* (DDF for short) when its base blocks are mutually disjoint. If, in addition, none of them meets N we will speak of a *strictly disjoint* difference family and we will write SDDF instead of DDF. There is a number of papers concerning DDFs with constant block size; in particular, it was proved the existence of a $(v,3,1)$-DDF for any $v\equiv 1 \pmod 6$ [24], the existence of a $(v,3,3,1)$-SDDF for any $v\equiv 3 \pmod 6$ [25, 14] and the existence of a $(\mathbb{F}_q,4,\lambda)$-DDF for any admissible pair (q,λ) with $\lambda\leqslant 2$ [36] where $\mathbb{F}_q$ denotes the elementary abelian group of order q. We also observe that any *radical* $(\mathbb{F}_q,k,1)$-DF (see [9]) with k odd is a DDF.

A (G,K,λ)-DF whose base blocks partition the whole group G is defined to be *partitioned* (PDF). This concept was recently introduced by Ding and Yin and used to construct optimal constant composition codes [22, 38]. It is clear that every PDF is disjoint but not strictly disjoint since it is relative to $N=\{0\}$ and, by definition, there is a base block of the family containing 0.

It is very elementary to see that every DDF gives rise to a PDF if we allow to have some base blocks of size one. It is also trivial to see that a PDF having all blocks of the same size cannot exist. What about PDFs having exactly two block sizes? As an easy example we have all pairs $\{D,\overline{D}\}$ with D a *difference set* (see [8]) and $\overline{D}$ its complement; if D has parameters (v,k,λ), the resultant PDF has parameters $(v,[k,v-k],v-2k+2\lambda)$. Thus, for instance, the so called $(2k-1,k-1,\frac{k}{2}-1)$ *Paley difference set* gives rise to a $(2k-1,[k-1,k],k-1)$-PDF.

In this paper we focus our attention to PDFs having, as in the above example, exactly two block sizes $k-1$ and k. We first show that such PDFs necessarily have exactly one block of size $k-1$.

Proposition 1.1 *If there exists a $(v,[^x(k-1),{}^yk],\lambda)$-PDF with $x\neq 0\neq y$, we necessarily have $v\equiv -1 \pmod k$, $x=1$, $y=(v-k+1)/k$ and $\lambda=k-1$.*

Proof. By definition of a PDF we must have

$$(k-1)(k-2)x+k(k-1)y=\lambda[(k-1)x+ky-1].$$

Solving this identity with respect to x we obtain

$$x = \frac{ky(k-1) - \lambda(ky-1)}{(k-1)(\lambda-k+2)} = \frac{ky+\lambda}{(k-1)(\lambda-k+2)} - \frac{ky}{k-1}.$$

Thus $\lambda-k+2$ is positive, that is $\lambda > k-2$, otherwise x would be negative. If $\lambda = k-1$, we see that $x = 1$. Now assume that $x > 1$ so that, consequently, $\lambda \geqslant k$. In this case we have $ky(k-1)-\lambda(ky-1) > (k-1)(\lambda-k+2)$ which implies $ky(k-1)-\lambda y(k-1) > (k-1)(\lambda-k+2)$ since it is obvious that $\lambda(ky-1) \geqslant \lambda y(k-1)$. Dividing by $k-1$ we get $(k-\lambda)y > \lambda-k+2$, namely $(k-\lambda)(y+1) > 2$, that is absurd since $k-\lambda \leqslant 0$. The assertion easily follows.□

In view of the above proposition there is no ambiguity in speaking of a $(v, \{k-1, k\}, k-1)$-PDF without specifying the multiplicity of $k-1$ and k in the multiset of block-sizes. Besides *starters* (see [23]), that can be equivalently viewed as $(2n+1, \{1,2\}, 1)$-PDFs, there are other combinatorial designs such as **Z**-*cyclic whist tournaments* and **Z**-*cyclic generalized whist tournaments* [7] that are strictly related with PDFs. For instance, any **Z**-cyclic whist tournament of order $4t$ (briefly Wh$(4t)$) can be seen as a partition of $\mathbf{Z}_{4t-1} \cup \{\infty\}$ into t ordered quadruples such that every non-zero element of $\mathbf{Z}_{4t-1}$ can be expressed as a *partner* (resp. *opponent*) difference of some quadruples in exactly one (resp. two) ways, where the partner differences of a quadruple (x_1, x_2, x_3, x_4) are $\pm(x_1 - x_3)$ and $\pm(x_2 - x_4)$, while the opponent differences are all the remaining ones. It is then clear that a **Z**-cyclic Wh$(4t)$ determines a $(4t-1, \{3,4\}, 3)$-PDF though the converse is not generally true.

In general, for a deep study of $(v, \{k, k-1\}, k-1)$-PDFs we have to focus our attention on 1-*rotational resolvable balanced incomplete block designs* that we are going to define below. First recall that a (v, k, λ)-BIBD is a pair $(V, \mathcal{B})$ where V is a set of v *points* and $\mathcal{B}$ is a collection of k-subsets of V (*blocks*) such that each pair of distinct points of V occurs in exactly λ blocks. Such a BIBD is *resolvable* if there exists a partition $\mathcal{R}$ of $\mathcal{B}$ (*resolution*) into classes (*parallel classes*) each of which is a partition of V. In this paper, speaking of a (v, k, λ)-RBIBD we mean a *resolved* (v, k, λ)-BIBD, i.e., a triple $(V, \mathcal{B}, \mathcal{R})$ such that $(V, \mathcal{B})$ is a resolvable (v, k, λ)-BIBD admitting $\mathcal{R}$ as a specific resolution of it.

An automorphism group of a BIBD or RBIBD as above is a group of permutations on V leaving invariant $\mathcal{B}$ or $\mathcal{R}$, respectively. In particular, a BIBD or RBIBD is said to be 1-*rotational* under G if it admits G as an automorphism group fixing one point and acting sharply transitively on the others.

In this paper we characterize 1-rotational (v, k, λ)-RBIBDs with an arbitrary λ in terms of 1-*rotational difference families*, generalizing the important case of $\lambda = 1$ that was treated in [17]. We will prove that a 1-rotational (v, k, λ)-RBIBD under a group G acting transitively on its resolution is completely equivalent to a $(v, \{k-1, k\}, k-1)$-PDF. In this way, exploiting old and new results on 1-rotational RBIBDs we are able to give constructions of many infinite classes of $(v, \{k-1, k\}, k-1)$-PDFs. In particular, we establish that for any $k > 1$ there are infinitely many values of v for which there exists a 1-rotational $(v, k, 1)$-RBIBD and, consequently, a $(v, \{k-1, k\}, k-1)$-PDF.

We finally point out that in Example 2.9 we give a $(45, 5, 2)$-RBIBD. We emphasize this fact since, up to now, no RBIBD with this parameters was known.

2 Resolvable 1-rotational difference families

From now on, G is an additive (but not necessarily abelian) group and ∞ is a symbol not in G. It will be understood that the action of G on $G \cup \{\infty\}$ is the addition on the right under the rule that $\infty + g = \infty$ for every $g \in G$.

For a given collection $\mathcal{P}$ of subsets of $G \cup \{\infty\}$, the G-stabilizer of $\mathcal{P}$ is the subgroup $G_{\mathcal{P}}$ of G of all elements g such that $B + g = B$. The *G-orbit* of $\mathcal{P}$ is the set $\mathcal{P}^G$ of all distinct translates of $\mathcal{P}$. In the case that $\mathcal{P} = \{B\}$ is a singleton we will write G_B and B^G rather than $G_{\{B\}}$ and $\{B\}^G$. We say that B is *full* when its G-orbit has full length $|G|$, i.e., when $G_B = \{0\}$. Observe that B is union of left cosets of G_B and possibly $\{\infty\}$. It follows, in particular, that if the size of $B - \{\infty\}$ is coprime with the order of G, then B is full.

Given $B \subset G$, it is easy to see that we have $\Delta B = {}^{|G_B|}\partial B$ for a suitable multiset ∂B that is defined to be the *list of partial differences of B*. The definition is extended to subsets of $G \cup \{\infty\}$ by setting $\partial(B \cup \{\infty\}) = \partial B \cup {}^{|B|/|G_B|}\{\infty\}$. Up to isomorphism, $(V, \mathcal{B})$ is a 1-rotational (v, k, λ)-BIBD under G if $V = G \cup \{\infty\}$ and $\mathcal{B} = \bigcup_{B \in \mathcal{F}} B^G$ for a suitable collection $\mathcal{F} \subset \mathcal{B}$ that is called a 1-*rotational* (G, k, λ) *difference family*. As pointed out in [2], a collection $\mathcal{F}$ of k-subsets of $G \cup \{\infty\}$ is a 1-rotational (G, k, λ) difference family if and only if $\bigcup_{B \in \mathcal{F}} \partial B$ covers exactly λ times all non-zero elements of $G \cup \{\infty\}$.

Definition 2.1 *We say that a 1-rotational (G, k, λ) difference family $\mathcal{F}$ is* resolvable *if it is partitionable into subfamilies $\mathcal{F}_1$, ..., $\mathcal{F}_t$ each of which is of the form:*

$$\mathcal{F}_i = {}^{|G_{A_i}:N_i|}\{A_i\} \cup \{B_{ij} \mid 1 \leqslant j \leqslant \ell_i\}$$

with

$G_{\mathcal{F}_i} = \{0\}$, $\infty \in A_i$, $N_i \leqslant G_{A_i}$, $\ell_i = \frac{|G|-k+1}{k|N_i|}$, $G_{B_{ij}} = \{0\}$ *for* $1 \leqslant j \leqslant \ell_i$,

$\bigcup_{j=1}^{\ell_i} B_{ij}$ *is a complete system of representatives for the left cosets of N_i in G that are not contained in A_i.*

Every partition $\mathcal{F} = \mathcal{F}_1 \cup ... \cup \mathcal{F}_t$ with the $\mathcal{F}_i$'s as above will be said a resolution *of $\mathcal{F}$.*

The following theorem generalizes Theorem 2.1 in [17]

Theorem 2.2 *There exists a 1-rotational (v, k, λ)-RBIBD under G if and only if there exists a resolvable 1-rotational (G, k, λ)-DF.*

Proof. ($\Longrightarrow$) Let $\mathcal{D} = (V, \mathcal{B}, \mathcal{R})$ be a 1-rotational (v, k, λ)-RBIBD under G. Of course v is a multiple of k so that the order of G, that is $v - 1$, is necessarily coprime with k. It follows that any block B of $\mathcal{D}$ not passing through ∞ is full, i.e., with trivial G-stabilizer.

Let $\{\mathcal{P}_1, ..., \mathcal{P}_t\}$ be a complete system of representatives for the G-orbits of the parallel classes of $\mathcal{R}$. Set $G_{\mathcal{P}_i} = N_i$ and let A_i be the block of $\mathcal{P}_i$ through ∞. Observe that N_i is

necessarily a subgroup of G_{A_i} so that $A_i - \{\infty\}$ is a union of left cosets of N_i in G. Of course the N_i-orbit of any block of $\mathcal{P}_i$ must be contained in $\mathcal{P}_i$. Thus, considering that the N_i-orbit of A_i is the singleton $\{A_i\}$ and that any $B \in \mathcal{P}_i - \{A_i\}$ is full, we can write

$$\mathcal{P}_i = \{A_i\} \cup \{B_{ij} + n \mid 1 \leqslant j \leqslant \ell_i; n \in N_i\}$$

for suitable full blocks B_{i1}, ..., B_{i,ℓ_i} with $\ell_i = \frac{v-k}{k|N_i|}$.

Considering that the blocks of $\mathcal{P}_i$ form a partition of $G \cup \{\infty\}$ we also have that for any fixed i the union of the B_{ij}'s is a complete system of representatives for the left cosets of N_i that are not contained in A_i. Now note that $\mathcal{P}_i^G = \{\mathcal{P}_i + s \mid s \in S_i\}$ where S_i is a complete system of representatives for the right cosets of N_i in G. Thus we can write

$$\bigcup_{\mathcal{P} \in \mathcal{P}_i^G} \mathcal{P} = \mathcal{A}_i \ \cup \ \mathcal{B}_{i1} \ \cup \ ... \ \cup \ \mathcal{B}_{i,\ell_i}$$

where

$$\mathcal{A}_i = \{A_i + s \mid s \in S_i\}$$

and

$$\mathcal{B}_{ij} = \{B_{ij} + n + s \mid n \in N_i; s \in S_i\} \quad \text{for } 1 \leqslant j \leqslant \ell_i.$$

Observe that $\mathcal{A}_i = {}^{|G_{A_i}:N_i|}(A_i^G)$ and that $\mathcal{B}_{ij} = B_{ij}^G$. Thus, setting

$$\mathcal{F}_i = {}^{|G_{A_i}:N_i|}\{A_i\} \ \cup \ \{B_{i1}, ..., B_{i,\ell_i}\},$$

we can write

$$\bigcup_{\mathcal{P} \in \mathcal{P}_i^G} \mathcal{P} = \bigcup_{B \in \mathcal{F}_i} B^G.$$

We conclude that we have:

$$\mathcal{B} \ = \ \bigcup_{\mathcal{P} \in \mathcal{R}} \mathcal{P} \ = \ \bigcup_{1 \leqslant i \leqslant t; \ \mathcal{P} \in \mathcal{P}_i^G} \mathcal{P} \ = \ \bigcup_{1 \leqslant i \leqslant t; \ B \in \mathcal{F}_i} B^G \ = \ \bigcup_{B \in \mathcal{F}} B^G$$

where

$$\mathcal{F} = \mathcal{F}_1 \ \cup \ ... \ \cup \ \mathcal{F}_t.$$

This means that $\mathcal{F}$ is a 1-rotational difference family generating the underlying BIBD of $\mathcal{D}$. Also, it is clear that the subfamilies $\mathcal{F}_1$, ..., $\mathcal{F}_t$ satisfy the properties of Definition 2.1 so that $\mathcal{F}$ is resolvable.

($\Longleftarrow$) Let $\mathcal{F}$ be a resolvable 1-rotational (G, k, λ) difference family. Thus there exists a partition of $\mathcal{F}$

$$\mathcal{F} = \mathcal{F}_1 \ \cup \ ... \ \cup \ \mathcal{F}_t$$

with each $\mathcal{F}_i$ as in Definition 2.1. Set, for $i = 1, ..., t$,

$$\mathcal{P}_i = \{A_i\} \ \cup \ \{B_{ij} + n \mid 1 \leqslant j \leqslant \ell_i; n \in N_i\}.$$

It is immediate to see that each $\mathcal{P}_i$ is a parallel class of the BIBD generated by $\mathcal{F}$ and that $\mathcal{P}_1^G \ \cup \ ... \ \cup \ \mathcal{P}_t^G$ is a G-invariant resolution of it. □

Example 2.3 Consider the following 5-subsets of $\mathbf{Z}_{24} \cup \{\infty\}$:

$$B_1 = \{1, 2, 3, 4, 11\}; \qquad B_2 = \{1, 5, 10, 14, 21\};$$

$$B_3 = \{1, 11, 14, 16, 21\}; \qquad B_4 = \{1, 14, 15, 17, 22\}.$$

We have:

$$\Delta B_1 = \pm\{\,^3 1,\ ^2 2, 3, 7, 8, 9, 10\}; \qquad \Delta B_2 = \pm\{\,^3 4,\ 5, 7, 8,\ ^2 9,\ ^2 11\};$$

$$\Delta B_3 = \pm\{2, 3, 4,\ ^2 5, 7, 9,\ ^2 10, 11\}; \qquad \Delta B_4 = \pm\{1, 2,\ ^2 3, 5, 7,\ ^2 8, 10, 11\}.$$

Thus, it is readily seen that $\bigcup_{i=1}^{4} \Delta B_i = {}^4(\mathbf{Z}_{24} - N)$ where $N = \{0, 6, 12, 18\}$ is the subgroup of order 4 of $\mathbf{Z}_{24}$. This means that $\{B_1, B_2, B_3, B_4\}$ is a $(24, 4, 5, 4)$-DF. Set $A = \{\infty, 0, 6, 12, 18\}$, observe that $G_A = N$ and hence that $\partial A = \{6, 12, 18, \infty\}$. Thus, considering that each B_i is full (so that $\partial B_i = \Delta B_i$) we can say that $\mathcal{F} = \{^4 A, B_1, B_2, B_3, B_4\}$ is a 1-rotational $(\mathbf{Z}_{24}, 5, 4)$-DF. Of course we can write $\mathcal{F} = \mathcal{F}_1 \cup \mathcal{F}_2 \cup \mathcal{F}_3 \cup \mathcal{F}_4$ with $\mathcal{F}_i = \{A, B_i\}$ for $1 \leqslant i \leqslant 4$. Now note that the reduction (mod 6) of each B_i is $\{1, 2, 3, 4, 5\}$ that is equivalent to say that each B_i is a complete system of representatives for the cosets of N that are not contained in A. We conclude that $\mathcal{F}_i$ satisfies the conditions given in Definition 2.1 with $N_i = N$ for each i and hence $\mathcal{F}$ is resolvable. Following the proof of Theorem 2.2 we can finally say that the above resolution of $\mathcal{F}$ gives rise to a 1-rotational $(25, 5, 4)$-RBIBD whose starter parallel classes are $\mathcal{P}_1$, ..., $\mathcal{P}_4$ where $\mathcal{P}_i = \{A, B_i, B_i + 6, B_i + 12, B_i + 18\}$ for $i = 1, ..., 4$.

Definition 2.4 *A* 1*-rotational DF will be said elementarily resolvable if it admits a resolution of size* 1*.*

Looking at the proof of Theorem 2.2 it is obvious that the following holds.

Proposition 2.5 *An elementarily resolvable* 1*-rotational* (G, k, λ)*-DF is completely equivalent to a* $(|G| + 1, k, \lambda)$*-RBIBD that is* 1*-rotational under* G *with* G *acting transitively on the resolution.*

The following example is taken from [2].

Example 2.6 Consider the collection $\mathcal{F} = \{A, B_1, B_2, B_3, B_4\}$ of 7-subsets of $\mathbf{Z}_{62} \cup \{\infty\}$ whose blocks are:

$$A = \{\infty, 11, 24, 27, 42, 55, 58\};$$

$$B_1 = \{6, 14, 32, 44, 49, 51, 52\} \quad B_2 = \{7, 8, 12, 30, 34, 36, 59\};$$

$$B_3 = \{26, 35, 40, 46, 47, 56, 60\}; \quad B_4 = \{0, 2, 10, 17, 23, 50, 53\}.$$

We have $G_A = \{0, 31\}$ and $\partial A = \pm\{3, 13, 15, 16, 18, 28\} \cup \{\,^3 31\}$. We also have:

$$\partial B_1 = \Delta B_1 = \{1, 2, 3, 5, 7,\ ^2 8, 12, 16,\ ^2 17, 18,\ ^2 19, 20,\ ^2 24, 25, 26, 27, 30\};$$

$$\partial B_2 = \Delta B_2 = \{1, 2,\ ^2 4, 5, 6, 10, 11, 15, 18,\ ^2 22,\ ^2 23, 24, 25, 26, 27, 28,\ ^2 29\};$$

$$\partial B_3 = \Delta B_3 = \{1, 4, 5, 6, 7, {}^2 9, 10, 11, 12, 13, {}^2 14, 16, {}^2 20, {}^2 21, 25, 28, 30\};$$

$$\partial B_4 = \Delta B_4 = \{2, 3, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 17, 19, 21, 22, 23, 26, 27, 29, 30\}.$$

Also here it is readily seen that $\mathcal{F}$ is a 1-rotational $(\mathbf{Z}_{62}, 7, 3)$ difference family. Now check that the reduction (mod 31) of $\bigcup_{i=1}^{4} B_i$ gives $\mathbf{Z}_{31} - \{11, 24, 27\}$. Then, considering that the cosets of $\{0, 31\}$ contained in A are exactly those represented by 11, 24 and 27, we can say that the union of the B_i's is a complete system of representatives for the left cosets of $N = \{0, 31\}$ in G that are not contained in A. Hence we conclude that $\mathcal{F}$ is elementarily resolvable and that a resolution of the corresponding $(63, 7, 3)$-RBIBD is the orbit under $\mathbf{Z}_{62}$ of the single parallel class $\mathcal{P} = \{A, B_1, B_2, B_3, B_4, B_1 + 31, B_2 + 31, B_3 + 31, B_4 + 31\}$.

Definition 2.7 *We say that a (G, N, k, λ)-DF with $|N| = k - 1$ is* resolvable *(and we write (G, N, k, λ)-RDF) if there is a suitable $N' \leqslant N$ such that $|N : N'| = \lambda$ and the union of the base blocks of $\mathcal{F}$ is a complete system of representatives for the left cosets of N' in G that are not contained in N.*

The above terminology is justified by the following proposition.

Proposition 2.8 *If there exists a (G, N, k, λ)-RDF, then there exists an elementarily resolvable 1-rotational (G, k, λ')-DF for a suitable divisor λ' of λ. Moreover, if N is abelian, there exists a (G, N, k, μ)-RDF for every μ such that $\lambda \mid \mu \mid k - 1$.*

Proof. Let $\mathcal{F}$ be a (G, N, k, λ)-RDF so that there is $N' \leqslant N$ satisfying the conditions prescribed by Definition 2.1. The blocks of $\mathcal{P} := \{N\} \cup \{B + n' \mid B \in \mathcal{F}; n' \in N'\}$ partition G by assumption. Considering that N is the unique subset of $\mathcal{P}$ of size $k-1$, it is obvious that $G_{\mathcal{P}}$ fixes N and hence $G_{\mathcal{P}} \leqslant G_N = N$. It is also obvious that $N' \leqslant G_{\mathcal{P}}$ so that we have $N' \leqslant G_{\mathcal{P}} \leqslant N$ and the index λ' of $G_{\mathcal{P}}$ in N is a divisor of λ. Now note that $\gcd(|G|, k) = 1$. In fact we have $|G| = (k-1)t$ for a suitable t and hence $|\mathcal{F}| = \frac{\lambda|G-N|}{k(k-1)} = \frac{\lambda(t-1)}{k}$. On the other hand $\gcd(\lambda, k) = 1$ since λ is a divisor of $|N| = k-1$. Hence we have $|G| = (k-1)(ku+1)$ for a suitable u. It follows that the G-stabilizer of every block of $\mathcal{P} - \{N\}$ is trivial and hence we can write $\mathcal{P} = \{N\} \cup \{B + g \mid B \in \mathcal{F}'; g \in G_{\mathcal{P}}\}$ where $\mathcal{F}'$ is a complete system of representatives for the $G_{\mathcal{P}}$-orbits on the blocks of $\mathcal{P} - \{N\}$. The fact that the blocks of $\mathcal{P}$ partition G is equivalent to say that the union of the blocks of $\mathcal{F}'$ is a complete system of representatives for the left cosets of $G_{\mathcal{P}}$ in G that are not contained in N. It is now easy to recognize that setting $A = N \cup \{\infty\}$ we have that ${}^{\lambda'}\{A\} \cup \mathcal{F}'$ is an elementarily resolvable 1-rotational (G, k, λ')-DF.

Finally, observe that $\{B + n \mid B \in \mathcal{F}; n \in N' - N''\}$ is a $(G, N, k, |N : N''|)$-RDF for every subgroup N'' of N'. The second part of the statement immediately follows. □

Example 2.9 Check that

$$\mathcal{F} = \Big\{\{12, 36, 40, 8, 9\}, \{24, 1, 26, 38, 7\}, \{28, 37, 42, 19, 43\}, \{13, 5, 10, 3, 39\}\Big\}$$

is a $(44, 4, 5, 2)$-DF, namely a $(G, N, 5, 2)$-DF with $G = \mathbf{Z}_{44}$ and $N = \{0, 22, 11, 33\}$.

Looking at the reduction (mod 22) of the blocks of $\mathcal{F}$

$$\{12,14,18,8,9\},\{2,1,4,16,7\},\{6,15,20,19,21\},\{13,5,10,3,17\}$$

we immediately see that their union is a complete system of representatives for the cosets of $N'=\{0,22\}$ not contained in N. Thus, having $|N:N'|=2$, we can say that $\mathcal{F}$ is resolvable and that the orbit of

$$\mathcal{P}:=\Big\{\{\infty,0,22,11,33\},\{12,36,40,8,9\},\{34,14,18,30,31\}\{24,1,26,38,7\},\{2,23,4,16,29\},$$
$$\{28,37,42,19,43\},\{6,15,20,41,21\},\{13,5,10,3,39\},\{35,27,32,25,17\}\Big\}$$

is a 1-rotational $(45,5,2)$-RBIBD.

The above example deserves particular attention since according to the last tables of small BIBDs [32] no resolvable $(45,5,2)$-RBIBD was known before. See also Table 7.38 in [1].

In [12] there are many classes of 1-rotational RBIBDs coming from suitable (G,N,k,λ)-DFs which, however, are not resolvable in the sense of Definition 2.1. In fact, in those DFs we have $|N|=k-1$ but λ is not a divisor of $k-1$. No RBIBD given in that paper is 1-rotational under a group acting transitively on the parallel classes.

In the next sections we will always consider DF's under the cyclic group.

3 Resolvable $((k-1)p,k-1,k,2)$-DFs with p a prime and $k=3$, 5 or 7

Given k odd, for the existence of a $((k-1)p,k-1,k,\lambda)$-RDF with p a prime and $\lambda=1$ or 2 it is trivially necessary that $p\equiv 1 \pmod{2k}$. When $\lambda=1$ this is not always sufficient since, for instance, an exhaustive computer search allows us to see that there is no $(44,4,5,1)$-RDF. On the other hand, as far as the authors are aware, for the time being there is no example of a pair (p,k) with k odd and $p\equiv 1 \pmod{2k}$ a prime for which it is known that a $((k-1)p,k-1,k,2)$-RDF does not exist. Indeed in this section we will prove that such an RDF always exists for $k=3$ and 5. We point out, however, that the difficulty of constructing such RDF's increases a lot with k. In fact, for $k=7$, we will be able to obtain only partial results.

$(2p,2,3,2)$-RDF's with p prime and $p\equiv 1 \pmod 6$

The existence of a $(2p,2,3,1)$-RDF, and hence that of a 1-rotational *Kirkman triple system* of order $2p+1$, has been determined in [17] for any prime $p\equiv 1 \pmod{12}$. For $p\equiv 1 \pmod 6$ but $p\not\equiv 1 \pmod{12}$, namely for $p\equiv 7 \pmod{12}$, such a DF does not exist since in this case a 1-rotational *Steiner triple system* of order $2p+1$ not even exists (see [34], Theorem 2.2). On the other hand now we show that a $(2p,2,3,\mathbf{2})$-DF exists for any prime $p\equiv 1 \pmod 6$.

Theorem 3.1 *There exists a $(2p,2,3,2)$-RDF for any prime $p\equiv 1 \pmod 6$*

Proof. Using the Chinese Remainder Theorem we identify $\mathbf{Z}_{2p}$ and its subgroup $p\mathbf{Z}_{2p}$ of order 2 with $G = \mathbf{Z}_2 \oplus \mathbf{Z}_p$ and $N = \mathbf{Z}_2 \oplus \{0\}$, respectively.

Let ϵ be a primitive cubic root of unity of $\mathbf{Z}_p$ and take the following 3-subsets of G:

$$B_1 = \{(0,1),(0,\epsilon),(0,\epsilon^2)\}, \quad B_2 = \{(1,\epsilon),(1,-\epsilon),(0,-1)\},$$
$$B_3 = \{(1,\epsilon^2),(1,-\epsilon^2),(0,-\epsilon)\}, \quad B_4 = \{(1,1),(1,-1),(0,-\epsilon^2)\}$$

where $< -\epsilon >$ is the multiplicative group generated by $-\epsilon$, namely the group of 6th roots of unity of $\mathbf{Z}_p$. We have:

$$\bigcup_{h=1}^{4} \Delta B_h = \{0\} \times (< -\epsilon > \cdot\{\epsilon - 1, 2\}) \ \cup \ \{1\} \times (< -\epsilon > \cdot\{\epsilon - 1, \epsilon + 1\}).$$

Thus, if S is a complete system of representatives for the cosets of $< -\epsilon >$ in $\mathbf{Z}_p^*$, we see that

$$\mathcal{F} = \{B_h \cdot (1,s) \mid 1 \leqslant h \leqslant 4; s \in S\}$$

is a $(G, N, 5, 2)$-DF. Now note that we have:

$$\bigcup_{h=1}^{4} B_h = \mathbf{Z}_2 \times < -\epsilon >$$

so that the union of all the base blocks of $\mathcal{F}$ gives $\mathbf{Z}_2 \times \mathbf{Z}_p^*$ that trivially is a complete system of representatives for the cosets of $N' = \{(0,0)\}$ that are not contained in N. Thus $\mathcal{F}$ is resolvable and the assertion follows. □

$(4p, 4, 5, 2)$-RDF's with p prime and $p \equiv 1 \pmod{10}$

There are some papers of the 90's [6, 11, 30] dealing with the construction of a 1-rotational $(G, N, 5, 1)$-DF with $G = \mathbf{Z}_2^2 \oplus \mathbf{Z}_p$ and $N = \mathbf{Z}_2^2 \oplus \{0\}$ where $p = 10n + 1$ is a prime. In particular, the existence has been proved for $41 \leqslant p \leqslant 1151$ in [6] and for p *sufficiently large* in [30]. Constructions for 1-rotational $(4p, 4, 5, 1)$-DF's with p as above, namely for 1-rotational $(G, N, 5, 1)$-DF with $G = \mathbf{Z}_{4p}$ and $N = p\mathbf{Z}_{4p}$, have been considered in [11]. In this case the existence has been proved for $p \equiv 31 \pmod{60}$ if certain cyclotomic conditions are satisfied but, still now, to solve the existence problem for every prime p does not seem to be easy. On the other hand here we are able to prove the existence of a $(4p, 4, 5, \mathbf{2})$-DF for any prime $p \equiv 1 \pmod{10}$. This will be achieved by using the following application of the Theorem of Weil on multiplicative character sums (see [31], Theorem 5.41) obtained in [15] (see also [20]).

Theorem 3.2 *Given a prime $p \equiv 1 \pmod{e}$, a t-subset $B = \{b_1, ..., b_t\}$ of $\mathbf{Z}_p$, and a t-tuple $(\beta_1, ..., \beta_t)$ of $\mathbf{Z}_e^t$, the existence of an element $x \in \mathbf{Z}_p$ satisfying the t cyclotomic conditions $x - b_i \in C_{\beta_i}^e$ $(i = 1, ..., t)$ is guaranteed for $p > Q(e,t)$ where*

$$Q(e,t) = \frac{1}{4}\Big(U + \sqrt{U^2 + 4te^{t-1}}\Big)^2 \quad \text{with } U = \sum_{h=1}^{t} \binom{t}{h} (e-1)^h (h-1).$$

In the above statement we have used the standard notation according to which C^e is the subgroup of index e of the multiplicative group $\mathbf{Z}_p^*$ of $\mathbf{Z}_p$, and C_i^e is the coset of C^e represented by r^i where r is a fixed generator of $\mathbf{Z}_p^*$.

Theorem 3.3 *There exists a $(4p, 4, 5, 2)$-RDF for any prime $p \equiv 1 \pmod{10}$.*

Proof. Using the Chinese Remainder Theorem we identify $\mathbf{Z}_{4p}$ and its subgroup $p\mathbf{Z}_{4p}$ of order 4 with $G = \mathbf{Z}_4 \oplus \mathbf{Z}_p$ and $N = \mathbf{Z}_4 \oplus \{0\}$, respectively.

Take four 5-subsets B_1, ..., B_4 of G of the following form:

$$B_1 = \{(0,1),(0,-1),(1,a),(1,-a),(2,b)\}; \quad B_2 = \{(0,c),(0,-c),(0,d),(1,-d),(2,-b)\};$$

$$B_3 = \{(3,1),(3,-1),(2,a),(2,-a),(1,b)\}; \quad B_4 = \{(3,c),(3,-c),(3,d),(2,-d),(1,-b)\}.$$

Note that $B_3 = \phi(B_1)$ and $B_4 = \phi(B_2)$ where $\phi : (x,y) \in G \longrightarrow (3x+3, y) \in G$. We have:F

$$\bigcup_{h=1}^{4} \Delta B_h = \bigcup_{i=0}^{3} \{i\} \times (\{1,-1\} \cdot \Delta_i) \tag{1}$$

where

$$\Delta_0 = {}^2\{2, 2a, 2c, c-d, c+d\};$$

$$\Delta_1 = \Delta_3 = \{a-1, a-1, a+1, a+1, a-b, a+b, c+d, c-d, 2d, b-d\};$$

$$\Delta_2 = {}^2\{b-1, b+1, b+c, b-c, b+d\}.$$

Assume that the quadruple (a,b,c,d) satisfies the following conditions:

$$\text{each } \Delta_i \text{ has exactly two elements in each coset of } C^5; \tag{2}$$

$$\{1,a,b,c,d\} \text{ has exactly one element in each coset of } C^5. \tag{3}$$

Denoted by S a complete system of representatives for the cosets of $\{1,-1\}$ in C^5, condition (2) implies that $\{1,-1\} \cdot \Delta_i \cdot S = {}^2\mathbf{Z}_p^*$ for each i and hence, by (1), we have that

$$\mathcal{F} = \{B_h \cdot (1,s) \mid 1 \leqslant h \leqslant 4; s \in S\}$$

is a $(G, N, 5, 2)$-DF. Now note that

$$\bigcup_{B \in \mathcal{F}} B = \{0,3\} \times (\{\pm 1, \pm c, d\} \cdot S) \ \cup \ \{1,2\} \times (\{\pm a, \pm b, -d\} \cdot S).$$

Thus, since (3) implies that $\{\pm 1, \pm a, \pm b, \pm c, \pm d\} \cdot S = \mathbf{Z}_p^*$, we see that the union of the blocks of $\mathcal{F}$ is a complete system of representatives for the cosets of $N' := \{(0,0),(2,0)\}$ that are not contained in N (namely of the cosets of N' distinct from N' itself and from $\{(1,0),(3,0)\}$). This means that $\mathcal{F}$ is resolvable.

In view of the above discussion, the theorem will be proved if we are able to find at least one *good* quadruple of $\mathbf{Z}_p$, namely a quadruple (a,b,c,d) of elements of $\mathbf{Z}_p$ for

Table 1: Good quadruples (a, b, c, d) for $71 \leqslant p < 1,000$

p	a	b	c	d	p	a	b	c	d
71	10	27	31	4	521	17	30	33	93
101	7	9	33	73	541	13	21	37	91
131	10	34	50	95	571	5	15	83	50
151	44	48	67	72	601	42	60	63	95
181	3	33	42	66	631	47	51	70	71
191	7	9	27	62	641	11	68	13	81
211	4	27	86	92	661	4	69	93	15
241	14	39	46	93	691	6	7	8	64
251	19	42	66	96	701	11	12	57	90
271	27	34	64	71	751	2	8	16	44
281	3	31	56	75	761	10	95	42	35
311	2	29	34	39	811	24	33	37	59
331	8	58	64	82	821	2	7	54	62
401	4	38	47	73	881	3	14	19	59
421	3	49	66	82	911	5	36	84	67
431	28	45	44	75	941	10	27	51	85
461	2	6	15	58	971	9	94	43	88
491	6	19	20	63	991	8	26	29	53

which (2) and (3) hold. By applying repeatedly Theorem 3.2 as done, for instance, in Application 2 of [15], we deduce that a such a good quadruple certainly exists for $p > Q(5, 5) = 87,915,625$.

If C_i^5 is the coset of C^5 containing 2, it is easy to see that (a, b, c, d) is good if (but not "only if"!) we have:

$$a \in C_1^5; \quad a-1 \in C_i^5; \quad a+1 \in C_{i+1}^5;$$

$$b \in C_4^5; \quad a-b \in C_{i+2}^5; \quad a+b \in C_{i+2}^5; \quad b-1 \in C_0^5; \quad b+1 \in C_1^5;$$

$$c \in C_2^5; \quad b+c \in C_2^5; \quad b-c \in C_3^5;$$

$$d \in C_3^5; \quad c-d \in C_{i+3}^5; \quad c+d \in C_{i+4}^5; \quad b-d \in C_{i+4}^5; \quad b+d \in C_4^5.$$

Using a computer we have found a good quadruple (a, b, c, d) also for $p < Q(5, 5)$ with the only exceptions of $p \in \{11, 31, 41, 61\}$. In Table 1 we report the computer results for $p < 1,000$.

Since a $(4 \cdot 11, 4, 5, 2)$-DF has been already determined in Example 2.9, it remains only to exhibit a $(4p, 4, 5, 2)$-DF for $p = 31$, 41 and 61. Such DF's can be also realized of the form $\{(1, s) \cdot B_i, (1, s) \cdot \phi(B_i) \mid s \in S; i = 1, 2\}$ where, again, S is a complete system of representatives for the cosets of $\{1, -1\}$ in C^5 and ϕ is the permutation on G defined by

the rule $\phi(x,y)=(3x+3,y)$. It suffices to take B_1 and B_2 as follows:

p	B_1	B_2
31	$\{(0,5),(0,14),(0,17),(1,26),(2,27)\}$	$\{(0,3),(0,4),(1,10),(1,21),(2,28)\}$
41	$\{(0,2),(2,8),(3,14),(3,15),(3,39)\}$	$\{(0,19),(1,22),(1,26),(3,27),(3,33)\}$
61	$\{(0,2),(0,5),(0,12),(1,41),(2,56)\}$	$\{(0,11),(0,20),(1,49),(1,50),(2,59)\}$

□

$(6p,6,7,2)$-RDF's with p prime and $p\equiv 1 \pmod{28}$

In the following, given a prime $p\equiv 1 \pmod{28}$ we will say that p is *good* if, denoted by ϵ a primitive 7th root of unity of $\mathbf{Z}_p$, then $\epsilon-1$, ϵ^2-1 and ϵ^3-1 are in pairwise distinct cosets of C^4. As an application of a general construction, in [17] it is proved the existence of a $(6p,6,7,1)$-RDF for any good prime $p=56t+1$ not exceeding 10,000. Here we prove the existence of a $(6p,6,7,\mathbf{2})$-RDF for any good prime $p=28t+1<100,000$ and for any good prime p sufficiently large.

Theorem 3.4 *There exists a $(6p,6,7,2)$-RDF for any good prime $p\equiv 1$ (mod 28) with $p>Q(4,7)$ or $p<100,000$.*

Proof. Apply, again, the Chinese Remainder Theorem and identify $\mathbf{Z}_{6p}$ and its subgroup of order 6 with $G=\mathbf{Z}_6\oplus\mathbf{Z}_p$ and $N=\mathbf{Z}_6\oplus\{0\}$, respectively. Let ϵ be a primitive 7th root of unity in $\mathbf{Z}_p$ and consider eight 7-subsets B_0, B_1, ..., B_7 of G of the following form:

$$B_i=\{(0,\epsilon^i a),(1,\epsilon^i b),(2,\epsilon^i c),(3,\epsilon^i d),(4,\epsilon^i e),(5,\epsilon^i f),(5,\epsilon^i g)\}\quad \text{for } 0\leqslant i\leqslant 6;$$

$$B_7=\{(0,1),(0,\epsilon),(0,\epsilon^2),(0,\epsilon^3),(0,\epsilon^4),(0,\epsilon^5),(0,\epsilon^6)\}.$$

An easy counting shows that

$$\bigcup_{h=0}^{7}\Delta B_h=\bigcup_{i=0}^{5}\{i\}\times(<\epsilon>\cdot\Delta_i) \tag{4}$$

where

$$\Delta_0=\pm\{f-g,\epsilon-1,\epsilon^2-1,\epsilon^3-1\};$$
$$\Delta_1=\Delta_5=\{b-a,c-b,d-c,e-d,f-e,g-e,a-f,a-g\};$$
$$\Delta_2=\Delta_4=\{c-a,d-b,e-c,f-d,g-d,a-e,b-f,b-g\};$$
$$\Delta_3=\pm\{a-d,b-e,c-f,c-g\}.$$

We also have

$$\bigcup_{h=0}^{7}B_h=\bigcup_{i=0}^{5}\{i\}\times(<\epsilon>\cdot L_i)$$

where: $L_0 = \{1, a\}$; $L_1 = \{b\}$; $L_2 = \{c\}$; $L_3 = \{d\}$; $L_4 = \{e\}$; $L_5 = \{f, g\}$. Thus, denoted by N' the subgroup of N of index $\lambda = 2$, namely $N' = \{(0,0), (2,0), (4,0)\}$, we can write

$$\bigcup_{h=0}^{7} B_h = \{0,2,4\} \times (<\epsilon> \cdot \{1,a,c,e\}) \cup \{1,3,5\} \times (<\epsilon> \cdot \{b,d,f,g\}) \pmod{N'}. \quad (5)$$

Assume that (a, b, c, d, e, f, g) is a 7-tuple of elements of $\mathbf{Z}_p$ such that the following conditions hold:

$$\text{each } \Delta_i \text{ has exactly two elements in each coset of } C^4; \quad (6)$$

$$\text{both } \{1, a, c, e\} \text{ and } \{b, d, f, g\} \text{ have exactly one element in each coset of } C^4. \quad (7)$$

Let S be complete system of representatives for the cosets of $<\epsilon>$ in C^4. Condition (6) implies that $<\epsilon> \cdot \Delta_i \cdot S = {}^2\mathbf{Z}_p^*$ for $0 \leqslant i \leqslant 5$ and hence, by (4), we deduce that

$$\mathcal{F} = \{B_h \cdot (1, s) \mid 0 \leqslant h \leqslant 7; s \in S\}$$

is a $(G, N, 7, 2)$-DF.

Condition (7) implies that $<\epsilon> \cdot \{1, a, c, e\} \cdot S = \mathbf{Z}_p^*$ and $<\epsilon> \cdot \{b, d, f, g\} \cdot S = \mathbf{Z}_p^*$ so that, by (5), we see that the union of all the base blocks of $\mathcal{F}$ is a complete system of representatives for the cosets of N' that are not contained in N, namely $\mathcal{F}$ is resolvable.

Thus the theorem is proved if one finds a *good* 7-tuple (a, b, c, d, e, f, g) of elements of $\mathbf{Z}_p$ satisfying (6) and (7). It is obvious that a necessary condition for the existence of such a good 7-tuple is that the three elements $\epsilon - 1$, $\epsilon^2 - 1$ and $\epsilon^3 - 1$ lie in pairwise distinct cosets of C^4 since otherwise Δ_0 would not satisfy (6). This is the reason for which it is fundamental to assume the *goodness* of p. For p good one can see, also here, that an iterated application of Theorem 3.2 guarantees the existence of a good 7-tuple for $p > Q(4, 7) = 4,848,810,000$. This is a quite huge number so that to test all primes $p \equiv 1 \pmod{28}$ that are smaller than it does not seem to be feasible. We have easily checked, however, that there is at least one good 7-tuple for every good $p < 100,000$. We report our computer results for $p < 5,000$ in Table 2. □

4 Asymptotic existence of $((k-1)p, k-1, k, 1)$-RDF's with p a prime

We recall that a (n, k, μ) *strong difference family* (SDF) is a collection of multisets (*blocks*) of size k with elements in $\mathbf{Z}_n$ whose lists of differences cover all of $\mathbf{Z}_n$ (zero included!) exactly μ times. It is trivial that every (n, k, μ)-SDF has μ necessarily even and that the number of its blocks is $\frac{\mu n}{k(k-1)}$. Hence, in particular, a $(k-1, k, \mu)$-SDF has $\mu = kt$ even and the number of its blocks is t.

The concept of an SDF, introduced in [12] and revisited in [33], is very useful for the construction of relative difference families. Indeed most direct constructions for (np, n, k, λ)-DFs with p a prime that one can find in the literature have been obtained via the more or less explicit use of a suitable (n, k, μ)-SDF. For instance, the reader may

Table 2: Good 7-tuples (a, b, c, d, e, f, g) for good primes $p \equiv 1 \pmod{28}$, $p < 5,000$

p	a	b	c	d	e	f	g
29	2	3	4	10	12	5	23
113	3	17	25	35	40	51	64
281	5	17	27	35	48	52	65
953	8	10	20	35	46	53	66
1009	3	15	43	48	61	86	92
1877	4	11	27	39	45	56	65
1933	2	14	29	34	40	51	63
2129	7	16	21	36	48	57	69
2297	3	11	21	36	52	57	78
2381	2	1	11	50	21	9	18
2969	3	2	37	30	52	9	26
3137	3	4	34	20	51	30	71
3697	5	1	31	41	47	25	46
4649	3	17	28	19	15	9	6
4733	5	7	13	18	2	40	14
4957	2	1	7	35	26	21	8

recognize that in the construction of the $(4p, 4, 5, 2)$-RDF's given in the previous section we implicitly used the $(4, 5, 10)$-SDF whose blocks are the multisets $\{0, 0, 1, 1, 2\}$ and $\{0, 0, 0, 1, 2\}$.

In [15] it was proved that every (n, k, μ)-SDF implies the existence of a $(np, n, k, 1)$-DF for every prime $p \equiv \mu + 1 \pmod{2\mu}$ sufficiently large. The aim of this section is to prove, with a quite similar reasoning, that given any integer k there exists a $((k-1)p, k-1, k, 1)$-RDF for any prime $p \equiv k^2 + k + 1 \pmod{2k^2 + 2k}$ sufficiently large.

Theorem 4.1 *If there exists a $(k-1, k, kt)$-SDF, then there exists a $((k-1)p, k-1, k, 1)$-RDF for any prime $p \equiv kt + 1 \pmod{2kt}$ with $p > Q(kt, k)$.*

Proof. Let $\{X_1, ..., X_t\}$ be a $(k-1, k, kt)$-SDF and set $X_i = \{x_{i1}, ..., x_{ik}\}$ for $i = 1, ..., t$. Let p be a prime as in the statement so that we have $p = ktn + 1$ with n odd. Once again we identify $\mathbf{Z}_{(k-1)p}$ and $p\mathbf{Z}_{(k-1)p}$ with $G = \mathbf{Z}_{k-1} \oplus \mathbf{Z}_p$ and $N = \mathbf{Z}_{k-1} \oplus \{0\}$, respectively. For each $i = 1, ..., t$, take a k-subset $Y_i = \{y_{i1}, ..., y_{ik}\}$ of $\mathbf{Z}_p^*$ and consider the k-subsets B_1, ..., B_t of G defined by $B_i = \{(x_{i1}, y_{i1}), ..., (x_{ik}, y_{ik})\}$ for $i = 1, ..., t$. It is immediate to see that

$$\bigcup_{h=1}^{t} \Delta B_h = \bigcup_{i=0}^{k-2} \{i\} \times \Delta_i$$

where each Δ_i is a list of kt elements of $\mathbf{Z}_p^*$. It is also obvious that $Y := \bigcup_{i=1}^{t} Y_i$ is, again, a list of kt elements of $\mathbf{Z}_p^*$ that is the projection of the union of the B_i's on $\mathbf{Z}_p^*$.

The hypothesis that $p > Q(kt,k)$ and an iterated use of Theorem 3.2 allow us to see that it is possible to choose the y_{ij}'s in such a way that the following condition holds:

each of the lists Δ_0, Δ_1, ..., Δ_{k-2}, Y has exactly one element in each coset of C^{kt}.

The above condition immediately implies that

$$\mathcal{F} = \{B_h \cdot (1,s) \mid 1 \leqslant h \leqslant t; s \in C^{kt}\}$$

is a $(G,N,k,1)$-RDF and hence the assertion follows. □

It is the case to observe that in the proof of the above theorem the hypothesis that n is odd is fundamental. In fact, the crucial condition on the y_{ij}'s cannot be satisfied for n even since in this case $-1 \in C^{kt}$ and hence, considering that $-\delta \in \Delta_0$ for every $\delta \in \Delta_0$, we would have pairs of elements of Δ_0 lying in the same coset of C^{kt}.

Corollary 4.2 *For any integer k and any prime $p \equiv k(k+1)+1 \ (mod\ 2k(k+1))$ sufficiently large there exists a $((k-1)p, k-1, k, 1)$-RDF.*

Proof. It is enough to apply Theorem 4.1 using the $(k-1,k,k(k+1))$-SDF whose $k+1$ blocks are ${}^k\{0\}$ and $\mathbf{Z}_{k-1} \cup \{0\}$ repeated k times. □

5 Characterizing PDFs by 1-rotational RBIBDs

Now we establish a very strong link between partitioned difference families and 1-rotational RBIBDs.

Theorem 5.1 *There exists a $(G, \{k-1,k\}, k-1)$-PDF in G if and only if there exists an elementarily resolvable 1-rotational (G,k,λ)-DF for a suitable λ.*

Proof. Assume that $\mathcal{P}^*$ is a $(G,\{k-1,k\},\lambda)$-PDF, let A^* be its unique base block of size $k-1$, and set $N = G_{\mathcal{P}^*}$. The order of G, that is $k(|\mathcal{P}^*|-1)+(k-1) = k|\mathcal{P}^*|-1$, is coprime with k so that each block of $\mathcal{P}^*$ distinct from A^* has trivial G-stabilizer. Also, it is obvious that N fixes A^* so that A^* is union of left cosets of N in G. This implies, in particular, that $|N|$ is a divisor of $k-1$, say $k-1 = \lambda|N|$. It is clear that we can write

$$\mathcal{P}^* = \{A^*\} \cup \{B_1 + n, ..., B_\ell + n \mid n \in N\}$$

where $\{B_1, ..., B_\ell\}$ is a complete system of representatives for the N-orbits on the blocks of $\mathcal{P}^* - \{A^*\}$ and hence $\ell = \frac{|\mathcal{P}^*|-1}{|N|} = \frac{|G|-k+1}{k|N|}$.

Set $A = A^* \cup \{\infty\}$. We have:

$$^{|N|}(\,^{|G_A:N|}\partial A) = {}^{|G_A|}\partial A = {}^{|G_A|}\partial A^* \cup {}^{|G_A|}(\,^{(k-1)/|G_A|}\{\infty\}) = \Delta A^* \cup {}^{\lambda|N|}\{\infty\}. \quad (8)$$

It is trivial that

$$\Delta(B_i + n) = \Delta B_i = \partial B_i \quad \text{for every pair } (i,n) \in \{1, ..., \ell\} \times N$$

so that we have

$$\bigcup_{n\in N}[\Delta(B_1+n)\ \cup\ ...\ \cup\Delta(B_\ell+n)] = {}^{|N|}(\partial B_1\ \cup\ ...\ \cup\ \partial B_\ell). \tag{9}$$

By assumption the ordinary differences of all the blocks of $\mathcal{P}^*$ cover all non-zero elements of G exactly $k-1=\lambda|N|$ times and hence we can write

$$\bigcup_{n\in N}[\Delta(B_1+n)\ \cup\ ...\ \cup\Delta(B_\ell+n)]\ \cup\ (\Delta A^*\ \cup\ {}^{\lambda|N|}\{\infty\}) = {}^{\lambda|N|}[(G\ \cup\{\infty\})-\{0\}]$$

which compared with (8) and (9) gives

$${}^{|N|}({}^{|G_A:N|}\partial A\ \cup\partial B_1\ \cup\ ...\ \cup\ \partial B_\ell) = {}^{\lambda|N|}[(G\ \cup\{\infty\})-\{0\}].$$

This means that the partial differences of $\mathcal{F} := {}^{|G_A:N|}\{A\}\cup\{B_1,...,B_\ell\}$ cover all non-zero elements of $G\ \cup\{\infty\}$ exactly λ times, i.e., $\mathcal{F}$ is a 1-rotational (G,k,λ) difference family.

Now note that the hypothesis that $\mathcal{P}^*$ is partitioned implies that $B_1\ \cup\ ...\ \cup\ B_\ell$ is a complete system of representatives for the left cosets of N in G that are not contained in A. It is finally obvious that $\mathcal{F}$ has trivial G-stabilizer. We conclude that $\mathcal{F}$ is elementarily resolvable.

Conversely, assume that $\mathcal{F}$ is an elementarily resolvable 1-rotational (G,k,λ)-DF. Thus we have $\mathcal{F} = {}^{|G_A:N|}\{A\}\ \cup\ \{B_1,...,B_\ell\}$ where A is the block of $\mathcal{F}$ through ∞, $N\leqslant G_A$, $\ell=\frac{|G|-k+1}{k|N|}$, $G_{\mathcal{F}}=G_{B_1}=...=G_{B_\ell}=\{0\}$ and $B_1\ \cup\ ...\ \cup\ B_\ell$ is a complete system of representatives for the left cosets of N in G that are not contained in A. Then, setting $A^*=A-\{\infty\}$ and reasoning as in the "if part" one can see that

$$\mathcal{P}^*=\{A^*\}\ \cup\ \{B_1+n,...,B_\ell+n\mid n\in N\}$$

is a $(G,\{k-1,k\},k-1)$-PDF. □

Looking at the proof of the above theorem we see, in particular, that the following corollary holds.

Corollary 5.2 *Every $((k-1)v,k-1,k,\lambda)$-RDF determines a $((k-1)v,\{k-1,k\},k-1)$-PDF whose block of size $k-1$ is $v\mathbf{Z}_{(k-1)v}$.*

Theorem 5.1 together with Propositions 1.1 and 2.5 allow us to state the following characterization of partitioned difference families with exactly two block sizes $k-1$ and k.

Theorem 5.3 *The partitioned difference families having exactly two block sizes $k-1$ and k are precisely those obtainable by deleting ∞ by a parallel class of a RBIBD with block size k that is 1-rotational under a group acting transitively on its resolution.*

6 Recursive constructions for partitioned difference families

We recall that a $(w, k, 1)$ *difference matrix* (DM for short) in an additive group H of order w is a $k \times w$ matrix M with entries in H such that the difference of any two distinct rows of M is a permutation of the elements of H. It is *good* or *homogeneous* if every row is also a permutation of the elements of H. If the group H is not specified, it is understood that $H = \mathbf{Z}_w$. For general background on difference matrices we refer to [21]. Here, we only recall that if $\gcd(w, k!) = 1$, namely if the least prime factor of w is greater than k, then the $k \times w$ matrix $M = (m_{ij})$ with $m_{ij} = ij$ trivially is a homogeneous $(w, k, 1)$-DM.

Difference matrices are very often useful for the recursive constructions of difference families [11]. In this section we use them for getting composition constructions for partitioned difference families.

Theorem 6.1 *If there exist a (nv, n, K, λ)-SDDF and a homogeneous $(w, k_{max}, 1)$-DM with k_{max} the maximum integer in K, then there exists a $(nvw, nw, {}^wK, \lambda)$-SDDF.*

Proof. Let $\mathcal{F} = \{A_1, ..., A_t\}$ be a (nv, n, K, λ)-DF with $A_i = \{a_{i1}, a_{i2}, ..., a_{ik_i}\}$, and let $M = (m_{ij})$ be a $(w, k_{max}, 1)$-DM. Then the following subsets of $\mathbf{Z}_{nvw}$

$$A'_{ij} = \{a_{i1} + nvm_{1j}, a_{i2} + nvm_{2j}, ..., a_{ik_i} + nvm_{k_ij}\} \quad 1 \leqslant i \leqslant t; 1 \leqslant j \leqslant w$$

form a $(nvw, nw, {}^wK, \lambda)$-DF. It is straightforward to check that this difference family is strictly disjoint in the hypothesis that $\mathcal{F}$ is also strictly disjoint and M is homogeneous. □

Theorem 6.2 *Assume that there exist:*

(i) *a (nv, n, K, λ)-SDDF whose base blocks partition $\mathbf{Z}_{nv} - v\mathbf{Z}_{nv}$;*

(ii) *a homogeneous $(w, k_{max}, 1)$-DM with $k_{\max} = \max\{k \mid k \in K\}$;*

(iii) *a (nw, K', λ)-PDF.*

Then there exists a $(nvw, {}^wK \cup K', \lambda)$-PDF.

Proof. Let $\mathcal{F}$ be a PDF as in (i) so that we have $\sum_{k\in K} k = |\mathbf{Z}_{nv} - v\mathbf{Z}_{nv}| = n(v-1)$. Let $\mathcal{F}'$ be a $(nvw, nw, {}^wK, n)$-SDDF obtainable using Theorem 6.1. The number of elements covered by its blocks is given by $\sum_{k\in {}^wK} k = w\sum_{k\in K} k = nw(v-1)$ that is just the size of $\mathbf{Z}_{nvw} - v\mathbf{Z}_{nvw}$. Recalling that the blocks of $\mathcal{F}'$ do not meet $v\mathbf{Z}_{nvw}$ by definition of a SDDF, we deduce that these blocks partition $\mathbf{Z}_{nvw} - v\mathbf{Z}_{nvw}$. Now, let $\mathcal{F}''$ be a PDF as in (iii) and set $\hat{\mathcal{F}}'' = \{vB \mid B \in \mathcal{F}''\}$. Interpreting the blocks of $\hat{\mathcal{F}}''$ as subsets of $\mathbf{Z}_{nvw}$, we see that $\hat{\mathcal{F}}''$ is a (nw, K', λ)-PDF in $v\mathbf{Z}_{nvw}$. It is then immediate that $\mathcal{F}' \cup \hat{\mathcal{F}}''$ is a $(nvw, {}^wK \cup K', \lambda)$-PDF. □

Corollary 6.3 *Let k, v be positive integers with $p \equiv 1 \pmod k$ for any prime p dividing v. Also assume that there exist a $(w, \{k-1, k\}, k-1)$-PDF and a homogeneous $(w, k, 1)$-DM. Then there exists a $(vw, \{k-1, k\}, k-1)$-PDF.*

Proof. There is a very well known result by Wilson [35] according to which if p is a prime and k is a divisor of $p-1$, then the set of all cosets of the k-th roots of unity in $\mathbf{Z}_p$ is a $(p, k, k-1)$-SDDF. This fact and an iterated use of Theorem 6.1 easily allow us to deduce the existence of a $(v, k, k-1)$-SDDF, namely a $(1 \cdot v, 1, k, k-1)$-DF whose base blocks partition $\mathbf{Z}_v - \{0\} = \mathbf{Z}_v - v\mathbf{Z}_v$. The assertion then follows by applying Theorem 6.2 with $n = 1$ and $\lambda = k-1$. □

Corollary 6.4 *If there exist a $((k-1)v, k-1, k, \lambda)$-RDF, a $((k-1)w, \{k-1, k\}, k-1)$-PDF and a homogeneous $(w, k, 1)$-DM, then there exists a $((k-1)vw, \{k-1, k\}, k-1)$-PDF.*

Proof. By Corollary 5.2, the existence of a $((k-1)v, k-1, k, \lambda)$-RDF implies that of a $((k-1)v, \{k-1, k\}, k-1)$-PDF whose block of size $k-1$ is $v\mathbf{Z}_{(k-1)v}$. It is then obvious that the remaining blocks partition $\mathbf{Z}_{(k-1)v} - v\mathbf{Z}_{(k-1)v}$ and form a $((k-1)v, k-1, k, k-1)$-DDF. Hence we get the assertion by applying Theorem 6.2 with $n = \lambda = k-1$. □

It is also worth noting the following result generalizing a construction for 1-rotational resolvable Steiner 2-designs given by Jimbo and Vanstone [28] and revisited in [17].

Theorem 6.5 *If there exist a $((k-1)v, k-1, k, \lambda)$-RDF, a $((k-1)w, k-1, k, \lambda)$-RDF and a homogeneous $(w, k, 1)$-DM, then there exists a $((k-1)vw, k-1, k, \lambda)$-RDF.*

Proof. First, starting from a $((k-1)v, k-1, k, \lambda)$-RDF, apply the construction given by Theorem 6.1 obtaining in this way a $((k-1)vw, (k-1)w, k, \lambda)$-SDDF, say $\mathcal{F}$. Now take a $((k-1)w, k-1, k, \lambda)$-RDF, say $\mathcal{F}'$, and consider the collection $\mathcal{F}''$ of k-subsets of $\mathbf{Z}_{(k-1)vw}$ defined by $\mathcal{F}'' = \{vB \mid B \in \mathcal{F}'\}$. It is not difficult to see that $\mathcal{F} \cup \mathcal{F}''$ is the required $((k-1)vw, k-1, k, k-1)$-RDF. □

Taking into account the main results obtained in the third section, we have the following immediate corollaries.

Corollary 6.6 (i) *There exists a $(2u, 2, 3, 2)$-RDF for any integer u whose prime factors are all congruent to 1 (mod 6).*
(ii) *There exists a $(4u, 4, 5, 2)$-RDF for any integer u whose prime factors are all congruent to 1 (mod 10).*
(iii) *There exists a $(6u, 6, 7, 2)$-RDF if for every prime factor p of u we have: $p \equiv 1 \pmod{28}$ is good and either $p < 10^5$ or $p > Q(4, 7)$.*

7 Infinite classes of partitioned difference families

We conclude by giving a great bulk of previously unnoticed partitioned difference families that we obtain combining direct and recursive constructions.

Theorem 7.1 *There exists a $(u, \{k-1, k\}, k-1)$-PDF for each pair (u, k) of the following forms:*

(i) *$u = (2k-1)v$ with k even, $2k-1$ a prime and $p \equiv 1 \pmod{k}$ for all prime factors p of v;*

(ii) *$u = vw$ and $k = 3$ with $w \in \{2, 8, 11, 17, 23, 29, 32, 35, 41\}$, and $p \equiv 1 \pmod{6}$ for all prime factors p of v;*

(iii) *$u = 4n - 1$ and $k = 4$ for every n for which a $\mathbf{Z}$-cyclic $Wh(4n)$ is known;*

(iv) *$u = vw$ and $k = 5$ with $w \in \{4, 19, 29, 39\}$ and $p \equiv 1 \pmod{10}$ for all prime factors p of v;*

(v) *$u = vw$ and $k = 6$ with $w \in \{11, 23, 29, 41\}$ and $p \equiv 1 \pmod{6}$ for all prime factors p of v;*

(vi) *$u = 5v$ and $k = 6$ with $p \equiv 1 \pmod{12}$ but $p \notin \{13, 37\}$ for all prime factors p of v;*

(vii) *$u = 41v$ and $k = 7$ with $p \equiv 1 \pmod{14}$ for all prime factors p of v;*

(viii) *$u = 6v$ and $k = 7$ with $p \equiv 1 \pmod{28}$ good, $p < 10^5$ or $p > Q(4, 7)$ for all prime factors p of v;*

(ix) *$u = 7v$ and $k = 8$ with $p \equiv 1 \pmod{8}$ but $p \notin \{17, 89\}$ for all prime factors p of v;*

(x) *$u = vw$ and $k = 8$ with $w \in \{31, 47, 71, 79, 103\}$ and $p \equiv 1 \pmod{8}$ for all prime factors p of v;*

(xi) *$u = q^n - 1$ and $k = q$ with q a prime power and n a positive integer.*

Proof. (i). As observed in the introduction, for k even and $2k-1$ prime, there exists a $(2k-1, \{k-1, k\}, k-1)$-PDF (this is also a special case of Theorem 3.6 in [38]). Also, it is trivial that there exists a $(2k-1, k, 1)$-DM. Hence the assertion follows from Corollary 6.3.

(ii). The case of $w = 2$ follows combining Corollary 6.6(i) and Corollary 5.2.

Among Examples 16.81 of [2] one can find an elementarily resolvable 1-rotational $(\mathbf{Z}_w, 3, 2)$-DF for $w \in W := \{11, 17, 23, 29, 35, 41\}$ and hence there exists a $(w, \{2, 3\}, 2)$-PDF for every $w \in W$. Thus the assertion follows from Corollary 6.3 considering that a homogeneous $(w, 3, 1)$-DM trivially exists for each $w \in W$.

The main result in [19] gives us a 1-rotational $(8v+1, 3, 1)$-RBIBD for every v as in the statement, which is equivalent to a $(8v, 2, 3, 1)$-RDF. The case of $w = 8$ then follows from Corollary 5.2.

It is known that there exists a 1-rotational $(33, 3, 1)$-RBIBD. The number of such RBIBDs up to isomorphism was determined in [18] but the very first example was given in [29]. Thus there exists a $(2 \cdot 16, 2, 3, 1)$-RDF and hence a $(2 \cdot 16, 2, 3, 2)$-RDF too. By Corollary 6.6(i) we also have a $(2v, 2, 3, 2)$-RDF for every v as in the statement. Thus,

considering that a homogeneous $(v, 3, 1)$-DM trivially exists, we get a $(2 \cdot 16v, 2, 3, 2)$-RDF by applying Theorem 6.5.

(iii). As observed in the introduction, any Wh$(4n)$ determines a $(4n-1, \{3, 4\}, 3)$-PDF.

(iv) The case of $w = 4$ follows combining Corollary 6.6(ii) and Corollary 5.2.

Among Examples 16.85 of [2] one can find an elementarily resolvable 1-rotational $(\mathbf{Z}_w, 5, 4)$-DF for $w \in W := \{19, 29, 39\}$ and hence there exists a $(w, \{4, 5\}, 4)$-PDF for every $w \in W$. Thus the assertion follows from Corollary 6.3 considering that there also exists a homogeneous $(w, 5, 1)$-DM for each $w \in W$. This is trivial for $w = 19$, 29 and a homogeneous $(39, 5, 1)$-DM can be found in [5].

(v) The case of $w = 11$ follows from (i). Among Examples 16.86 of [2] one can find an elementarily resolvable 1-rotational $(\mathbf{Z}_w, 6, 5)$-DF for $w \in W := \{11, 23, 29, 41\}$ and hence there exists a $(w, \{5, 6\}, 5)$-PDF for every $w \in W$. Thus the assertion follows from Corollary 6.3 considering that a homogeneous $(w, 5, 1)$-DM trivially exists for each $w \in W$.

(vi) It is known that there exists a $(5v, 5, 6, 1)$-RDF for any v as in the statement [13, 27]. Then the assertion follows from Corollary 5.2.

(vii) Among Examples 16.87 in [2] there is an elementarily resolvable 1-rotational $(42, 7, 6)$-RBIBD and, consequently, a $(41, \{6, 7\}, 6)$-PDF. Thus the assertion follows from Corollary 6.3 considering that a homogeneous $(41, 5, 1)$-DM trivially exists.

(viii) It is enough to combine Corollary 6.6(iii), giving a $(6v, 7, 6, 2)$-RDF, and Corollary 5.2.

(ix) It is known that there exists a $(7v, 7, 8, 1)$-RDF for any v as in the statement [13, 27]. Then the assertion follows from Corollary 5.2.

(x) Partly from Examples 16.87 of [2] and partly from Appendix II in [4], one can deduce the existence of an elementarily resolvable 1-rotational $(\mathbf{Z}_w, 8, 7)$-DF, and hence the existence of a $(w, \{7, 8\}, 7)$-PDF, for $w \in W := \{31, 47, 71, 79, 103\}$. Thus the assertion follows from Corollary 6.3 considering that a homogeneous $(w, 8, 1)$-DM trivially exists for every $w \in W$.

(xi) Let $\mathcal{L}$ be the set of lines of the affine space of order n over the field $\mathbb{F}_q$ of order q, and let $\mathcal{R}$ be the partition of $\mathcal{L}$ into parallel classes. It is clear that $\mathcal{D} = (\mathbb{F}_{q^n}, \mathcal{L}, \mathcal{R})$ is a $(q^n, q, 1)$-RBIBD admitting the multiplication by a primitive element of $\mathbb{F}_{q^n}$ as an automorphism of order $q^n - 1$ fixing 0. Thus $\mathcal{D}$ is 1-rotational under $\mathbf{Z}_{q^n-1}$ so that it is generated by a $(q^n - 1, q - 1, q, 1)$-RDF. The assertion follows from Corollary 5.2. □

Regarding Theorem 7.1(iii), as far as the authors are aware the last up date about the known values of n for which a $\mathbf{Z}$-cyclic Wh$(4n)$ exists is given in [7]. Concerning the set of values of n for which a $\mathbf{Z}$-cyclic Wh$(4n+1)$ is known (and hence a $(4n+1, [1, {}^n4], 3)$-PDF is known too) we also refer to [7] but some recent new results can be found in [3, 15, 26].

Finally, as a consequence of the results obtained in the fourth section we can state the following theorem.

Theorem 7.2 *For any fixed $k > 1$ there are infinitely many values of v for which there exists a $(v, \{k-1, k\}, k-1)$-PDF.*

Acknowledgments

The authors would like to sincerely thank Professor J. Yin for his valuable comments and suggestions for the research topic of this paper.

References

[1] R.J.R. Abel, G. Ge and J. Yin, *Resolvable and near-resolvable designs*, Handbook of Combinatorial Designs, Second Edition, C.J. Colbourn and J.H. Dinitz (Editors), Chapman & Hall/CRC, Boca Raton, FL, 2006, 124–132.

[2] R.J.R. Abel and M. Buratti, *Difference families*, Handbook of Combinatorial Designs, Second Edition, C.J. Colbourn and J.H. Dinitz (Editors), Chapman & Hall/CRC, Boca Raton, FL, 2006, 392-409.

[3] R.J.R. Abel, N.J. Finizio, G. Ge and M. Greig, *New Z-cyclic triplewhist frames and triplewhist tournament designs*, Discrete Applied Mathematics, **154** (2006), 1649–1673.

[4] R.J.R. Abel, N.J. Finizio, M. Greig and L.B. Morales, *Existence of* $(2, 8)$ *GWhD*(v) *and* $(4, 8)$ *GWhD*(v) *with* $v \equiv 0, 1$ $(mod\ 8)$, Des. Codes and Cryptogr. **51** (2009), 79–97.

[5] R.J.R. Abel and G. Ge, *Some difference matrix constructions and an almost completion for the existence of triplewhist tournaments*, European J. Combin. **26** (2005), 1094-1104.

[6] R.J.R. Abel and M. Greig, *Some new RBIBDs with block size* 5 *and PBDs with block sizes* $\equiv 1$ $(mod\ 5)$, Australas. J. Combin. **15** (1997) 177-202.

[7] I. Anderson and N.J. Finizio, *Whist tournaments*, Handbook of Combinatorial Designs, Second Edition, C.J. Colbourn and J.H. Dinitz (Editors), Chapman & Hall/CRC, Boca Raton, FL, 2006, 663-668.

[8] T. Beth, D. Jungnickel and H. Lenz, Design Theory. Cambridge University Press, 1999.

[9] M. Buratti, *On simple radical difference families*, J Combin Des **3** (1995), 161-168.

[10] M. Buratti, *Some constructions for 1-rotational BIBDs with block-size* 5, Australas. J. Combin. **17** (1998), 199–227.

[11] M. Buratti, *Recursive constuctions for difference matrices and relative difference families*, J. Combin. Des. **6** (1998), 165-182.

[12] M. Buratti, *Old and new designs via strong difference families*, J. Combin. Des. **7** (1999), 406-425.

[13] M. Buratti and N.J. Finizio, *Existence results for* 1*-rotational resolvable Steiner* 2*-designs with block size* 6 *or* 8, Bull Inst. Combin. Appl. **50** (2007), 29–44.

[14] M. Buratti and D. Ghinelli, *On disjoint* $(3t, 3, 1)$ *difference families*, J. Statist. Plann. Inference **140** (2010), 1918-1922.

[15] M. Buratti and A. Pasotti, *Combinatorial designs and the theorem of Weil on multiplicative character sums*, Finite Fields Appl. **15** (2009), 332–344.

[16] M. Buratti and A. Pasotti, *Further progress on difference families with block size* 4 *or* 5, Des. Codes and Cryptogr. **56** (2010), 1–20.

[17] M. Buratti and F. Zuanni, *G-invariantly resolvable Steiner* 2*-designs which are* 1*-rotational over* G, Bull Belg. Math. Soc. **5** (1998), 221–235.

[18] M. Buratti and F. Zuanni, *The* 1*-rotational Kirkman triple systems of order* 33, J. Statist. Plann. Inference, **86/2** (2000), 369-377.

[19] M. Buratti and F. Zuanni, *Explicit constructions for* 1*-rotational Kirkman triple systems*, Util. Math. **59** (2001), 27–30.

[20] Y.X. Chang and L. Ji, *Optimal* $(4up, 5, 1)$ *optical orthogonal codes*, J. Combin. Des. **12** (2004), 135–151.

[21] C.J. Colbourn, *Difference matrices*, Handbook of Combinatorial Designs, Second Edition, C.J. Colbourn and J.H. Dinitz (Editors), Chapman & Hall/CRC, Boca Raton, FL, 2006, 411-419.

[22] C. Ding and J. Yin, *Combinatorial Constructions of Optimal Constant Composition Codes*, IEEE Trans. Inform. Theory **51** (2005), 3671–3674.

[23] J.H. Dinitz, *Starters*, Handbook of Combinatorial Designs, Second Edition, C.J. Colbourn and J.H. Dinitz (Editors), Chapman & Hall/CRC, Boca Raton, FL, 2006, 622-628.

[24] J.H. Dinitz and P. Rodney, *Block disjoint difference families for Steiner triple systems*, Util. Math **52** (1997), 153-160.

[25] J.H. Dinitz and N. Shalaby, *Block disjoint difference families for Steiner triple systems:* $v \equiv 3$ (*mod* 6), J. Statist. Plann. Inference **106** (2002), 77-86.

[26] N.J. Finizio and F.J. Palladino, *Improvements to the spectrum of known* Z*-cyclic whist tournament designs*, preprint.

[27] M. Greig, *Some group divisible design construction*, J. Combin. Math. Combin. Comput. **27** (1998), 33-52.

[28] M. Jimbo and S.A. Vanstone, *Recursive Constructions for resolvable and doubly resolvable* 1*-rotational Steiner* 2*-designs*, Utilitas Math. **26** (1984), 45–61.

[29] S. Kageyama, *A survey of resolvable solutions of balanced incomplete block designs*, Internat. Statist. Rev. **40** (1972), 269-273.

[30] P. Leonard, *Realizations for direct constructions of resolvable Steiner* 2*-designs with block size* 5, J. Combin. Des. **8** (2000), 207–217.

[31] R. Lidl and H. Neiderreiter, Finite fields. Encyclopedia of Mathematics, Volume 20, Cambridge University Press, Cambridge, UK, 1983.

[32] R. Mathon and A. Rosa, $2-(v,k,\lambda)$ *designs of small order*, Handbook of Combinatorial Designs, Second Edition, C.J. Colbourn and J.H. Dinitz (Editors), Chapman & Hall/CRC, Boca Raton, FL, 2006, 25-58.

[33] K. Momihara, *Strong difference families, difference covers, and their applications for relative difference families*, Des. Codes Cryptogr. **51**, 253–273 (2009).

[34] K.T. Phelps and A. Rosa, *Steiner triple systems with rotational automorphisms*, Discrete Math. **33** (1981), 57-66.

[35] R.M. Wilson, *Cyclotomic and difference families in elementary abelian groups*, J Number Theory **4** (1972), 17-47.

[36] D. Wu, J. Yang, S. Chen and D. Li, *The existence of* $(v,4,\lambda)$ *disjoint difference families*, Australas. J. Combin. **44** (2009), 225-234.

[37] J. Yin, *Some combinatorial constructions for optical orthogonal codes*, Discrete Math. **185** (1998), 193–198.

[38] J. Yin, X. Shan and Z. Tian, *Constructions of partitioned difference families*, European J. Combin. **29** (2008), 1507–1519.