G-invariantly resolvable Steiner 2-designs which are 1-rotational over G

Marco Buratti   Fulvio Zuanni

Abstract

A *1-rotational* $(G, N, k, 1)$ *difference family* is a set of k-subsets *(base blocks)* of an additive group G whose list of differences covers exactly once $G - N$ and zero times N, N being a subgroup of G of order $k - 1$. We say that such a difference family is *resolvable* when the base blocks union is a system of representatives for the nontrivial right (or left) cosets of N in G.

A Steiner 2-design is said to be *1-rotational* over a group G if it admits G as an automorphism group fixing one point and acting regularly on the remainder. We prove that such a Steiner 2-design is *G-invariantly resolvable* (i.e. it admits a G-invariant resolution) if and only if it is generated by a suitable *1-rotational resolvable difference family* over G.

Given an odd integer k, an additive group G of order $k - 1$, and a prime power $q \equiv 1 \pmod{k(k+1)}$, a construction for 1-rotational (possibly resolvable) $(G \oplus \mathbb{F}_q, G \oplus \{0\}, k, 1)$ difference families is presented. This construction method always succeeds (resolvability included) for $k = 3$. For small values of $k > 3$, the help of a computer allows to find some new 1-rotational (in many cases resolvable) $((k-1)q+1, k, 1)$-BIBD's. In particular, we find $(1449, 9, 1)$ and $(4329, 9, 1)$-BIBD's the existence of which was still undecided.

Finally, we revisit a construction by Jimbo and Vanstone [12] that has apparently been overlooked by several authors. Using our terminology, that construction appears to be a recursive construction for resolvable 1-rotational difference families over cyclic groups. Applying it in a particular case, we get a better result than previously known on *cyclically resolvable* 1-rotational $(v, 4, 1)$-BIBD's.

Received by the editors August 1997.
Communicated by Jean Doyen.
1991 *Mathematics Subject Classification.* 05B05, 05B10, 51E10.
Key words and phrases. Resolvable Steiner 2-design, 1-rotational difference family.

1 Preliminaries

Recall that a $(v,k,1)$-BIBD (*Steiner 2-design* of order v and block-size k) is a pair $(V,\mathcal{B})$ where V is a set of v *points* and $\mathcal{B}$ is a set of k-subsets of V (*blocks*) such that any 2-subset of V is contained in exactly one block.

A $(v,n,k,1)$ *groop divisible design* (GDD) is a triple $(V,\mathcal{C},\mathcal{B})$ where V is a set of v *points*, $\mathcal{C}$ is a set of n-sets (*groops*) partitioning V, and $\mathcal{B}$ is a set of k-subsets of V (*blocks*) such that each block meets each groop in at most one point and any two points lying in distinct groops belong to exactly one block. Of course, when $n=1$ the pair $(V,\mathcal{B})$ is a $(v,k,1)$-BIBD.

Let Σ be a BIBD or GDD. An *automorphism group* of Σ is a group of bijections on the point-set V leaving invariant the block-set $\mathcal{B}$.

A BIBD admitting an automorphism group G is said to be *1-rotational over* G when G fixes one point and acts regularly on the remainder.

A BIBD is *resolvable* (RBIBD) when there exists a partition of its blocks (*resolution*) in classes (*parallel classes*), each of which is a partition of the point-set. An RBIBD is G*-invariantly resolvable* when it admits G as an automorphism group leaving invariant at least one resolution.

A G-invariantly resolvable BIBD is G*-transitively resolvable* when there exists a G-invariant resolution on which G acts transitively. If this is the case and G is cyclic, we say that the BIBD is *cyclically resolvable*. Of course, in order to give a resolution on which G acts transitively it suffices to give only one parallel class (*the starter parallel class*).

Let G be an additive group of order v, let N be a subgroup of G of order n, and let k be a positive integer. A $(G,N,k,1)$ *difference family* (also called $(v,n,k,1)$ *difference family over* G *and relative to* N) is a set of k-subsets of G (*base blocks*) such that each element of $G-N$ is representable in exactly one way as the difference of two elements lying in the same base block while no element of N admits such a representation. If G is cyclic we just speak of $(v,n,k,1)$ difference family.

A $(G,N,k,1)$ difference family generates a groop divisible design $(V,\mathcal{C},\mathcal{B})$ where $V=G$, $\mathcal{C}$ is the set of right cosets of N in G and $\mathcal{B}$ is the family of all the right translates (under G) of the base blocks (see[6]).

When $N=\{0\}$ we obtain a GDD with groop-size 1 and hence a $(|G|,k,1)$-BIBD. Also, in the case where $|N|=k$ the pair $(G,\mathcal{B}\cup\mathcal{C})$ is a $(|G|,k,1)$-BIBD.

A $(G,N,k,1)$ difference family where $|N|=k-1$ is said to be a 1*-rotational difference family*. Such a difference family generates a $(|G|+1,k,1)$-BIBD with point-set $G\cup\{\infty\}$ and block-set $\mathcal{B}\cup\{C\cup\{\infty\}|C\in\mathcal{C}\}$, where ∞ is a symbol not in G. This BIBD is 1-rotational over G. All but one of its block-orbits are *full* (namely of size $|G|$), and $\{C\cup\{\infty\}|C\in\mathcal{C}\}$ is the unique *short* block-orbit.

A *multiplier* of a $(G,N,k,1)$ difference family $\mathcal{F}$ is an automorphism μ of the group G which is also an automorphism of the design generated by $\mathcal{F}$.

2 Resolvable 1-rotational difference families

In this section we want to establish the conditions under which a 1-rotational Steiner 2-design over a group G admits a G-invariant resolution. In order to do this, we introduce the following concept.

Definition 1 *A 1-rotational* $(G, N, k, 1)$ *difference family is said to be resolvable if the union of its base blocks is a complete system of representatives for the non-trivial right (or left) cosets of* N *in* G.

Remark 1 Let $\mathcal{F}$ be a 1-rotational $(N \oplus H, N \oplus \{0\}, k, 1)$ difference family and let π be the projection of $N \oplus H$ over H. Then $\mathcal{F}$ is resolvable if and only if $\bigcup_{A \in \mathcal{F}} \pi(A) = H - \{0\}$.

In [5], the first author - starting from the work of Genma, Jimbo and Mishima [10] - also introduced the definition of *resolvable* $(G, N, k, 1)$ difference family in the case where $|N| = k$. This concept is used in the study of G-invariantly resolvable BIBD's arising from these families.

Theorem 1 *A 1-rotational Steiner 2-design over a group* G *admits a* G*-invariant resolution if and only if it is generated by a suitable resolvable 1-rotational* $(G, N, k, 1)$ *difference family.*

Proof. $(\Rightarrow)$. Let $\Sigma = (V, \mathcal{B})$ be a 1-rotational Steiner 2-design over an additive group G. Of course, we may identify the point-set V with $G \cup \{\infty\}$ and the action of G on V with the addition on the right (under the rule that $\infty + g = \infty$ for any $g \in G$). It is easy to see that the block B through 0 and ∞ has the form $N \cup \{\infty\}$ where N is the stabilizer of B under G.

An easy computation shows that any resolution of Σ contains exactly $\rho := |G : N|$ parallel classes. Now, let $\mathcal{R}$ be a G-invariant resolution of Σ, let $S = \{s_0 = 0, s_1, \ldots, s_{\rho-1}\}$ be a complete system of representatives for the right cosets of N in G, and let $\mathcal{P}_0$ be the parallel class of $\mathcal{R}$ containing $N \cup \{\infty\}$. Since $\mathcal{R}$ is G-invariant, $\mathcal{P}_i := \mathcal{P}_0 + s_i$ is a parallel class for every $i = 0, 1, \ldots, \rho - 1$. Also, for $i \neq j$ we have $\mathcal{P}_i \neq \mathcal{P}_j$, otherwise $\mathcal{P}_i$ would contain the distinct blocks $B + s_i = (N + s_i) \cup \{\infty\}$ and $B + s_j = (N + s_j) \cup \{\infty\}$ which is absurd. Hence the $\mathcal{P}_i$'s are pairwise distinct and their number is exactly equal to $|\mathcal{R}|$, so that we have $\mathcal{R} = \{\mathcal{P}_0, \mathcal{P}_1, \ldots, \mathcal{P}_{\rho-1}\}$.

Since B, i.e. $N \cup \{\infty\}$, is fixed by N, $\mathcal{P}_0$ is fixed by N too. Thus, if A is a block belonging to $\mathcal{P}_0$, each block of type $A + n$ with $n \in N$ belongs also to $\mathcal{P}_0$. On the other hand $\mathcal{P}_0$ does not contain blocks of type $A + g$ with $g \notin N$. In fact $g \notin N$ implies that $g = n + s_i$ for a suitable $n \in N$ and a suitable $i \neq 0$, so that $A + g = (A + n) + s_i \in \mathcal{P}_0 + s_i = \mathcal{P}_i \neq \mathcal{P}_0$.
It easily follows that there are suitable blocks $A_1, A_2, \ldots, A_t$ - where $t = (\rho - 1)/k$ - belonging to pairwise distinct full orbits under G such that

$$\mathcal{P}_0 = \{A_i + n | i = 1, 2, \ldots, t; n \in N\} \cup \{B\}$$

It is not difficult to see that $\mathcal{F} := \{A_1, A_2, \ldots, A_t\}$ is a 1-rotational $(G, N, k, 1)$ difference family. Also, since the union of the blocks belonging to $\mathcal{P}_0$ gives all of G, we have $\bigcup_{1 \leq i \leq t}(A_i + N) = G - N$. It is equivalent to say that $\bigcup_{1 \leq i \leq t} A_i$ is a complete system of representatives for the nontrivial left cosets of N in G, namely that $\mathcal{F}$ is resolvable.
$(\Leftarrow)$. Assume that $\mathcal{F}$ is a resolvable $(G, N, k, 1)$ difference family. Set $\mathcal{P}_0 := \{A + n | A \in \mathcal{F}; n \in N\} \cup \{N \cup \{\infty\}\}$ and fix a complete system S of representatives for the right cosets of N in G. Then $\mathcal{R} := \{\mathcal{P}_0 + s | s \in S\}$ is a G-invariant resolution of the BIBD generated by $\mathcal{F}$. ■

Remark 2 It follows from the proof of the above theorem that any Steiner 2-design which is 1-rotational over G and admits a G-invariant resolution, is G-transitively resolvable. Thus the BIBD is cyclically resolvable in the case where G is cyclic.

The following theorem gives a well-known class of cyclically resolvable 1-rotational BIBD's.

Theorem 2 *The incidence structure of points and lines of any affine geometry $AG(n,q)$ is a cyclically resolvable $(q^n,q,1)$-BIBD which is 1-rotational over $\mathbb{Z}_{q^n-1}$.*

More than one hundred years ago a class of resolvable 1-rotational difference families was found by the following construction.

Theorem 3 (Moore [14]) *There exists a resolvable $(\mathbb{Z}_3 \oplus \mathbb{F}_q, \mathbb{Z}_3 \oplus \{0\}, 4, 1)$ difference family for any prime power $q \equiv 1(\text{mod}4)$.*

Proof. Set $q = 4n+1$ and let ω be a primitive element in $\mathbb{F}_q$. Then $\mathcal{F} := \{\{(0,\omega^i),(0,-\omega^i),(1,\omega^{i+n}),(1,-\omega^{i+n})\} | 0 \le i < n\}$ is the required difference family. ■

Corollary 1 *For any prime $p \equiv 1(\text{mod}4)$ there exists a cyclically resolvable $(3p+1,4,1)$-BIBD which is 1-rotational over $\mathbb{Z}_{3p}$.*

Example 1 Applying Theorem 3 with $q = 13$ we get a $(\mathbb{Z}_3 \oplus \mathbb{Z}_{13}, \mathbb{Z}_3 \oplus \{0\}, 4, 1)$ resolvable difference family whose base blocks are:

$\{(0,1),(0,12),(1,5),(1,8)\}$, $\{(0,2),(0,11),(1,10),(1,3)\}$, $\{(0,4),(0,9),(1,7),(1,6)\}$.

By the ring isomorphism $\psi : (a,b) \in \mathbb{Z}_3 \oplus \mathbb{Z}_{13} \to (13a-12b) \in \mathbb{Z}_{39}$, we may recognize the above family as a $(39,3,4,1)$ difference family with base blocks :

$$\{27,12,31,34\}, \{15,24,10,16\}, \{30,9,7,19\}.$$

Let Σ be the 1-rotational $(40,4,1)$-BIBD generated by this difference family. By Theorem 1, Σ is $\mathbb{Z}_{39}$-invariantly resolvable and a resolution of Σ can be obtained by developing the following starter parallel class:

$\mathcal{P}_0 = \{\{27,12,31,34\},\ \{1,25,5,8\},\ \{14,38,18,21\},\ \{15,24,10,16\},\ \{28,37,23,29\},$
$\{2,11,36,3\},\ \{30,9,7,19\},\ \{4,22,20,32\},\{17,35,33,6\},\ \{0,13,26,\infty\}\}$

We warn the reader that Σ is not isomorphic to the $(40,4,1)$-RBIBD associated with the 3-dimensional projective geometry over $\mathbb{Z}_3$. In fact, one can see that the full stabilizer of a point of the latter BIBD does not have any cyclic subgroup of order 39. Thus we have:

Remark 3 There are at least two non-isomorphic (40,4,1)-RBIBD's.

What we have mentioned above has been overlooked for a long time. For instance, in the parameter tables of small BIBD's recently given by Mathon and Rosa [13], it is stated that the only known $(40,4,1)$-RBIBD is the one obtainable from $PG(3,3)$.

3 Some direct constructions for 1-rotational (possibly resolvable) difference families

With the following direct constructions, given a prime power $q \equiv 1 \pmod{k(k+1)}$ with k odd, we want to find a 1-rotational (possibly resolvable) $(G\oplus\mathbb{F}_q, G\oplus\{0\}, k, 1)$ difference family where G is a suitable additive group of order $k-1$. This will be achieved under the assumption that there exists a k-tuple $X = (x_0, x_1, \ldots, x_{k-1}) \in {\mathbb{F}_q}^k$ satisfying suitable conditions.

Construction 1 Let $q = k(k+1)t + 1$ be a prime power with k odd, let δ be a generator of $(k+1)-st$ powers in $\mathbb{F}_q$, and let $(g_1 = 0, g_2, \ldots, g_{k-1})$ be an ordering of a fixed additive group G of order $k-1$. Set $g_0 = 0$ and let $X = (x_0, x_1, \ldots, x_{k-1}) \in {\mathbb{F}_q}^k$ such that the following conditions hold:

(1) $S_1 := \pm(x_1 - x_0, \delta^t - 1, \delta^{2t} - 1, \ldots, \delta^{(k-1)t/2} - 1)$ is a system of representatives for the cosets of $\langle\delta\rangle$ in ${\mathbb{F}_q}^*$.

(2) $S_h := (x_i - x_j | (i,j) \in \{0, 1, \ldots, k-1\}^2, g_i - g_j = g_h)$ is a system of representatives for the cosets of $\langle\delta\rangle$ in ${\mathbb{F}_q}^*$ for $2 \le h < k$.

Then the family

$$\mathcal{E} = \{\{(g_0, \delta^i x_0), (g_1, \delta^i x_1), \ldots, (g_{k-1}, \delta^i x_{k-1})\} | 0 \le i < kt\} \cup$$
$$\cup \{\{0\} \times (\delta^j \langle\delta^t\rangle) | 0 \le j < t\}$$

is a 1-rotational $(G \oplus \mathbb{F}_q, G \oplus \{0\}, k, 1)$ difference family. Moreover, $\mathcal{E}$ is resolvable if the following additional condition is satisfied:

(3) $S_k := (x_0, x_1, \ldots, x_{k-1}, 1)$ is a system of representatives for the cosets of $\langle\delta\rangle$ in ${\mathbb{F}_q}^*$.

Proof. It is easy to check that the list $\Delta\mathcal{E}$ of differences from $\mathcal{E}$ is given by

$$\Delta\mathcal{E} = \bigcup_{1 \le h < k} \{g_h\} \times (S_h \langle\delta\rangle)$$

On the other hand, in view of (1) and (2), $S_h\langle\delta\rangle = {\mathbb{F}_q}^*$ for each $h = 1, \ldots, k-1$, so that $\Delta\mathcal{E} = G \times {\mathbb{F}_q}^*$. The first part of the statement follows.

Note that the projection of the union of the blocks of $\mathcal{E}$ over $\mathbb{F}_q$ is given by $S_k\langle\delta\rangle$. Hence, assuming that condition (3) is satisfied too, such a projection coincides with ${\mathbb{F}_q}^*$. Therefore, the second part of the statement follows from Remark 1. ∎

Construction 2 Let $q = k(k+1)t + 1$ be a prime power with $k = 2^n + 1$, let δ be a generator of $(k+1)-st$ powers in $\mathbb{F}_q$, and let $(g_1 = 0, g_2, \ldots, g_{k-1})$ be an ordering of ${\mathbb{Z}_2}^n$. Set $g_0 = 0$ and let $X = (x_0, x_1, \ldots, x_{k-1}) \in {\mathbb{F}_q}^k$ such that the following conditions hold:

(4) $T_1 := (x_1 - x_0, \delta^t - 1, \delta^{2t} - 1, \ldots, \delta^{(k-1)t/2} - 1)$ is a system of representatives for the cosets of $\langle\sqrt{\delta}\rangle$ in ${\mathbb{F}_q}^*$.

(5) $T_h := (x_i - x_j | 0 \leq i < j \leq k-1, g_i - g_j = g_h)$ is a system of representatives for the cosets of $\langle\sqrt{\delta}\rangle$ in ${\mathbb{F}_q}^*$, for $2 \leq h < k$.

Then the family $\mathcal{E}$ defined like in Construction 1 is a 1-rotational $({\mathbb{Z}_2}^n \oplus \mathbb{F}_q, {\mathbb{Z}_2}^n \oplus \{0\}, k, 1)$ difference family. Moreover, $\mathcal{E}$ is resolvable if the following additional condition is satisfied:

(6) $(x_0, x_1, \ldots, x_{k-1}, 1) = \pm T_k$ where T_k is a system of representatives for the cosets of $\langle\sqrt{\delta}\rangle$ in ${\mathbb{F}_q}^*$.

Proof. This time we can write:

$$\Delta\mathcal{E} = \bigcup_{1 \leq h < k} \{g_h\} \times (\pm T_h \langle\delta\rangle)$$

On the other hand, $\pm\langle\delta\rangle = \langle\sqrt{\delta}\rangle$ so that, in view of (4) and (5), $\pm T_h\langle\delta\rangle = {\mathbb{F}_q}^*$ for each $h = 1, \ldots, k-1$. Hence $\Delta\mathcal{E} = G \times {\mathbb{F}_q}^*$ and the first part of the statement follows.
Assuming that condition (6) is satisfied too, the projection of the union of the blocks of $\mathcal{E}$ over $\mathbb{F}_q$ is given by $\pm T_k\langle\delta\rangle = {\mathbb{F}_q}^*$. Therefore, the second part of the statement follows again from Remark 1. ∎

Construction 3 Let $q = k(k+1)t+1$ be a prime power with $\gcd(2t, k) = 1$, let δ be a generator of $(k+1)-st$ powers in $\mathbb{F}_q$ and let $(g_1 = 0, g_2, \ldots, g_{k-1})$ be an ordering of a fixed additive group G of order $k-1$. Set $g_0 = 0$ and let $X = (x_0, x_1, \ldots, x_{k-1}) \in {\mathbb{F}_q}^k$ such that condition (2) holds. Finally, let $Y = (y_0, y_1, \ldots, y_{k-1}) \in {\mathbb{F}_q}^k$ such that its list of differences ΔY satisfies the following condition:

(7) $Z := \pm(x_1 - x_0)\langle\delta^t\rangle \cup \Delta Y$ is a system of representatives for the cosets of $\langle\delta^k\rangle$ in ${\mathbb{F}_q}^*$.

Then the family

$$\mathcal{E} = \{\{(g_0, \delta^i x_0), (g_1, \delta^i x_1), \ldots, (g_{k-1}, \delta^i x_{k-1})\} | 0 \leq i < kt\} \cup$$

$$\cup \{\{(0, \delta^{kj} y_0), (0, \delta^{kj} y_1), \ldots, (0, \delta^{kj} y_{k-1})\} | 0 \leq j < t\}$$

is a 1-rotational $(G \oplus \mathbb{F}_q, G \oplus \{0\}, k, 1)$ difference family.
Moreover, $\mathcal{E}$ is resolvable under the additional hypothesis that X satisfies condition (3) and that Y satisfies the following condition:

(8) Y is a system of representatives for the cosets of $\langle\delta^k\rangle$ in $\langle\delta\rangle$.

Proof. It is easy to check that the list of differences from $\mathcal{E}$ is given by

$$\Delta\mathcal{E} = \{g_1\} \times [\pm(x_1 - x_0)\langle\delta\rangle \cup (\Delta Y)\langle\delta^k\rangle \cup \bigcup_{2\leq h<k} \{g_h\} \times (S_h\langle\delta\rangle).$$

On the other hand, since $\gcd(t,k) = 1$, we can write $\langle\delta\rangle = \langle\delta^t\rangle\langle\delta^k\rangle$. It follows that $\pm(x_1 - x_0)\langle\delta\rangle \cup (\Delta Y)\langle\delta^k\rangle = Z\langle\delta^k\rangle = {\mathbb{F}_q}^*$ (by (7)). Also, by (2), $S_h\langle\delta\rangle = {\mathbb{F}_q}^*$ for each $h = 2, 3, \ldots, k-1$. So $\Delta\mathcal{E} = G \times {\mathbb{F}_q}^*$ and the first part of the statement follows.

Now assume that (3) and (8) hold. The projection of the union of the blocks of $\mathcal{E}$ over $\mathbb{F}_q$ is given by $\langle\delta\rangle X \cup \langle\delta^k\rangle Y$. But, by (8), $\langle\delta^k\rangle Y = \langle\delta\rangle$ so that $\langle\delta\rangle X \cup \langle\delta^k\rangle Y = \langle\delta\rangle(X \cup \{1\}) = {\mathbb{F}_q}^*$ (by (3)). Therefore, the second part of the statement follows from Remark 1. ∎

Remark 4 (i). Note that conditions (1), ..., (8) are compatible with the sizes of the lists S_h's, T_h's, Y and Z. In fact, all the S_h's have size $k+1 = |{\mathbb{F}_q}^* : \langle\delta\rangle|$, all the T_h's have size $(k+1)/2 = |{\mathbb{F}_q}^* : \langle\sqrt{\delta}\rangle|$, Z has size $k(k+1) = |{\mathbb{F}_q}^* : \langle\delta^k\rangle|$ and, finally, Y has size $k = |\langle\delta\rangle : \langle\delta^k\rangle|$.

(ii). In order to apply the previous constructions a computer is needed, in general. First of all, we need to find a primitive root ω in $\mathbb{F}_q$. Then we have to construct the *index function* $ind : \omega^i \in {\mathbb{F}_q}^* \to i \in \mathbb{Z}_{q-1}$. Finally, using this function, for a given choice of X (and Y in Construction 3) we should check which of the conditions (1), ..., (8) hold. For instance, (1), (2) and (3) hold if and only if $ind(S_h) = \mathbb{Z}_{k+1} \pmod{(k+1)}$ for $1 \leq h \leq k$.

(iii). Obviously, in order for condition (1) to hold, q must be such that any two elements of the set $\{\delta^t - 1, \delta^{2t} - 1, \ldots, \delta^{(k-1)t/2} - 1\}$ lie in distinct cosets of $\langle\delta\rangle$ in ${\mathbb{F}_q}^*$. Any prime power $q \equiv 1 \pmod{k(k+1)}$ with k odd and satisfying this property will be called *good*. So both Constructions 1, 2 may succeed only if q is good.

(iv). Constructions 1 and 3 may succeed only for t odd. In fact, assuming that t is even, let g_h be an involution of G. Then $-1 \in \langle\delta\rangle$ and $S_h = \pm(T_h)$. Consequently, for any $z \in T_h$, the elements z and $-z$, both of which belong to S_h, represent the same coset of $\langle\delta\rangle$ in ${\mathbb{F}_q}^*$, so that (2) cannot be satisfied.

(v). It is easy to see that the difference families given by Constructions 1 and 2 admit δ as a multiplier of order kt, while the difference family obtainable by Construction 3 admits δ^k as a multiplier of order t.

4 Some resolvable $(2p, 2, 3, 1)$ difference families

Here we show that Construction 2 always succeeds in the case where q is prime and $k = 3$.

Theorem 4 *For any prime $p = 12t+1$ there exists a resolvable $(2p, 2, 3, 1)$ difference family.*

Proof. Let δ be a generator of 4th powers (mod p), and let $X = (x_0, x_1, x_2) \in {\mathbb{Z}_p}^3$ be defined as follows:
$X = (a, -a, -1)$ with $a = \min\{n \in N | n$ and $n+1$ are non-squares (mod p)$\}$ when 2 and $\delta^t - 1$ are both squares or both non-squares (mod p);
$X = (-1, a, -a)$ with $a = \min\{n \in N | n$ is a non-square (mod p)$\}$ when 2 is a square and $\delta^t - 1$ is a non-square (mod p);
$X = (-1, 1/2, -1/2)$ when 2 is a non-square and $\delta^t - 1$ is a square (mod p).
Now, one can easily check that applying Construction 2 with $G = \mathbb{Z}_2$, $(g_1, g_2) = (0, 1)$, and $X = (x_0, x_1, x_2) \in {\mathbb{Z}_p}^3$ defined as above,

$$\mathcal{E} = \{\{(0, \delta^i x_0), (0, \delta^i x_1), (1, \delta^i x_2)\} | 0 \leq j < 3t\} \cup \{\{(0, \delta^j), (0, \delta^{t+j}), (0, \delta^{t+j})\} | 0 \leq j < t\}$$

is a resolvable $(\mathbb{Z}_2 \oplus \mathbb{Z}_p, \mathbb{Z}_2 \oplus \{0\}, 3, 1)$ difference family. ■

Corollary 2 *For any prime $p \equiv 1$ (mod 12), there exists a cyclically resolvable $(2p + 1, 3, 1)$-BIBD which is 1-rotational over $\mathbb{Z}_{2p}$.*

We recall that the existence problem for 1-rotational $(2v + 1, 3, 1)$-BIBD's over the cyclic group has been completely settled by Phelps and Rosa [15]. As far as we know, the analogous problem for 1-rotational RBIBD's is open.

Example 2 Let us apply Theorem 4 with $t = 1$, namely with $p = 13$. We can take $\delta = 3$ as a generator of 4th powers (mod 13). Note that $2 = \delta^t - 1$ is not a square (mod 13) and that $a = 5$ is the first integer such that both a and $a + 1$ are non-squares (mod 13). Thus, according to the proof of Theorem 4, we use the triple $X = (5, 8, 12)$. The base blocks of the resultant resolvable $(\mathbb{Z}_2 \oplus \mathbb{Z}_{13}, \mathbb{Z}_2 \oplus \{0\}, 3, 1)$ difference family are the following:

$$\{(0, 5), (0, 8), (1, 12)\}, \{(0, 2), (0, 11), (1, 10)\},$$

$$\{(0, 6), (0, 7), (1, 4)\}, \{(0, 1), (0, 3), (0, 9)\}.$$

By the ring isomorphism $\psi : (a, b) \in \mathbb{Z}_2 \oplus \mathbb{Z}_{13} \to (13a - 12b) \in \mathbb{Z}_{26}$, we may identify the above family as a (26, 2, 3, 1) difference family, say $\mathcal{E}$, with the following base blocks:

$$\{18, 8, 25\}, \{2, 24, 23\}, \{6, 20, 17\}, \{14, 16, 22\}.$$

A starter parallel class of the (27, 3, 1)-RBIBD generated by $\mathcal{E}$ is

$$\mathcal{P}_0 = \{\{18, 8, 25\}, \{5, 21, 12\}, \{2, 24, 23\}, \{15, 11, 10\}, \{6, 20, 17\},$$

$$\{19, 7, 4\}, \{14, 16, 22\}, \{1, 3, 9\}, \{0, 13, \infty\}\}.$$

5 Some 1-rotational difference families with block size 5, 7, 9

In [7] the first author showed that a prime $p \equiv 1 \pmod{30}$ is good if and only if $(11+5\sqrt{5})/2$ is not a cube (mod p) and essentially applying Construction 2 proved the existence of a $({\mathbb{Z}_2}^2 \oplus \mathbb{Z}_p, {\mathbb{Z}_2}^2 \oplus \{0\}, 5, 1)$ difference family for any good prime $p \equiv 1 \pmod{30}$. It is reasonable to believe that Construction 2 almost always succeeds in realizing *resolvable* $({\mathbb{Z}_2}^2 \oplus \mathbb{Z}_p, {\mathbb{Z}_2}^2 \oplus \{0\}, 5, 1)$ difference families having p a good prime. But this is not easy to prove. However, with the aid of a computer, it has been shown that success is guaranteed for $p < 1000$ with the only exception of $p = 61$.
In order to apply the constructions of Section 3 when $k > 5$, the help of a computer seems to be essential even if we are interested only in 1-rotational designs, without asking for resolvability. Here are a few computer results for the cases $k = 7$ and $k = 9$.

k = 7. Construction 1 gives us a 1-rotational resolvable $(6p+1, 7, 1)$-BIBD for any good prime $p = 56t + 1 < 10000$ with t odd. It suffices to take $G = \mathbb{Z}_6$, $(g_1, g_2, \ldots, g_6) = (0, 1, \ldots, 5)$ and $X \in {\mathbb{Z}_p}^7$ as indicated in the following table.

p	**X**
281	(2, 5, 7, 26, 199, 42, 46)
953	(2, 4, 3, 5, 219, 545, 253)
2297	(2, 8, 3, 5, 26, 1052, 1241)
2969	(3, 37, 7, 13, 69, 1946, 2168)
4649	(2, 5, 3, 6, 12, 1786, 4297)
5881	(2, 41, 6, 13, 33, 301, 5647)
6217	(2, 6, 5, 10, 8, 3353, 1312)
6329	(2, 3, 4, 8, 6, 3406, 1871)
6553	(5, 25, 7, 22, 53, 1784, 5754)
7561	(2, 25, 3, 13, 39, 1988, 5303)
8233	(2, 5, 10, 11, 55, 797, 6792)
8681	(2, 4, 3, 6, 8, 907, 7913)
9241	(2, 15, 7, 17, 34, 715, 5395)
9689	(2, 3, 4, 8, 27, 132, 7284)

Construction 3 gives us a 1-rotational $(6p+1, 7, 1)$-BIBD for any bad prime $p = 56t+1 < 10000$ having t odd. It suffices to take $G = \mathbb{Z}_6$, $(g_1, g_2, \ldots, g_6) = (0, 1, \ldots, 5)$ and $X, Y \in {\mathbb{Z}_p}^7$ as indicated in the following table.

p	**X**	**Y**
617	(0, 1, 2, 5, 12, 70, 423)	(0, 3, 12, 100, 306, 456, 490)
1289	(0, 1, 3, 8, 6, 403, 758)	(0, 3, 9, 47, 638, 820, 1029)

2521	(0, 1, 2, 5, 3, 529, 2390)	(0, 2, 8, 19, 178, 1995, 2418)
2857	(0, 1, 2, 5, 10, 121, 592)	(0, 3, 10, 29, 659, 1240, 1718)
5209	(0, 1, 3, 8, 30, 267, 4756)	(0, 5, 15, 22, 481, 2844, 3454)
5657	(0, 1, 2, 5, 3, 26, 4480)	(0, 2, 5, 12, 262, 953, 4682)
7001	(0, 1, 2, 5, 3, 27, 1814)	(0, 2, 5, 26, 134, 1302, 2642)
7673	(0, 1, 2, 5, 3, 89, 3224)	(0, 2, 5, 11, 172, 1904, 6058)
8009	(0, 1, 2, 5, 3, 31, 4280)	(0, 2, 5, 32, 233, 1208, 2369)

k = 9. Construction 2 gives us a 1-rotational resolvable $(8p+1, 9, 1)$-BIBD for each good prime $p = 90t + 1 < 10000$ with t odd. It suffices to take $G = {\mathbb{Z}_2}^3$, $(g_1, g_2, \ldots, g_8) = ((000), (001), (010), (011), (100), (101), (110), (111))$ and $X \in {\mathbb{Z}_p}^9$ as indicated in the following table.

p	**X**
991	(2, 987, 4, 989, 14, 980, 939, 762, 786)
1531	(2, 1527, 4, 1529, 12, 1503, 804, 153, 720)
6571	(2, 6560, 3, 6568, 18, 6566, 5228, 2666, 6288)
9631	(2, 9629, 4, 9630, 6, 9627, 1316, 4832, 6194)

For $p \in \{181, 541, 631, 1171, 6121\}$, Constructions 2 or 3 give us a 1-rotational $(8p+1, 9, 1)$-BIBD. The constructions are applied with G and $(g_1, g_2, \ldots, g_8)$ as above. In the table below we indicate how to take the 9tuple X when Construction 2 is applied and how to take the 9tuples X and Y when Construction 3 is applied.

p	**X**	**Y**
181	(1, 14, 2, 3, 41, 64, 92, 88, 142)	
541	(1, 3, 4, 5, 13, 7, 210, 305, 224)	
631	(1, 2, 3, 4, 10, 11, 30, 614, 277)	(0, 2, 13, 247, 433, 452, 486, 588, 574)
1171	(1, 2, 3, 4, 19, 5, 1018, 310, 589)	(0, 2, 8, 102, 255, 794 , 939, 1095, 1123)
6121	(1, 3, 4, 5, 10, 6, 21, 5278, 4300)	

Remark 5 Abel and Greig ([2], Table 2.12) give the set of values of t for which the existence of a $(72t + 9, 9, 1)$-BIBD is still undecided. One can check that the $(8p + 1, 9, 1)$-BIBD's that we obtain with $p = 181$ and $p = 541$, allow to remove 20 and 60 from this set.

6 Recursive constructions for resolvable 1-rotational difference families over cyclic groups

Concerning recursive constructions of 1-rotational difference families over cyclic groups, we recall results on this matter that seem to have been missed by several authors. In a 1983 paper, Jimbo [11] gave a recursive construction for cyclic

1-rotational Steiner 2-designs. Starting from this construction, one year later Jimbo and Vanstone [12] obtained a composition theorem for cyclically resolvable 1-rotational designs. Here, we revisit the construction of Jimbo and Vanstone using our terminology. Namely, their construction is presented as a composition theorem for resolvable 1-rotational difference families. We observe that, as a corollary, it is possible to obtain a better result on cyclically resolvable 1-rotational BIBD's with block-size 4. First we need a definition.

Definition 2 *A $k \times w$ matrix $A = (a_{ih})$ with elements from $\mathbb{Z}_w$ is said to be a $(w,k,1)$ difference matrix if the following condition is satisfied:*

$$(a_{r1} - a_{s1}, a_{r2} - a_{s2}, \ldots, a_{rw} - a_{sw}) = \mathbb{Z}_w (\mathrm{mod} w), 1 \leq r < s \leq k$$

namely if the difference of any two distinct rows of A contains each element of $\mathbb{Z}_w$ exactly once.

We say that a $(w,k,1)$ difference matrix is *good* if no row of A contains repeated elements. It is easy to see that such a good difference matrix exists if and only if there exists a $(w,k+1,1)$ difference matrix.

Lemma 1 *If $gcd(w,k!) = 1$, namely if the least prime dividing w is larger than k, then the matrix*

$$A = (i(h-1))_{i=1,\ldots,k;h=1,\ldots,w}$$

is a good $(w,k,1)$ difference matrix.

We refer to [9] for general results on difference matrices. Some generalizations can be found in [6].

Difference matrices are used by Jimbo and Vanstone [12] to get a recursive construction that we restate below in terms of difference families.

Construction 4 Let $\mathcal{D} = \{D_i | i \in I\}$ and $\mathcal{E} = \{E_j | j \in J\}$ be $(nv, n, k, 1)$ and $(nw, n, k, 1)$ difference families respectively. Then, let $A = (a_{ih})$ be a $(w,k,1)$ difference matrix. For each $D_i = \{d_{i1}, d_{i2}, \ldots, d_{ik}\} \in \mathcal{D}$ and each $h \in \{1, \ldots, w\}$, set $D_{(i,h)} = \{d_{i1} + nva_{1h}, d_{i2} + nva_{2h}, \ldots, d_{ik} + nva_{kh}\}$. For each $E_j = \{e_{j1}, e_{j2}, \ldots, e_{jk}\} \in \mathcal{E}$, set $E_j{}^* = \{ve_{j1}, ve_{j2}, \ldots, ve_{jk}\}$. Then the family

$$\mathcal{F} = \{D_{(i,h)}(\mathrm{mod}(nvw)) | i \in I, 1 \leq h \leq w\} \cup \{E_j{}^*(\mathrm{mod}(nvw)) | j \in J\}$$

is a $(nvw, n, k, 1)$ difference family.

We point out that the above construction can also be obtained as a consequence of a much more general result (see [6], Corollary 5.10). This construction has many applications. For instance, applying it with $n = k$, $\gcd(w, (k-1)!) = 1$ and $A = ((i-1)(h-1))$, one obtains a construction for *cyclic block designs* given by M. Colbourn and C. Colbourn [8]. On the other hand, when $n = k - 1$, we get the recursive construction for 1-rotational Steiner 2-designs given by Jimbo [11].

Now we give a recursive construction for resolvable 1-rotational difference families over cyclic groups.

Theorem 5 *Let $\mathcal{D} = \{D_i | i \in I\}$ and $\mathcal{E} = \{E_j | j \in J\}$ be resolvable $((k-1)v, k-1, k, 1)$ and $((k-1)w, k-1, k, 1)$ difference families respectively. Assume that* $\gcd(w, k-1) = 1$ *and let $A = (a_{ih})$ be a good $(w, k, 1)$ difference matrix. Then the $((k-1)vw, k-1, k, 1)$ difference family $\mathcal{F}$ obtainable by Construction 4 (with $n = k-1$) is also resolvable.*

Proof. Let x, x' be elements lying in the base blocks union of $\mathcal{F}$ and assume that $x \equiv x' \pmod{vw}$ holds. There are three possibilities:
1st case: x is of the form $d_{ir} + (k-1)va_{rh}$ and x' is of the form $d_{i'r'} + (k-1)va_{r'h'}$. In this case we should get $d_{ir} \equiv d_{i'r'} \pmod{v}$ which, since $\mathcal{D}$ is resolvable, implies that $i = i'$ and $r = r'$. It follows that $(k-1)a_{rh} \equiv (k-1)a_{rh'} \pmod{w}$ and hence, since $\gcd(w, k-1) = 1$, $a_{rh} \equiv a_{rh'} \pmod{w}$. Then, since A is good, we also have $h = h'$.
2nd case: x is of the form $d_{ir} + (k-1)va_{rh}$ and x' is of the form $ve_{jr'}$. In this case we should get $d_{ir} \equiv 0 \pmod{v}$ which is absurd since $\mathcal{D}$ is resolvable.
3rd case: x is of the form ve_{jr} and x' is of the form $ve_{j'r'}$. In this case we should get $e_{jr} \equiv e_{j'r'} \pmod{w}$ which, since $\mathcal{E}$ is resolvable, implies $j = j'$ and $r = r'$.
Now observe that no element x lying in a certain base block of $\mathcal{F}$ can be equivalent to $0 \pmod{vw}$. In fact, if $x = d_{ir} + (k-1)va_{rh}$, we should have $d_{ir} \equiv 0 \pmod{v}$, contradicting the fact that $\mathcal{D}$ is resolvable, while if $x = ve_{js}$ we should have $e_{js} \equiv 0 \pmod{w}$, contradicting the fact that $\mathcal{E}$ is resolvable.
In conclusion, we have proved that any two distinct elements x, x' lying in the union of the base blocks of $\mathcal{F}$ are distinct modulo vw and that no element of this union is zero modulo vw. This means that the union of the base blocks of $\mathcal{F}$ and zero is a system of representatives for the cosets of $\{0, vw, 2vw, \ldots, (k-2)vw\}$ in $\mathbb{Z}_{(k-1)vw}$. The assertion follows. ∎

As a consequence of the above theorem we find again the mentioned result by Jimbo and Vanstone [12].

Corollary 3 (Jimbo and Vanstone [12]) *Assume that there exists a cyclically resolvable 1-rotational $((k-1)v+1, k, 1)$-BIBD, a cyclically resolvable 1-rotational $((k-1)w+1, k, 1)$-BIBD and a $(w, k+1, 1)$ difference matrix. Then, if* $\gcd(w, k-1) = 1$*, there exists a cyclically resolvable 1-rotational $((k-1)vw+1, k, 1)$-BIBD.*

Corollary 4 *There exists a cyclically resolvable 1-rotational $(v, 3, 1)$-BIBD for all v of the form $2p_1p_2 \ldots p_n + 1$ where each p_j is a prime $\equiv 1$ (mod 12).*

Proof. By Corollary 2 there exists a cyclically resolvable 1-rotational $(2p_j+1, 3, 1)$-BIBD for each $j = 1, \ldots, n$. By Lemma 1, there exists a good $(p_j, 3, 1)$ difference matrix for each $j = 1, \ldots, n$. The assertion follows by iteratively applying Corollary 3. ∎

The following corollary improves a recent result by Anderson and Finizio [3].

Corollary 5 *There exists a cyclically resolvable 1-rotational $(v, 4, 1)$-BIBD for all v of the form $3p_1p_2 \ldots p_n + 1$ where each p_j is a prime $\equiv 1$ (mod 4).*

Proof. By Corollary 1 there exists a cyclically resolvable 1-rotational $(3p_j+1,4,1)$-BIBD for each $j=1,\dots,n$. By Lemma 1, there exists a good $(p_j,4,1)$ difference matrix for each $j=1,\dots,n$. The assertion follows by iteratively applying Corollary 3. ∎

The following example gives a cyclically resolvable (664, 4, 1)-BIBD obtainable by Construction 4.

Example 3 Take the resolvable (39, 3, 4, 1) difference family $\mathcal{D}=\{D_1,D_2,D_3\}$ (constructed in Example 1) whose base blocks are:

$$D_1=\{27,12,31,34\},\ D_2=\{15,24,10,16\},\ D_3=\{30,9,7,19\}.$$

Now, using Theorem 3 with $q=17$, we construct the resolvable $(\mathbb{Z}_3\oplus\mathbb{Z}_{17},\mathbb{Z}_3\oplus\{0\},4,1)$ difference family whose base blocks are:

$\{(0,1),(0,16),(1,4),(1,13)\},\ \{(0,3),(0,14),(1,12),(1,5)\},$

$\{(0,9),(0,8),(1,2),(1,15)\},\quad \{(0,10),(0,17),(1,6),(1,11)\}.$

Using the ring isomorphism $\psi:(a,b)\in\mathbb{Z}_3\oplus\mathbb{Z}_{17}\to(18b-17a)\in\mathbb{Z}_{51}$, the above family may be identified with the (51, 3, 4, 1) difference family

$\mathcal{E}=\{E_1,E_2,E_3,E_4\}$ where

$E_1=\{18,33,4,13\},\ E_2=\{3,48,46,22\},$

$E_3=\{9,42,19,49\},\ E_4=\{27,24,40,28\}.$

Finally, let us apply Construction 4 with $\mathcal{D}$ and $\mathcal{E}$ as above, using the (17, 3, 1) good difference matrix $A=(i(h-1))_{i=1,2,3;h=1,\dots,17}$. In such a way we get a resolvable $(3\cdot 13\cdot 17,3,4,1)$ difference family $\mathcal{F}$ whose base blocks are:

$\{27,12,31,34\}$ $\{15,24,10,16\}$ $\{30,9,7,19\}$
$\{66,90,148,190\}$ $\{54,102,127,172\}$ $\{69,87,124,175\}$
$\{105,168,265,346\}$ $\{93,180,244,328\}$ $\{108,165,241,331\}$
$\{144,246,382,502\}$ $\{132,258,361,484\}$ $\{147,243,358,487\}$
$\{183,324,499,658\}$ $\{171,336,478,640\}$ $\{186,321,475,643\}$
$\{222,402,616,151\}$ $\{210,414,595,133\}$ $\{225,399,592,136\}$
$\{261,480,70,307\}$ $\{249,492,49,289\}$ $\{264,477,46,292\}$
$\{300,558,187,463\}$ $\{288,570,166,445\}$ $\{303,555,163,448\}$
$\{339,636,304,619\}$ $\{327,648,283,601\}$ $\{342,633,280,604\}$
$\{378,51,421,112\}$ $\{366,63,400,94\}$ $\{381,48,397,97\}$
$\{417,129,538,268\}$ $\{405,141,517,250\}$ $\{420,126,514,253\}$
$\{456,207,655,424\}$ $\{444,219,634,406\}$ $\{459,204,631,4\}$
$\{495,285,1,580\}$ $\{483,297,88,562\}$ $\{498,282,85,565\}$
$\{534,363,226,73\}$ $\{522,375,205,55\}$ $\{537,360,202,58\}$
$\{573,441,343,229\}$ $\{561,453,322,211\}$ $\{576,438,319,214\}$
$\{612,519,460,385\}$ $\{600,531,439,367\}$ $\{615,516,436,370\}$
$\{651,597,577,541\}$ $\{639,6,556,523\}$ $\{654,594,553,526\}$

$\{234,429,52,169\}$ $\{39,624,598,286\}$ $\{117,546,247,637\}$ $\{351,312,520,364\}$

We point out that in the h-th row ($h=1,\dots,17$) we have the blocks D_{1h}, D_{2h}, D_{3h}, while the blocks in the last row are $13E_1$, $13E_2$, $13E_3$, $13E_4$.

Developing the blocks of $\mathcal{F}$ (mod $13{\cdot}17$) and adding the block $\{0, 13{\cdot}17, 2{\cdot}13{\cdot}17, \infty\}$, we get the starter parallel class of a cyclically resolvable (664, 4, 1)-BIBD.

References

[1] R. J. R. Abel. Difference families. In *CRC Handbook of Combinatorial Designs* (C. J. Colbourn and J. H. Dinitz (eds.)), CRC Press, Boca Raton, FL, 1996, 270-287.

[2] R. J. R. Abel and M. Greig. BIBDs with small block size. In CRC Handbook of Combinatorial Designs (C. J. Colbourn and J. H. Dinitz (eds.)), CRC Press, Boca Raton, FL, 1996, 41-47.

[3] I. Anderson and N. J. Finizio. Cyclically resolvable designs and triple whist tournaments. *J. Combin. Des.* 1 (1993), 347-358.

[4] T. Beth, D. Jungnickel and H. Lenz. *Design Theory* Cambridge University Press, Cambridge (1993).

[5] M. Buratti. On resolvable difference families. *Des. Codes Cryptogr.* 11 (1997), 11-23.

[6] M. Buratti. Recursive constructions for difference matrices and relative difference families. *J. Combin. Des.*, to appear.

[7] M. Buratti. Some constructions for 1-rotational BIBD's with block size 5. Australas. J. Combin., to appear.

[8] M. J. Colbourn and C. J. Colbourn. Recursive constructions for cyclic block designs. *J. Statist. Plann. Inference* 10 (1984), 97-103.

[9] C. J. Colbourn and W. de Launey. Difference matrices. In *CRC Handbook of Combinatorial Designs* (C. J. Colbourn and J. H. Dinitz (eds.)), CRC Press, Boca Raton, FL, 1996, 287-297.

[10] M. Genma, M. Jimbo and M. Mishima. Cyclic resolvability of cyclic Steiner 2-designs. *J. Combin. Des.* 5 (1997), 177-187.

[11] M. Jimbo. A recursive construction of 1-rotational Steiner 2-designs. *Aequationes Math.* 26 (1983), 184-190.

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

[13] R. Mathon and A. Rosa. $2-(v, k, \lambda)$ designs of small order. In *CRC Handbook of Combinatorial Designs* (C. J. Colbourn and J. H. Dinitz (eds.)), CRC Press, Boca Raton, FL, 1996, 3-41.

[14] E. H. Moore. Tactical Memoranda I-III. *Amer. J. Math.* 18 (1896), 264-303.

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

Marco BURATTI and Fulvio ZUANNI
University of L'Aquila
Department of Electrical Engineering
I - 67040 Monteluco di Roio (AQ)
ITALY
Tel.: ++39 - (0) 862 - 434429
Fax.: ++39 - (0) 862 - 434403
e-mail: buratti@marte.mat.uniroma1.it
e-mail: zuanni@ing.univaq.it