Some constructions for 1-rotational BIBD's with block size 5

Marco Buratti
Dipartimento di Ingegneria Elettrica, Universita' de L'Aquila,
67040 Poggio di Roio (Aq), Italy

Abstract. We give miscellaneous constructions for 1-rotational $(4q+1,5,\lambda)$-BIBD's, being q an odd prime power, investigating their possible resolvability whenever $q \equiv 1 \pmod{10}$. Concerning Steiner 2-designs, the strongest result that we obtain, is the explicit construction of a 1-rotational (4q+1,5,1)-BIBD (with a multiplier of order 5) for each prime $q \equiv 1 \pmod{30}$ such that $(11+5\sqrt{5})/2$ is not a cube (mod q).

As a particular consequence of our constructions, we get new (125,5,1) and new (156,6,1) BIBD's. The only ones with these parameters previously known were those obtainable from the 3-dimensional affine and projective geometries over $\mathbb{Z}_5$.

1. Introduction

We assume familiarity with the concepts of balanced incomplete block design (BIBD) and resolvable balanced incomplete block design (RBIBD).

Australasian Journal of Combinatorics 17(1998), pp.199–227

A $(v+1,k,\lambda)$-BIBD is said to be *1-rotational* over a group G of order v, if admits G as an automorphism group fixing one special point ∞ and acting sharply transitively on the other points.

Existence results on 1-rotational Steiner 2-designs are the following.

Theorem 1.1 (Phelps and Rosa [12]). There exists a 1-rotational $(v+1,3,1)$-BIBD over $\mathbb{Z}_v$ if and only if $v \equiv 2, 8 \pmod{24}$.

Theorem 1.2 (Moore [11]). For any prime power $q \equiv 1 \pmod 4$ there exists a 1-rotational $(3q+1,4,1)$-BIBD over $\mathbb{Z}_3 \oplus \mathbb{F}_q$ being $\mathbb{F}_q$ the field of order q.

Some recursive constructions for 1-rotational Steiner 2-designs with block size 4 are given by Liaw [9].
Greig [8] gives constructions for 1-rotational Steiner 2-designs with block size 6 and 8. Abel and Greig [2] give constructions for 1-rotational Steiner 2-designs with block size 5.
About 1-rotational designs with higher index see e.g. [2, 6, 7].

In this paper we propose miscellaneous constructions for 1-rotational $(4q+1,5,\lambda)$-BIBD's over $\mathbb{Z}_2^2 \oplus \mathbb{F}_q$ or 1-rotational $(4p+1,5,\lambda)$-BIBD's over $\mathbb{Z}_{4p}$, for p an odd prime.

Throughout the paper we will use the following notation.
Notation. For a given prime power q, we denote by ω a primitive root in $\mathbb{F}_q$, and by $\mathbb{F}_q^{(5)}$ the set of ordered quintuples of pairwise distinct elements from $\mathbb{F}_q$.
G will denote a group of order 4 (hence $G = \mathbb{Z}_4$ or $G = \mathbb{Z}_2^2$).
Each element (a,b) of $\mathbb{Z}_2^2$ will be written as a_b.

π will denote the projection of $G \oplus \mathbb{F}_q$ over $\mathbb{F}_q$.

For a given 5-set $A = \{(g_1, x_1), ..., (g_5, x_5)\} \subset G \oplus \mathbb{F}_q$ and a given element w of $\mathbb{F}_q$, we denote by wA the set $\{(g_1, wx_1), ..., (g_5, wx_5)\}$. Also, the list of differences from A will be denoted by ΔA.

For realizing our constructions we will use the following standard method.

Find a family $\mathcal{F}$ of 5-subsets of $G \oplus \mathbb{F}_q$ whose list of differences covers $(G \oplus \mathbb{F}_q) - (G \times \{0\})$ exactly λ times. Take a symbol ∞ and consider the incidence structure $(V, \mathcal{B})$ with point set $V = (G \oplus \mathbb{F}_q) \cup \{\infty\}$ and block family $\mathcal{B}$ consisting in all the translates (under $G \oplus \mathbb{F}_q$) of the members of $\mathcal{F}$ (called *base blocks*) plus λ times all the sets of type $(G \times \{h\}) \cup \{\infty\}$, $h \in \mathbb{F}_q$. This structure is a 1-rotational $(4q+1,5,\lambda)$-BIBD over $G \oplus \mathbb{F}_q$. Using the same notation and terminology as in [5], $\mathcal{F}$ is a $(G \oplus \mathbb{F}_q, G \times \{0\}, 5, 1)$ *difference family*. But here, we will refer to $\mathcal{F}$ as a 1-rotational (4q,5,1) difference family over $G \oplus \mathbb{F}_q$.

Let $\mathcal{F}$ be a 1-rotational (4q,5,1) difference family over $G \oplus \mathbb{F}_q$ and let w be a primitive n-th root of unity in $\mathbb{F}_q$. We say that w is a multiplier of order n of the family $\mathcal{F}$ if whenever $A \in \mathcal{F}$, $wA \in \mathcal{F}$. In such a case we have that the map $\hat{w}$ defined on $(G \oplus \mathbb{F}_q) \cup \{\infty\}$ by the rule $\hat{w}(\infty) = \infty$ and $\hat{w}(g, x) = (g, wx)$ for any $(g, x) \in G \oplus \mathbb{F}_q$, is an automorphism of the BIBD generated by $\mathcal{F}$.

A BIBD is said to be *cyclically resolvable* when it admits a cyclic group of automorphisms acting sharply transitively on a resolution of the BIBD. All the resolvable 1-rotational Steiner 2-designs over $G \oplus \mathbb{F}_q$ that we obtain in this paper admit a resolution on which $\mathbb{F}_q$ acts sharply transitively. Thus, when q is a prime they are cyclically resolvable.

[1] is a paper concerning the construction of cyclically resolvable 1-rotational Steiner 2-designs with block-size 4.

The following lemma is useful for checking the possible resolvability of a BIBD generated by a 1-rotational $(4q,5,\lambda)$ difference family.

Lemma 1.3. Let $\mathcal{F}$ be a 1-rotational $(4q,5,\lambda)$ difference family over $G \oplus \mathbb{F}_q$ and let π be the projection of $G \oplus \mathbb{F}_q$ over $\mathbb{F}_q$. Then the BIBD generated by $\mathcal{F}$ admits a resolution invariant under $G \oplus \mathbb{F}_q$ provided that $\mathcal{F}$ is partitionable in λ subfamilies $\mathcal{F}_0, \mathcal{F}_1, \ldots, \mathcal{F}_{\lambda-1}$ satisfying the following condition:

$$\bigcup_{A \in \mathcal{F}_j} \pi(A) = \mathbb{F}_q^* \text{ for } j = 0, 1, \ldots, \lambda-1.$$

Proof. If the above condition holds, it is easily seen that

$$\mathcal{R}_{j,h} = \{A + (g, h) \mid A \in \mathcal{F}_j; g \in G\} \cup \{(G \times \{h\}) \cup \{\infty\}\}$$

$$j = 0, 1, \ldots, \lambda-1; h \in \mathbb{F}_q,$$

are the parallel classes of a resolution of the BIBD generated by $\mathcal{F}$. Obviously, this resolution is invariant under $G \oplus \mathbb{F}_q$. □

2. 1-rotational $(4q,5,\lambda)$-DF's over $\mathbb{Z}_2^2 \oplus \mathbb{F}_q$. A generalization of a construction by Abel and Greig

Abel and Greig [2] have recently given constructions for 1-rotational $(4q+1,5,1)$-BIBD's over $\mathbb{Z}_2^2 \oplus \mathbb{F}_q$ starting from two blocks of type $\{(0_0, x_1), (0_0, x_2), (0_0, x_3), (1_0, x_4), (0_1, x_5)\}$ and $\{(0_0, y_1), (1_0, y_2),$

$(1_0,y_3)$, $(0_1, y_4)$, $(0_1, y_5)\}$. Here, we slightly improve their results and generalize their construction considering also the case where $\lambda = 5$. In this section, for a fixed prime power q, with each 10tuple $X = (x_1, ..., x_{10}) \in \mathbb{F}_q^{10}$ we associate the following quintuples:

$$X_{0,0} = (x_2-x_1, x_3-x_1, x_3-x_2, x_8-x_7, x_{10}-x_9),$$

$$X_{1,0} = (x_4-x_1, x_4-x_2, x_4-x_3, x_7-x_6, x_8-x_6),$$

$$X_{0,1} = (x_5-x_1, x_5-x_2, x_5-x_3, x_9-x_6, x_{10}-x_6),$$

$$X_{1,1} = (x_5-x_4, x_9-x_7, x_9-x_8, x_{10}-x_7, x_{10}-x_8).$$

Theorem 2.1. There exists a 1-rotational (4q+1,5,5)-BIBD over $\mathbb{Z}_2^2 \oplus \mathbb{F}_q$ for any odd prime power $q \geq 5$.

Proof. Fix $X = (x_1, ..., x_{10}) \in \mathbb{F}_q^{10}$ in such a way that both $(x_1, x_2, x_3, x_4, x_5)$ and $(x_6, x_7, x_8, x_9, x_{10})$ belong to $\mathbb{F}_q^{(5)}$. Consider the 5-subsets A_1, A_2 of $\mathbb{Z}_2^2 \oplus \mathbb{F}_q$ defined as follows:

$$A_1 = \{(0_0, x_1), (0_0, x_2), (0_0, x_3), (1_0, x_4), (0_1, x_5)\}$$

$$A_2 = \{(0_0, x_6), (1_0, x_7), (1_0, x_8), (0_1, x_9), (0_1, x_{10})\}$$

It is easily seen that

$$\Delta A_1 \cup \Delta A_2 = \{0_0\}\times(\pm X_{0,0}) \cup \{1_0\}\times(\pm X_{1,0}) \cup \{0_1\}\times(\pm X_{0,1}) \cup \{1_1\}\times(\pm X_{1,1})$$

Let $S = \{\omega^i \mid 0 \leq i < \frac{q-1}{2}\}$. Since $\pm S = \mathbb{F}_q^*$ and each $X_{i,j}$ is a quintuple of non-zero elements of $\mathbb{F}_q$, we have that $(\pm X_{i,j})S$ covers $\mathbb{F}_q^*$ exactly 5 times. It follows that the differences from the family

$$\mathcal{F} = (sA_i \mid s \in S, i = 1, 2)$$

cover $(\mathbb{Z}_2^2 \oplus \mathbb{F}_q) - (\mathbb{Z}_2^2 \times \{0\})$ exactly 5 times, namely $\mathcal{F}$ is a 1-rotational (4q,5,5) difference family. The assertion follows. □

The smallest designs that we obtain applying the previous theorem have parameters (21,5,5) and (29,5,5). In the parameter tables of small BIBD's given by Mathon and Rosa [10] it is pointed out that there are at least 10^9 non-isomorphic known (21,5,5)-BIBDs. We do not know if our 1-rotational (21,5,5)-BIBD's are among them or not. However, our 1-rotational (29,5,5)-BIBD's are new. In fact, according to Mathon and Rosa again, the only known (29,5,5)-BIBD (discovered by Hanani) is simple. Instead, our (29,5,5)-BIBD's have 7 blocks repeated 5 times.

Theorem 2.2. There exists a 1-rotational (4q+1,5,5)-RBIBD over $\mathbb{Z}_2^2 \oplus \mathbb{F}_q$ for any prime power $q = 10t+1$.

Proof. Construct a 1-rotational (4q,5,5) difference family $\mathcal{F}$ as in the proof of Theorem 2.1 but choosing as X an arbitrary ordering of the set of 10th roots of unity in $\mathbb{F}_q$. For $j = 0, 1, ..., 4$, set $S_j = \{\omega^{i+jt} \mid 0 \leqslant i < t\}$ and $\mathcal{F}_j = (sA_i \mid s \in S_j,\ i = 1, 2)$. Since the S_j's partition S and $\pm S = \mathbb{F}_q^*$, we have that the $\mathcal{F}_j$'s partition $\mathcal{F}$. Also, we have $\bigcup_{A \in \mathcal{F}_j} \pi(A) = S_jX$. On the other hand, since X is the set of 10th roots of unity and S_j is a system of representatives for the cosets of these roots for any j, we have that $S_jX = \mathbb{F}_q^*$. Then, applying Lemma 1.3 the assertion follows. □

In the case where $q \equiv 1 \pmod{10}$ again, a more appropriate choice of the 10tuple X could lead to a 1-rotational, possibly resolvable, (4q+1,5,1)-BIBD. In fact we have:

Theorem 2.3. Let $q = 10t+1$ be a prime power and let 2^e be the largest power of 2 dividing t. A 10tuple $X \in \mathbb{F}_q^{10}$ may possibly satisfy some of the following conditions:

i) Each $X_{i,j}$ is a system of representatives for the cosets of 5th powers in $\mathbb{F}_q$.

ii) $X = \pm Y$ where Y is a system of representatives for the cosets of 5th powers in $\mathbb{F}_q$.

iii) Each $X_{i,j}$ is a system of representatives for the cosets of 2^e5th powers in the group of 2^eth powers.

iv) X is a system of representatives for the cosets of 2^e10th powers in the group of 2^eth powers.

We have:

If (i) holds, then there exists a 1-rotational (4q,5,1) difference family $\mathcal{F}$ without non-trivial multipliers.

If (i) and (ii) hold, then the BIBD generated by $\mathcal{F}$ is resolvable.

If (iii) holds, then there exists a 1-rotational (4q,5,1) difference family $\mathcal{F}'$ admitting $\omega^{2^e 10}$ as a multiplier of order $t/2^e$.

If (iii) and (iv) hold, then the BIBD generated by $\mathcal{F}'$ is resolvable.

Proof. First of all, starting from X, construct the sets A_1, A_2 as in the proof of Theorem 2.1.

Assume that (i) holds and set $S = \{\omega^{5i} \mid 0 \leqslant i < t\}$. As $\pm S$ is the set of 5th powers in $\mathbb{F}_q$, we have that $(\pm X_{i,j})S = \mathbb{F}_q^*$ for each $X_{i,j}$. It follows that the family $\mathcal{F} = (sA_i \mid s \in S,\ i = 1, 2)$ is a 1-rotational (4q,5,1) difference family.

Assume that (i) and (ii) hold and let $\mathcal{F}$ be the difference family described above. We have: $\bigcup_{A \in \mathcal{F}} \pi(A) = SX = \pm SY$. On the other hand, since $\pm S$ is the group of 5th powers and Y is a system of

representatives for the cosets of this group, we have $\pm SY = \mathbb{F}_q^*$. Then the assertion follows from Lemma 1.3.

Assume that (iii) holds and set $S' = \{\omega^{2^e 10i + j} \mid 0 \leqslant i < t/2^e; 0 \leqslant j < 2^e\}$, namely $S' = TU$ where $T = \{\omega^{2^e 10i} \mid 0 \leqslant i < t/2^e\}$ is the group of $2^e 10$th powers and $U = \{\omega^j \mid 0 \leqslant j < 2^e\}$ is a system of representatives for the cosets of the group, say V, of 2^eth powers. Since $\pm T$ is the group of $2^e 5$th powers and each $X_{i,j}$ is a system of representatives for the cosets of this group in V, we have that $(\pm X_{i,j})T = V$ for each $X_{i,j}$. This implies that $(\pm X_{i,j})S' = (\pm X_{i,j})TU = VU = \mathbb{F}_q^*$ for each $X_{i,j}$. It follows that the family $\mathcal{F}' = (s'A_i \mid s' \in S', i = 1, 2)$ is a 1-rotational (4q,5,1) difference family.

Assume that (iii) and (iv) hold and let $\mathcal{F}'$ be the difference family described above. We have: $\bigcup_{A \in \mathcal{F}'} \pi(A) = S'X = (TU)X$. On the other hand we have $TX = V$ because X is a system of representatives for the cosets of T in V. Hence $(TU)X = UV = \mathbb{F}_q^*$. Then, applying Lemma 1.3 the assertion follows. □

Remark 2.4. Needless to say that for realizing 1-rotational BIBD's or RBIBD's using the previous theorem, one needs the help of a computer. Abel and Greig [2], essentially using conditions (i) and (ii), find a (4q+1,5,1)-RBIBD for all primes $q \equiv 1 \pmod{10}$ with $q \leqslant 1.151$ with the only exceptions of $q = 11$, $q = 31$ and $q = 41$.

Anyway, Theorem 2.3 is a slight improvement of the construction given by Abel and Greig for two reasons.

The first reason is that Theorem 2.3 also succeds for $q = 31$. The second reason is that, using (iii) and (iv) we obtain RBIBD's possessing a multiplier group of order $t/2^e$ that the RBIBD's of Abel and Greig do not generally have.

In the following table we report the primes $q \leq 1.151$ for which there exists a 10tuple X, also reported, satisfying conditions (iii) and (iv) of Theorem 2.3. We conjecture that such a 10tuple X always exists for primes $q = 10t+1$ having t odd (namely $e = 0$) with the only exception of $q = 11$. The first prime $q = 10t+1$ appearing in the table and having t even is $q = 421$.

q	X
31	(1, 2, 4, 11, 16, 12, 9, 13, 6, 23)
71	(1, 2, 5, 6, 14, 7, 23, 47, 31, 43)
131	(1, 2, 4, 7, 8, 13, 14, 47, 31, 43)
151	(1, 3, 14, 9, 11, 17, 46, 126, 108, 139)
191	(1, 2, 4, 8, 11, 3, 95, 112, 28, 174)
211	(1, 2, 4, 7, 9, 3, 12, 53, 69, 141)
251	(1, 2, 14, 7, 11, 3, 36, 117, 165, 184)
271	(1, 2, 4, 6, 7, 3, 19, 113, 89, 189)
311	(1, 2, 4, 6, 12, 11, 22, 95, 204, 221)
331	(1, 2, 5, 6, 10, 8, 20, 44, 108, 265)
421	(1, 4, 16, 344, 343, 64, 418, 48, 401, 363)
431	(1, 5, 26, 35, 38, 7, 29, 69, 107, 279)
461	(1, 408, 172, 367, 311, 4, 294, 350, 58, 91)
491	(1, 2, 8, 4, 10, 5, 21, 65, 237, 312)
541	(1, 4, 16, 170, 316, 64, 353, 463, 139, 159)
571	(1, 2, 7, 10, 15, 5, 30, 65, 96, 307)
631	(1, 2, 4, 14, 19, 6, 8, 24, 247, 506)
661	(1, 4, 16, 493, 47, 64, 97, 617, 55, 562)
691	(1, 2, 5, 6, 7, 8, 10, 25, 138, 208)
701	(1, 64, 472, 591, 297, 4, 610, 100, 154, 585)
751	(1, 2, 6, 7, 13, 4, 12, 40, 39, 699)

811 (1, 2, 4, 8, 9, 6, 15, 88, 96, 366)

821 (1, 64, 258, 785, 368, 4, 49, 799, 199, 45)

911 (1, 3, 20, 11, 21, 9, 34, 100, 209, 554)

941 (1, 256, 217, 39, 465, 4, 600, 802, 463, 228)

971 (1, 2, 12, 6, 17, 9, 34, 100, 209, 554)

991 (1, 2, 4, 11, 20, 3, 27, 39, 330, 465)

1021 (1, 100, 301, 922, 254, 811, 744, 563, 814, 788)

1031 (1, 2, 5, 6, 7, 8, 28, 41, 201, 228)

1051 (1, 2, 6, 7, 10, 3, 17, 46, 21, 785)

1061 (1, 64, 684, 584, 501, 4, 880, 784, 609, 41)

1091 (1, 2, 8, 4, 14, 7, 23, 152, 116, 1069)

1151 (1, 2, 4, 9, 13, 3, 26, 103, 61, 411)

1.481 is the first prime equivalent to 41 (mod 80) (namely having e = 2) for which conditions (iii) and (iv) succeed in finding a (4q+1,5,1)-RBIBD. It suffices to use the 10tuple X = (1, 26, 1.251, 1.033, 1.244, 81, 162, 1.332, 1.021, 149).

3. 1-rotational (4q,5,λ)-DF's over $Z_2^2 \oplus F_q$ with a multiplier of order 5

In this section, given a prime power q and a fixed primitive 5th root of unity ε in F_q, we associate the following triples with each $X = (x_1, x_2, x_3, x_4, x_5) \in F_q^{(5)}$:

$$X_{0,0} = (x_2-x_1, \varepsilon-1, \varepsilon^2-1), \qquad X_{1,0} = (x_3-x_1, x_3-x_2, x_5-x_4),$$

$$X_{0,1} = (x_4-x_1, x_4-x_2, x_5-x_3) \qquad X_{1,1} = (x_5-x_1, x_5-x_2, x_4-x_3).$$

Also, we set $X^+ = (1, x_1, x_2, x_3, x_4, x_5)$.

The reader will may easily check that all the BIBD's here obtained arise from 1-rotational difference families admitting ε as a multiplier.

Theorem 3.1. There exists a 1-rotational (4q+1,5,3)-BIBD over $\mathbb{Z}_2^2 \oplus \mathbb{F}_q$ for any prime power $q \equiv 1 \pmod{10}$.

Proof. Fix an arbitrary quintuple $X \in \mathbb{F}_q^{(5)}$ and consider the 5-subsets A, B of $\mathbb{Z}_2^2 \oplus \mathbb{F}_q$ defined as follows:

$$A = \{(0_0, 1), (0_0, \varepsilon), (0_0, \varepsilon^2), (0_0, \varepsilon^3), (0_0, \varepsilon^4)\}$$

$$B = \{(0_0, x_1), (0_0, x_2), (1_0, x_3), (0_1, x_4), (1_1, x_5)\}$$

It is easily seen that:

$$\Delta A = \{0_0\} \times (\pm\langle\varepsilon\rangle\{\varepsilon\text{-}1, \varepsilon^2\text{-}1\})$$

$$\Delta B = \{0_0\}\times\{\pm(x_2\text{-}x_1)\} \cup \{1_0\}\times(\pm X_{1,0}) \cup \{0_1\}\times(\pm X_{0,1}) \cup \{1_1\}\times(\pm X_{1,1})$$

Setting $A_0 = A$ and $A_i = \varepsilon^{i-1}B$ for $1 \leqslant i \leqslant 5$, we have that:

$$\bigcup_{0\leqslant i\leqslant 5} \Delta A_i = \{0_0\}\times(\pm\langle\varepsilon\rangle X_{0,0}) \cup \{1_0\}\times(\pm\langle\varepsilon\rangle X_{1,0}) \cup \{0_1\}\times(\pm\langle\varepsilon\rangle X_{0,1}) \cup \{1_1\}\times(\pm\langle\varepsilon\rangle X_{1,1}).$$

Let $S = \{\omega^i \mid 0 \leqslant i < \frac{q-1}{10}\}$. Since $\pm\langle\varepsilon\rangle$ is the group of 10th roots of unity in $\mathbb{F}_q$ and S is a complete system of representatives for the cosets of this group, we have that $\pm\langle\varepsilon\rangle S = \mathbb{F}_q^*$. Hence, the list $(\pm\langle\varepsilon\rangle X_{i,j})S$ covers $\mathbb{F}_q^*$ exactly 3 times for each $X_{i,j}$. It follows that the list of differences from the family

$$\mathcal{F} = (sA_i \mid s \in S, 0 \leqslant i \leqslant 5)$$

covers $(\mathbb{Z}_2^2 \oplus \mathbb{F}_q) - (\mathbb{Z}_2^2 \times \{0\})$ exactly 3 times, namely $\mathcal{F}$ is a 1-rotational (4q,5,3) difference family. The assertion follows. □

Theorem 3.2. There exists a 1-rotational (4q+1,5,3)-RBIBD over $\mathbb{Z}_2^2 \oplus \mathbb{F}_q$ for any prime power $q \equiv 1 \pmod{30}$.

Proof. Construct a 1-rotational (4q,5,3) difference family $\mathcal{F}$ as in the proof of Theorem 3.1, but choosing the quintuple X in such a way that X^+ is a system of representatives for the cosets of $<\varepsilon>$ in the group of 30th roots of unity in $\mathbb{F}_q$. For j = 0, 1, 2, set $S_j = \{\omega^{i+jt} \mid 0 \leqslant i < \frac{q-1}{30}\}$ and $\mathcal{F}_j = (sA_i \mid s \in S_j, i = 1, 2)$. Since the S_j's partition S, we have that the $\mathcal{F}_j$'s partition $\mathcal{F}$. Also, we have $\bigcup_{A \in \mathcal{F}_j} \pi(A) = S_j X^+ <\varepsilon>$. But $X^+ <\varepsilon>$ is the set of 30th roots of unity and S_j is a system of representatives for the cosets of these roots, so that $S_j X^+ <\varepsilon> = \mathbb{F}_q^*$. Then, applying Lemma 1.3 the assertion follows. □

Now, in order to give our strongest result, we need the following lemmas.

Lemma 3.3. Let $q \equiv 1 \pmod 6$ be a prime, $q > 7$. Then there exists $X \in \mathbb{Z}_q^{(5)}$ such that each of the lists $X_{1,0}$, $X_{0,1}$, $X_{1,1}$ is a system of representatives for the cosets of the cubes (mod q).

Proof. Let *ind* be the map from $\mathbb{Z}_q^*$ into $\mathbb{Z}_{q-1}$ defined by $\text{ind}(\omega^i) = i$. Of course, in order that a 3-subset {a, b, c} of $\mathbb{Z}_q^*$ is a system of representatives for the cosets of the cubes (mod q), we should have $\text{ind}(\{a, b, c\}) = \mathbb{Z}_3 \pmod 3$. Set:

$\text{ind}(2) \equiv h \pmod 3$; $\text{ind}(3) \equiv i \pmod 3$; $\text{ind}(5) \equiv j \pmod 3$.

In the following table we exibhit a working quintuple $X \in \mathbb{Z}_q^{(5)}$, i.e. such that $X_{1,0}$, $X_{0,1}$, $X_{1,1}$ satisfy the condition of the lemma, for each

possible triple (h, i, j) with the only exceptions of the triples (0, 0, 0), (1, 2, 1) and (2, 1, 2).

(h, i, j)	**X**
(0, 0, 1) and (0, 0, 2)	(0, 9, -15, 25, 225)
(0, 1, 0) and (0, 2, 0)	(0, 8, 3, 9, 18)
(0, 1, 1) and (0, 2, 2)	(0, 6, 9, 10, 18)
(0, 1, 2) and (0, 2, 1)	(0, 2, 5, 8, 10)
(1, 0, 0) and (2, 0, 0)	(0, 9, 4, 36, 54)
(1, 0, 1) and (2, 0, 2)	(0, 3, 2, 8, 12)
(1, 0, 2) and (2, 0, 1)	(0, 2, 4, 5, 6)
(1, 1, 0) and (2, 2, 0)	(0, 5, 4, 8, 10)
(1, 1, 1) and (2, 2, 2)	(0, 5, 1, 4, 6)
(1, 1, 2) and (2, 2, 1)	(0, 3, 1, 2, 6)
(1, 2, 0) and (2, 1, 0)	(0, 6, 9, 10, 15)
(1, 2, 2) and (2, 1, 1)	(0, 3, 1, 2, 5)

For finding a working X also in the case where (h, i, j) = (1, 2, 1) or (2, 1, 2), we have to involve also ind(7):

for ind(7) = 0 take X = (0, 1, 2, 5, 9);

for ind(7) = 1 take X = (0, 1, 2, 5, 8);

for ind(7) = 2 take X = (0, 1, 2, 3, 10).

In such a way, we have found a quintuple X satisfying the condition of the lemma in the case where 2, 3 and 5 are not all cubes (mod q). Now, suppose that 2 and 3 are cubes (mod q) and let p be the smallest prime which is not a cube (mod q). Then, each positive integer smaller than p is a cube (mod q). Consider the quintuple $X \in \mathbb{Z}_q^{(5)}$ defined by:

$$X = (0, 9, 3\sigma p, p^2, 9p^2)$$

with $\sigma = 1$ or -1 according to whether $p \equiv 3$ or $1 \pmod 4$ respectively.

We have:

$$X_{1,0} = (x_3-x_1, x_3-x_2, x_5-x_4) = (3\sigma p, 3\sigma(p-3\sigma), 8p^2)$$

$$X_{0,1} = (x_4-x_1, x_4-x_2, x_5-x_3) = (p^2, (p-3)(p+3), 3p(3p-\sigma))$$

$$X_{1,1} = (x_5-x_1, x_5-x_2, x_4-x_3) = (9p^2, 9(p-1)(p+1), p(p-3\sigma))$$

We can write $p\pm 3 = 2(p\pm 3)/2$, $p\pm 1 = 2(p\pm 1)/2$, $p-3\sigma = 4(p-3\sigma)/4$ and $3p-\sigma = 4(3p-\sigma)/4$. On the other hand the integers $(p\pm 3)/2$, \f((p\pm 1)/2, $(p-3\sigma)/4$ and $(3p-\sigma)/4$ are cubes (mod q) because they are smaller than p. It follows that $p\pm 3$, $p\pm 1$, $p-3\sigma$ and $3p-\sigma$ are all cubes (mod q) and hence that $X_{1,0}$, $X_{0,1}$, $X_{1,1}$ are systems of representatives for the cosets of the cubes (mod q). The assertion follows. □

Lemma 3.4. Let $q \equiv 1 \pmod{30}$ be a prime power and let ε be a primitive 5th root of unity in $\mathbb{F}_q$. Then $\varepsilon-1$ and ε^2-1 lie in distinct cosets of the cubes in $\mathbb{F}_q$ if and only if $(11+5\sqrt{5})/2$ is not a cube in $\mathbb{F}_q$.

Proof. Firstly note that $\varepsilon-1$ and ε^2-1 lie in the same coset of the cubes in $\mathbb{F}_q$ if and only if $\varepsilon+1$ is a cube in $\mathbb{F}_q$. On the other hand $\varepsilon+1$ is a cube if and only if the set $C = \{\pm(\varepsilon+1)^5, \pm(\varepsilon^2+1)^5\}$ is contained in the set of cubes. So, for proving the lemma it is enough to show that $(11+5\sqrt{5})/2$ belongs to C. By means of a trivial calculation we have that (cf. also [4, p.19]):

$$(\varepsilon+1)^5(\varepsilon^2+1)^5 = -1 \qquad (\varepsilon+1)^5 + (\varepsilon^2+1)^5 = -11.$$

This implies that $(\varepsilon+1)^5$ and $(\varepsilon^2+1)^5$ are the roots of the equation $x^2+11x-1 = 0$ in $\mathbb{F}_q$. The assertion easily follows. □

Lemma 3.5. Let $q = 30t+1$ be a prime such that $(11+5\sqrt{5})/2$ is not a cube (mod q). Then there exists $X \in \mathbb{Z}_q^{(5)}$ such that each of the lists $X_{0,0}$, $X_{1,0}$, $X_{0,1}$, $X_{1,1}$ is a system of representatives for the cosets of the cubes (mod q).

Proof. Using Lemma 3.3, choose $Y \in \mathbb{Z}_q^{(5)}$ in such a way that $Y_{1,0}$, $Y_{0,1}$, $Y_{1,1}$ are systems of representatives for the cosets of the cubes (mod q). By Lemma 3.4, $\varepsilon-1$ and ε^2-1 lie in distinct cosets of the cubes (mod q). This allows us to choose $c \in \mathbb{Z}_q^*$ in such a way that $\{c(y_2-y_1), \varepsilon-1, \varepsilon^2-1\}$ is also a system of representatives for the cosets of the cubes (mod q). It follows that the *normalized* quintuple $X = cY$ is such that all the $X_{i,j}$'s are systems of representatives for the cosets of the cubes (mod q). □

Theorem 3.6. Let $q = 30t+1$ be a prime such that $(11+5\sqrt{5})/2$ is not a cube (mod q). Then there exists a 1-rotational (4q+1,5,1)-BIBD.

Proof. By Lemma 3.5, there exists $X \in \mathbb{Z}_q^{(5)}$ such that all the $X_{i,j}$'s are systems of representatives for the cosets of the cubes (mod q). Using such a quintuple X, consider the sets A_0, A_1, ..., A_5 defined like in the proof of Theorem 3.1 and set $S = \{\omega^{3i} \mid 0 \leqslant i < t\}$. It is easily seen that $\pm\langle\varepsilon\rangle S$ is the set of cubes (mod q) so that $(\pm\langle\varepsilon\rangle X_{i,j})S = \mathbb{Z}_q^*$ for all the $X_{i,j}$'s.

It follows that

$$\mathcal{F} = (sA_i \mid s \in S, 0 \leqslant i \leqslant 5)$$

is a 1-rotational (4q,5,1) difference family. The assertion follows. □

Remark 3.7. Under the same hypothesis of the above theorem, a slightly different 1-rotational (4q,5,1) difference family can be realized in the case where t is odd. This family is $\mathcal{F}' = (s'A_i \mid s' \in S', 0 \leqslant i \leqslant 5)$ where $S' = \{\omega^{6i} \mid 0 \leqslant i < t\}$. In fact, if t is odd, the quintuple X used in the proof of Theorem 3.6 is such that $\pm X_{i,j}$ is a system of representatives for the cosets of the 6th powers (mod q) for each pair $(i, j) \in \{0, 1\}^2$. On the other hand, the set of 6th powers is given by $<\varepsilon>S'$ and hence $(\pm<\varepsilon>X_{i,j})S' = \mathbb{Z}_q^*$.

Note that $\mathcal{F}'$ admits ω^6 as a multiplier of order 5t.

Theorem 3.8. Let $q \equiv 1 \pmod{30}$ be a prime such that $(11+5\sqrt{5})/2$ is not a cube (mod q). Then there exists a 1-rotational (4q+1,5,1)-RBIBD if one of the following conditions holds:

(i) $\exists\ X = (a, -a, -1, b, -b) \in \mathbb{Z}_q^{(5)}$ such that the $X_{i,j}$'s and $\{1, a, b\}$ are systems of representatives for the cosets of cubes (mod q).

(ii) t is odd and $\exists\ X \in \mathbb{Z}_q^{(5)}$ such that the $X_{i,j}$'s are systems of representatives for the cosets of the cubes (mod q) and X^+ is a system of representatives for the cosets of 6th powers (mod q).

Proof. Let $\mathcal{F}$ be the 1-rotational (4q,5,1) difference family obtainable applying Theorem 3.6 with a quintuple X satisfying (i). We have: $\bigcup_{A \in \mathcal{F}} \pi(A) = SX^+<\varepsilon> = \pm S\{1, a, b\}<\varepsilon>$. On the other hand, since $\pm S<\varepsilon>$ is the set of cubes and $\{1, a, b\}$ a system of representatives for the cosets of the cubes, we have that $\pm S\{1, a, b\}<\varepsilon> = \mathbb{Z}_q^*$. Then, applying Lemma 1.3 the assertion follows.

Now assume that t is odd and let $\mathcal{F}'$ be the 1-rotational (4q,5,1) difference family obtainable applying Remark 3.7 with a quintuple X satisfying (ii). We have: $\bigcup_{A \in \mathcal{F}} \pi(A) = S'X^+<\varepsilon>$. So, since $S'<\varepsilon>$ is the group of 6th powers and X^+ is a system of representatives for the cosets of

this group, we have $S'X^+<\varepsilon> = \mathbb{Z}_q^*$. Then, applying Lemma 1.3 the assertion follows. □

As application of the above theorem, we find a 1-rotational (4q+1,5,1)-RBIBD (with a multiplier of order at least 5) for any prime $q = 30t+1 < 1.000$ such that $(11+5\sqrt{5})/2$ is not a cube (mod q) with the only exception of $q = 61$. In fact, in the next table we exibhit a pair (a, b) satisfying (i) or a quintuple X satisfying (ii) for each of these primes.

q	(a, b)	X
31		(3, 29, 20, 25, 26)
181	(32, 47)	
211	(4, 16)	
241	(18, 19)	
271	(6, 50)	
421	(17, 31)	
571		(3, 243, 9, 27, 260)
601	(5, 70)	
631	(22, 23)	
691		(3, 81, 9, 27, 206)
751	(14, 29)	
991		(6, 216, 36, 311, 363)

4. A variant construction for 1-rotational Steiner 2-designs

Here, by means of an additional construction, given a prime $q \equiv 1$ (mod 30) we show that even in the case where $(11+5\sqrt{5})/2$ is a cube

(mod q), there are good chances of realizing a 1-rotational (4q,5,1) difference family starting from two blocks of type $\{(0_0, y_1), (0_0, y_2), (0_0, y_3), (0_0, y_4), (0_0, y_5)\}$ and $\{(0_0, x_1), (0_0, x_2), (1_0, x_3), (0_1, x_4), (1_1, x_5)\}$.

Theorem 4.1. There exists a 1-rotational (4q+1,5,1)-BIBD over $\mathbb{Z}_2^2 \oplus \mathbb{Z}_q$ for any prime $q \equiv 1 \pmod{30}$ but $q \not\equiv 1 \pmod{150}$, provided that there exists a quintuple $Y \in \mathbb{Z}_q^{(5)}$ such that $\mathrm{ind}(y_j - y_i \mid 0 \leqslant i < j \leqslant 5) = \mathbb{Z}_{15} - \{0, 3, 6, 9, 12\} \pmod{15}$.

Proof. Fix an arbitrary quintuple Z satisfying the hypothesis of Lemma 3.3. Then consider the quintuple $X = \frac{1}{z_2 - z_1} Z$. Note that X also satisfies the hypothesis of Lemma 3.3 and, moreover, that $x_2 - x_1 = 1$. Set:

$$L_{0,0} = \{y_j - y_i \mid 0 \leqslant i < j \leqslant 5\} \cup \langle \varepsilon \rangle$$

$$L_{i,j} = \langle \varepsilon \rangle X_{i,j} \qquad \text{for } (i, j) \in \{0, 1\}^2 - \{(0, 0)\}.$$

Since $q \not\equiv 1 \pmod{150}$, we have that $\mathrm{ind}(\langle \varepsilon \rangle) = (0, 3, 6, 9, 12) \pmod{15}$. This and the hypothesis on Y imply that $\mathrm{ind}(L_{0,0}) = \mathbb{Z}_{15} \pmod{15}$. Also, for $(i, j) \in \{0, 1\}^2 - \{(0, 0)\}$, since $X_{i,j}$ is a system of representatives for the cosets of cubes (mod q), we have that $\mathrm{ind}(L_{i,j}) = \mathbb{Z}_{15} \pmod{15}$. In other words, all the $L_{i,j}$'s are systems of representatives for the cosets of 15th powers (mod q).

Now, consider the 5-subsets $A_0, A_1, \ldots, A_6$ of $\mathbb{Z}_2^2 \oplus \mathbb{Z}_q$ defined as follows:

$$A_0 = \{(0_0, y_1), (0_0, y_2), (0_0, y_3), (0_0, y_4), (0_0, y_5)\}$$

$$A_i = \varepsilon^{i-1}\{(0_0, x_1), (0_0, x_2), (1_0, x_3), (0_1, x_4), (1_1, x_5)\}, \quad 1 \leqslant i \leqslant 5$$

We have:

$$\bigcup_{0\leq i\leq 5} \Delta A_i = \{0_0\}\times(\pm L_{0,0}) \cup \{1_0\}\times(\pm L_{1,0}) \cup \{0_1\}\times(\pm L_{0,1}) \cup \{1_1\}\times(\pm L_{1,1})$$

Let $S = \{\omega^{15i} \mid 0 \leq i < (q-1)/30\}$. Since $\pm S$ is the group of 15th powers (mod q) and each $L_{i,j}$ is a set of representatives for the cosets of this group, we have $(\pm L_{i,j})S = \mathbb{Z}_q^*$ for each $L_{i,j}$. It follows that the list of differences from the family

$$\mathcal{F} = (sA_i \mid s \in S, 0 \leq i \leq 5)$$

covers $(\mathbb{Z}_2^2 \oplus \mathbb{Z}_q) - (\mathbb{Z}_2^2 \times \{0\})$ exactly once, namely $\mathcal{F}$ is a 1-rotational (4q,5,1) difference family. The assertion follows. □

Remark 4.2. The difference families obtainable using the above theorem generally are without non-trivial multipliers. But, under the same hypothesis of the theorem, we have that in the case where t is odd the family $\mathcal{F}' = (s^2A_i \mid s \in S, 0 \leq i \leq 5)$ is a (4q,5,1) difference family admitting ω^{30} as a multiplier of order t.

As an example, consider the prime q = 541. For this prime we cannot use Theorem 3.6 since $(11+5\sqrt{5})/2$ is a cube (mod 541). Anyway, it is easy to check that Y = (0, 16, 25, 28, 47) is a quintuple for which Theorem 4.1 succeeds in finding a 1-rotational (4q+1,5,1)-BIBD.

5. 1-rotational (4p,5,λ)-DF's over $\mathbb{Z}_{4p}$

The aim of constructing 1-rotational designs with block size 5 over $\mathbb{Z}_{4p}$ appears more difficult than over $\mathbb{Z}_2^2 \oplus \mathbb{Z}_p$. In this section p will

always denote an odd prime and $\mathbb{Z}_{4p}$ will be identified with the ring $\mathbb{Z}_4 \oplus \mathbb{Z}_p$.

Theorem 5.1. There exists a 1-rotational (4p+1,5,5)-BIBD over $\mathbb{Z}_{4p}$ for any prime $p > 5$.

Proof. Consider the 5-subsets A, B of $\mathbb{Z}_4 \oplus \mathbb{Z}_p$ defined as follows:

$$A_1 = \{(0, 0), (0, 1), (0, 2), (1, 3), (3, 4)\}$$

$$A_2 = \{(0, 0), (1, -1), (1, 4), (3, 2), (3, -2)\}$$

We have:

$$\Delta A_1 \cup \Delta A_2 = \{0\}\times L_0 \cup \{1\}\times L_1 \cup \{2\}\times L_2 \cup \{3\}\times L_3$$

where L_1, L_2, L_3, L_4 are the following lists of elements of $\mathbb{Z}_p^*$:

$L_0 = \pm(1, 1, 2, 5, 4)$ $\quad L_1 = L_3 = \pm(1, 2, 2, 3, 4)$ $\quad L_2 = \pm(1, 1, 2, 3, 6)$.

Let $S = \{\omega^i \mid 0 \leqslant i < \frac{q-1}{2}\}$. Since $\pm S = \mathbb{Z}_p^*$, we have that the list L_iS covers $\mathbb{Z}_p^*$ exactly 5 times, i = 0, 1, 2, 3. It follows that

$$\mathcal{F} = (sA_i \mid s \in S, i = 1, 2)$$

is a 1-rotational (4p,5,5) difference family. The assertion follows. □

With similar argumentations to those used in Theorem 2.3, one can prove the following theorem:

Theorem 5.2. Let $p = 10t+1$ be a prime and let 2^e be the largest power of 2 dividing t. Let $X \in \mathbb{Z}_p^{10}$ such that each of the lists

$\pm(x_2-x_1, x_3-x_1, x_3-x_2, x_8-x_7, x_{10}-x_9)$

$(x_4-x_1, x_4-x_2, x_4-x_3, x_1-x_5, x_2-x_5, x_3-x_5, x_7-x_6, x_8-x_6, x_6-x_9, x_6-x_{10})$

$\pm(x_5-x_4, x_9-x_7, x_9-x_8, x_{10}-x_7, x_{10}-x_8)$

is a system of representatives for the cosets of 2^e10th powers in the group of 2^eth powers.

Then, setting

$A_1 = \{(0, x_1), (0, x_2), (0, x_3), (1, x_4), (3, x_5)\}$,

$A_2 = \{(0, x_6), (1, x_7), (1, x_8), (3, x_9), (3, x_{10})\}$ and

$S = \{\omega^{2^e 10i + j} \mid 0 \leqslant i < t/2^e; 0 \leqslant j < 2^e\}$,

we have that $\mathcal{F} = (sA_i \mid s \in S, i = 1, 2)$ is a 1-rotational (4p,5,1) difference family admitting $\omega^{2^e 10}$ as a multiplier of order $t/2^e$.

If, in addition, X is a system of representatives for the cosets of 2^e10th powers in the group of 2^eth powers, then the BIBD generated by $\mathcal{F}$ is resolvable.

In the remainder of this section p will be equivalent to 1 (mod 10) and ε will denote a primitive 5th root of unity (mod p). Also, with each quintuple $X = (x_1, ..., x_5) \in \mathbb{Z}_p^{(5)}$ we associate the following sextuples:

$X_0 = \pm(x_2-x_1, \varepsilon-1, \varepsilon^2-1)$,

$X_1 = (x_3-x_1, x_3-x_2, x_4-x_3, x_5-x_4, x_1-x_5, x_2-x_5)$,

$X_2 = \pm(x_4-x_1, x_4-x_2, x_5-x_3)$,

$X_3 = -X_1$,

$X^+ = (1, x_1, x_2, x_3, x_4, x_5)$.

Theorem 5.3. There exists a 1-rotational (4p+1,5,3)-BIBD over $\mathbb{Z}_{4p}$ for any prime $p \equiv 11 \pmod{20}$.

Proof. Let ε be a primitive 5th root of unity (mod p) and let $X \in \mathbb{Z}_p^{(5)}$ such that the list X_1 has exactly three squares (mod p). Note that such a quintuple X surely exists. For instance, one can take X = (0, 3,

1, 2, 4) if 2 is a square (mod p) or X = (0, 1, 2, 3, -1) if 2 is a non-square. Consider the 5-subsets A, B of $\mathbb{Z}_4 \oplus \mathbb{Z}_p$ defined as follows:

$$A = \{(0, 1), (0, \varepsilon), (0, \varepsilon^2), (0, \varepsilon^3), (0, \varepsilon^4)\}$$

$$B = \{(0, x_1), (0, x_2), (1, x_3), (2, x_4), (3, x_5)\}$$

Set $A_0 = A$ and $A_i = \varepsilon^{i-1}B$ for $1 \leqslant i \leqslant 5$. We have:

$$\bigcup_{0\leqslant i\leqslant 5} \Delta A_i = \{0\}\times(<\varepsilon>X_0) \cup \{1\}\times(<\varepsilon>X_1) \cup \{2\}\times(\pm<\varepsilon>X_2) \cup \{1\}\times(<\varepsilon>X_3)$$

Let $S = \{\omega^{2i} \mid 0 \leqslant i < \frac{p-1}{10}\}$. Note that $<\varepsilon>S$ is the set of non-zero squares (mod p). Also, note that each of the X_i's has exactly three squares and three non-squares; in X_1 by choice of X, in X_0 and X_2 because -1 is a non-square (mod p). It follows that $<\varepsilon>X_iS$ covers $\mathbb{Z}_p^*$ exactly 3 times (for i = 0, 1, 2, 3) so that

$$\mathcal{F} = (sA_i \mid s \in S, 0 \leqslant i \leqslant 5)$$

is a 1-rotational (4p,5,3) difference family. The assertion follows. □

Example 5.4. Let us apply the above theorem in the case where p = 11. Take $\varepsilon = 3$ as primitive 5th root of unity (mod 11) and check that $X \in \mathbb{Z}_{11}^{(5)} = (0, 1, 2, 3, 4)$ is such that X_1 has three squares and three non-squares (mod 11). Then we have that

$A_0 = \{(0, 1), (0, 3), (0, 9), (0, 5), (0, 4)\}$
$A_1 = \{(0, 0), (0, 1), (1, 2), (2, 3), (3, 4)\}$
$A_2 = \{(0, 0), (0, 3), (1, 6), (2, 9), (3, 1)\}$
$A_3 = \{(0, 0), (0, 9), (1, 7), (2, 5), (3, 3)\}$
$A_4 = \{(0, 0), (0, 5), (1, 10), (2, 4), (3, 9)\}$
$A_5 = \{(0, 0), (0, 4), (1, 8), (2, 1), (3, 5)\}$

are base blocks of a 1-rotational (44,5,3)-DF over $\mathbb{Z}_4 \oplus \mathbb{Z}_{11}$. Using the ring isomorphism ψ: (a, b) $\in \mathbb{Z}_4 \oplus \mathbb{Z}_{11} \rightarrow$ 12b-11a $\in \mathbb{Z}_{44}$, we may identify the above family as a 1-rotational (44,5,3)-DF over $\mathbb{Z}_{44}$ with base blocks:

{12, 36, 20, 16, 4} {0, 12, 13, 14, 15} {0, 36, 17, 42, 23}

{0, 20, 29, 38, 3} {0, 16, 21, 26, 31} {0, 4, 41, 34, 27}

In the following theorems saying that p is a *good* prime, we mean that $(11+5\sqrt{5})/2$ is not a cube (mod p)

Theorem 5.5. Let $p \equiv 31 \pmod{60}$ be a good prime. There exists a 1-rotational (4p+1,5,1)-BIBD over $\mathbb{Z}_{4p}$ provided that there exists $Y \in \mathbb{Z}_p^{(5)}$ such that Y_1 and Y_2 are systems of representatives for the cosets of the 6th powers (mod p).

Proof. Let Y be a quintuple satisfying the assumption. Reasoning like in the proof of Lemma 3.5 we deduce that there is a suitable $c \in \mathbb{Z}_p^*$ for which the *normalized* quintuple X = cY is such that all the X_i's are systems of representatives for the cosets of 6th powers. Starting from X, consider the sets $A_0, A_1, \ldots, A_5$ defined like in the proof of Theorem 5.3 and let $S = \{\omega^{6i} \mid 0 \leqslant i < \frac{p-1}{30}\}$. It is easily seen that $<\varepsilon>S$ is the set of 6th powers (mod p) so that $X_iS = \mathbb{Z}_p^*$ for i = 0, 1, 2, 3. It follows that the family

$$\mathcal{F} = (sA_i \mid s \in S, 0 \leqslant i \leqslant 5)$$

is a 1-rotational (4p,5,1) difference family. The assertion follows. □

Theorem 5.6. Let $p \equiv 31 \pmod{60}$ be a good prime. There exists a 1-rotational (4p+1,5,1)-RBIBD over $\mathbb{Z}_{4p}$ provided that there exists

$X \in \mathbb{Z}_p^{(5)}$ such that X_0, X_1, X_2 and X^+ are systems of representatives for the cosets of 6th powers (mod p).

Proof. Let $\mathcal{F}$ be the 1-rotational (4p,5,1) difference family obtainable as in the proof of Theorem 5.5 using the quintuple X. We have: $\bigcup_{A \in \mathcal{F}} \pi(A) = SX^+ <\varepsilon> = \mathbb{Z}_q^*$ because $S<\varepsilon>$ is the group of 6th powers and X^+ is by assumption a system of representatives for the cosets of this group. Then, applying Lemma 1.3 the assertion follows. □

Applying the previous theorem we find a 1-rotational (4p+1,5,1)-RBIBD over $\mathbb{Z}_{4p}$ for each good prime p = 60t+31 < 1.000. It suffices to take X as indicated in the following table.

p = 31 X = (3, 29, 20, 28, 11)

p = 211 X = (4, 32, 2, 124, 126)

p = 271 X = (6, 188, 36, 173, 62)

p = 571 X = (3, 243, 9, 551, 236)

p = 631 X = (3, 9, 27, 366, 54)

p = 691 X = (3, 81, 9, 591, 237)

p = 751 X = (3, 81, 9, 157, 136)

p = 991 X = (6, 305, 710, 591, 240).

6. Some new (125,5,1) and (156,6,1) BIBD's

The only previously known (125,5,1) and (156,6,1) BIBD's were those obtainable from the 3-dimensional affine and projective geometries over $\mathbb{Z}_5$ [cf. 10].

Using the constructions seen in the previous sections it is possible to get new (125,5,1)-BIBDs. Also, having a new (125,5,1)-RBIBD, we

immediately get a new (156,6,1)-BIBD using the same argument that one uses in classical geometry for constructing PG(3,5) starting from AG(3,5).

Theorem 6.1. No (125,5,1)-BIBD obtainable using Theorems 2.3, 3.6, 3.8, 4.1, 5.5 and 5.6 is isomorphic to the BIBD of points and lines of AG(3,5).

Proof. All the (125,5,1)-BIBD's obtainable using Theorems 2.3, 3.6, 3.8, 4.1 admit $\mathbb{Z}_2^2 \oplus \mathbb{Z}_{31}$ as an automorphism group fixing one point, while the stabilizer of a point of AG(3,5), namely GL(3,5), does not admit $\mathbb{Z}_2^2 \oplus \mathbb{Z}_{31}$ as a subgroup.

Now, let Σ be a (125,5,1)-BIBD obtainable using Theorems 5.5 or 5.6. The stabilizer of ∞ in the full automorphism group of Σ has the following property. It admits a subgroup H of order 31 and an element $\hat{\epsilon}$ of order 5 normalizing H. But the same property is not satisfied by GL(3,5). □

Let us see, concretely, some of these new (125,5,1)-BIBD's.

a) Applying Theorem 2.3 using the 10tuple X = (1, 2, 4, 11, 16, 12, 9, 13, 6, 23) we get a 1-rotational (125,5,1)-RBIBD whose blocks can be obtained developing (mod $\mathbb{Z}_2^2 \oplus \mathbb{Z}_{31}$) the following blocks:

$A_0 = \{(0_0, 1), (0_0, 2), (0_0, 4), (1_0, 11), (0_1, 16)\}$

$A_1 = \{(0_0, 5), (0_0, 10), (0_0, 20), (1_0, 24), (0_1, 18)\}$

$A_2 = \{(0_0, 25), (0_0, 19), (0_1, 7), (1_0, 27), (0_1, 28)\}$

$A_3 = \{(0_0, 12), (1_0, 9), (1_0, 13), (0_1, 6), (0_1, 23)\}$

$A_4 = \{(0_0, 29), (1_0, 14), (1_0, 3), (0_1, 30), (0_1, 22)\}$

$A_5 = \{(0_0, 21), (1_0, 8), (1_0, 15), (0_1, 26), (0_1, 17)\}$

$A_6 = \{(0_0, 0), (0_1, 0), (1_0, 0), (1_1, 0), \infty\}$

b) Applying Theorem 3.8 using $\varepsilon = 2$ as a primitive 5th root of unity (mod 31) and using the quintuple X = (3, 29, 20, 25, 26), we get a 1-rotational (125,5,1)-RBIBD whose blocks can be obtained developing (mod $\mathbb{Z}_2^2 \oplus \mathbb{Z}_{31}$) the following blocks:

$A_0 = \{(0_0, 1), (0_0, 2), (0_0, 4), (0_0, 8), (0_0, 16)\}$
$A_1 = \{(0_0, 3), (0_0, 29), (0_1, 20), (1_0, 25), (1_1, 26)\}$
$A_2 = \{(0_0, 6), (0_0, 27), (0_1, 9), (1_0, 19), (1_1, 21)\}$
$A_3 = \{(0_0, 12), (0_0, 23), (0_1, 18), (1_0, 7), (1_1, 11)\}$
$A_4 = \{(0_0, 24), (0_0, 15), (0_1, 5), (1_0, 14), (1_1, 22)\}$
$A_5 = \{(0_0, 17), (0_0, 30), (0_1, 10), (1_0, 28), (1_1, 13)\}$
$B = \{(0_0, 0), (0_1, 0), (1_0, 0), (1_1, 0), \infty\}$

c) Applying Theorem 5.6 using $\varepsilon = 2$ as a primitive 5th root of unity (mod 31) and using the quintuple X = (3, 29, 20, 28, 11) we get a 1-rotational (125,5,1)-RBIBD whose blocks can be obtained developing (mod $\mathbb{Z}_4 \oplus \mathbb{Z}_{31}$) the following blocks:

$A_0 = \{(0, 1), (0, 2), (0, 4), (0, 8), (0, 16)\}$
$A_1 = \{(0, 3), (0, 29), (1, 20), (2, 28), (3, 11)\}$
$A_2 = \{(0, 6), (0, 27), (1, 9), (2, 25), (3, 22)\}$
$A_3 = \{(0, 12), (0, 23), (1, 18), (2, 19), (3, 13)\}$
$A_4 = \{(0, 24), (0, 15), (1, 5), (2, 7), (3, 26)\}$
$A_5 = \{(0, 17), (0, 30), (1, 10), (2, 14), (3, 21)\}$
$A_6 = \{(0, 0), (1, 0), (2, 0), (3, 0), \infty\}$

Using the ring isomorphism ψ: (a, b) $\in \mathbb{Z}_4 \oplus \mathbb{Z}_{31} \rightarrow$ 32b-31a $\in \mathbb{Z}_{124}$, we may identify the point-set of the above design with $\mathbb{Z}_{124} \cup \{\infty\}$ and its blocks with all the translates (under $\mathbb{Z}_{124}$) of the following blocks:

{32, 64, 4, 8, 16} {96, 60, 113, 90, 11}
{68, 120, 40, 56, 84} {12, 116, 80, 112, 44}
{24, 108, 36, 100, 88} {48, 92, 72, 76, 52}
{0, 31, 62, 93, ∞ }

Each of the above RBIBD's gives rise to a new (156,6,1)-BIBD admitting $G \oplus \mathbb{Z}_{31}$ as an automorphism group ($G = \mathbb{Z}_2^2$ in cases a) and b), $G = \mathbb{Z}_4$ in case c)). It suffices to proceed as follows. Take a 31-set $\{\infty_0, \infty_1, ..., \infty_{30}\}$. Using the cyclic difference set D = {1, 5, 11, 24, 25, 27} in $\mathbb{Z}_{31}$, we get a new (156,6,1)-BIBD with point-set $G \oplus \mathbb{Z}_{31} \cup \{\infty, \infty_0, \infty_1, ..., \infty_{30}\}$ and blocks obtainable from the 8 blocks:

$A_i \cup \{\infty_0\}$ $0 \leq i \leq 6$, $B = \{\infty_1, \infty_5, \infty_{11}, \infty_{24}, \infty_{25}, \infty_{27}\}$

developing them (mod $G \oplus \mathbb{Z}_{31}$) under the rules that

$\infty + (g, h) = \infty$; $\infty_i + (g, h) = \infty_{i+h \pmod{31}}$ for any $(g, h) \in G \oplus \mathbb{Z}_{31}$.

Of course, it would be interesting to establish how many pairwise non-isomorphic (125,5,1) and (156,6,1)-BIBD's are obtainable using the constructions given in this paper.

In a future joint-work with F. Zuanni, the author will give constructions for 1-rotational ((k-1)q+1,k,1)-BIBD's (or RBIBD's) where q is a prime power equivalent to 1 mod k(k+1). This constructions generalize the constructions for Steiner 2-designs given in Sections 3 and 4.

Acknowledgement

The author wishes to thank A. Pasini for some very helpful comments and suggestions.

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, pp. 270-287.

[2] 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.

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

[4] M. Buratti, *Improving two theorems of Bose on difference families*, J. Combin. Designs 3 (1995), 169-175.

[5] M. Buratti, *Recursive constructions for difference matrices and relative difference families*, to appear in J. Combin. Designs.

[6] M. Buratti, *Small quasimultiple of affine and projective planes; some improved bounds*, preprint.

[7] M. Buratti, *Old and new designs via strong difference families*, preprint.

[8] M. Greig, *Some group divisible design constructions*, to appear in J. of Comb. Mathematics and Comb. Computing.

[9] Y.S. Liaw, *1-rotational designs with block size 4*, Bull. Ist. Comb. Appl. 13 (1995), 91-98.

[10] R. Mathon and A. Rosa, *2-(v,k,λ) designs of small order*, in CRC Handbook of Combinatorial designs (C.J. Colbourn and J. H. Dinitz eds.), CRC Press, Boca Raton FL, 1996 pp. 3-41.

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

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

(Received 29/4/97)