SOME REGULAR STEINER 2-DESIGNS WITH BLOCK SIZE 4

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

Abstract.
We give a constructive and very simple proof of a theorem by Check and Colbourn [7] stating the existence of a cyclic $(4p,4,1)$-BIBD (i.e. regular over Z_{4p}) for any prime $p \equiv 13 \pmod{24}$. We extend the theorem to primes $p \equiv 1 \pmod{24}$ although in this case the construction is not explicit. Anyway, for all these primes p, we explicitly construct a regular $(4p,4,1)$-BIBD over $Z_2^2 \oplus Z_p$.

1. Introduction

A $(v,k,1)$-BIBD (*Steiner 2-design of order v and block-size k*) is *regular* over a group G, if admits G as an automorphism group acting sharply transitively on the point-set. When $G = Z_v$ the BIBD is said to be *cyclic*. The problem of establishing the spectrum $C(k)$ of all the v's for which a cyclic $(v,k,1)$-BIBD exists appears to be very difficult. It is completely solved only for k = 3 (cf. [3, VII. 4.6]) while very little is known for $k > 3$. Maybe, the analogous problem of establishing the spectrum $R(k)$ of all the v's for which a regular $(v,k,1)$-BIBD exists is slightly more easy.

In a recent paper [7] Check and Colbourn, correcting in part a previous construction by Mathon [9], proved that $4p \in C(4)$ for any prime $p \equiv 13 \pmod{24}$. Here, this result will be proved in a much more easy and constructive way. Also, combining a recent result by Chen and Zhu [8] with another by the author [4], we extend the theorem to primes $p \equiv 1 \pmod{24}$ although in this case the construction is not explicit. Anyway, we succeed in explicitly construct a regular $(4p,4,1)$-BIBD over $Z_2^2 \oplus Z_p$ for any prime $p \equiv 1 \pmod{24}$.

For realizing our designs we will use the following standard construction.

Let G be an additive group of order 4 (hence $G = Z_4$ or $G = Z_2^2$). Let D be a family of 4-subsets of $G \oplus Z_p$ whose list of differences covers $(G \oplus Z_p) - (G \oplus \{0\})$ exactly once. Then D, which is a *$(4p,4,1)$ difference family (over $G \oplus Z_p$ and relative to $G \oplus \{0\}$)*, generates a regular $(4p,4,1)$-

BIBD over $G \oplus Z_p$. This BIBD has $G \oplus Z_p$ as point-set and block-set consisting in all the translates of the components of D plus all the translates of $G \oplus \{0\}$. Note that this BIBD is cyclic when $G = Z_4$ since $Z_4 \oplus Z_p$ is isomorphic to Z_{4p}.

For a more general definition of difference family one can see [1, 6].

2. Two explicit constructions of regular (4*p*,4,1)-BIBD's with *p* a prime.

In the constructions that follow we set $t = \frac{p-1}{12}$ and we denote by ω and ε a primitive element and a primitive 3rd root of unity mod p, respectively.

Theorem 2.1. There exists a cyclic $(4p,4,1)$-BIBD for any prime $p \equiv 13 \pmod{24}$.

Proof. Let define the cyclotomic classes C_0, C_1, C_2, C_3 as the cosets of the 4th powers mod p:

$$C_i = \{\omega^{4h+i} \mid 0 \le h < 3t\},\ i = 0,1,2,3.$$

Given $x \in Z_p - \{0\}$, let $C_{i(x)}$ be the cyclotomic class containing x. By elementary facts of number theory (see e.g. [2]) we have that:

$$\mathrm{i}(-1) = 2 \qquad \mathrm{i}(2) = 1 \text{ or } 3 \qquad \mathrm{i}(3) = 0 \text{ or } 2 \tag{1}$$

Also, it is easy to see that:

$$\varepsilon\text{-}1 \text{ is a square if and only if } \mathrm{i}(3) = 2 \tag{2}$$

In the case of i(3) = 0, combining a well-known construction by R.C. Bose (see [3, Theorem VII.5.2]) with [5, Theorem 2.1] we may explicitely construct a cyclic $(4p,4,1)$-BIBD via the following $(4p,4,1)$ difference family over $Z_4 \oplus Z_p$:

$$\boldsymbol{D} = (\{(0,0),(0,\omega^{2i}),(0,\omega^{2i+4t}),(0,\omega^{2i+8t})\} \mid 0 \le i < t) \cup$$

$$\cup (\{(0,\omega^{i}),(1,\omega^{i+3t})),(2,-\omega^{i}),(3,-\omega^{i+3t})\} \mid 0 \le i < 3t)$$

In the following we assume that i(3) = 2.
Consider the pair $(a,b) \in Z_p \times Z_p$ defined by:

$$(a,b) = \begin{cases} (-2,7) & \text{if } i(7) = 0 \\ (1/2, 9/25) & \text{if } i(7) = 1 \text{ or } 3 \\ (2,-7) & \text{if } i(7) = 2 \end{cases}$$

and consider the subsets D_1, D_2, D_3, D_4 of $Z_4 \oplus Z_p$ defined by:

$D_i = \{(0,0),(0,\varepsilon^i),(1,a\varepsilon^i),(3,b\varepsilon^i)\}$ for i = 1, 2, 3;

$D_4 = \{(0,0),(2,2),(2,2\varepsilon),(2,2\varepsilon^2)\}$.

The list of differences from the sets D_i's is given by

$$[\{0\} \times (<\varepsilon> X_0)] \cup [\{1\} \times (<\varepsilon> X_1)] \cup [\{2\} \times (<\varepsilon> X_2)] \cup [\{3\} \times (<\varepsilon> X_3)]$$

where the X_i's are the following lists:

$$X_0 = (\pm 1, \pm 2(\varepsilon - 1)) \qquad X_1 = (a, a-1, -b, -b+1)$$
$$X_2 = (\pm 2, \pm(a-b)) \qquad X_3 = -X_1$$

In view of (1) and (2) it is very easy to check that each of the previous lists has elements lying in pairwise distinct cyclotomic classes. In other words, each X_i is a system of representatives for the cosets of the 4th powers mod p. Then, setting $S = \{\omega^{4i} \mid 0 \le i < t\}$ we have that $<\varepsilon> X_i S = Z_p - \{0\}$ (for i = 0, 1, 2, 3) because $<\varepsilon> S$ is easily seen to be the group of 4th powers mod p.

It follows that the differences from the family $D = (sD_i \mid s \in S; 1 \le i \le 4)$ cover exactly once $(Z_4 \oplus Z_p) - (Z_4 \oplus \{0\})$, i.e. D is a $(4p,4,1)$ difference family over $Z_4 \oplus Z_p$. The assertion follows. □

Theorem 2.2. There exists a regular $(4p,4,1)$-BIBD over $Z_2^2 \oplus Z_p$ for any prime $p \equiv 1 \pmod{24}$.

Proof. Here, saying that an integer x is a quadratic residue, we mean that x is a square mod p. From the assumption we have that -1 and 2 are quadratic residues. Let q be the first prime which is not a quadratic residue. Then each positive integer smaller than q is a quadratic residue. Consider the ordered triple $(a,b,c) \in Z_p \oplus Z_p \oplus Z_p$ defined by:

$$(a,b,c) = \begin{cases} (q+1, q, q) & \text{if } \varepsilon - 1 \text{ is a quadratic residue} \\ (q, -q, 1) & \text{otherwise} \end{cases}$$

Consider the following subsets D_1, D_2, D_3, D_4 of $Z_2^2 \oplus Z_p$:

$$D_i = \{(0_0, 0), (0_0, \varepsilon^i), (1_0, a\varepsilon^i), (0_1, b\varepsilon^i)\} \text{ for i = 1, 2, 3;}$$
$$D_4 = \{(0_0, 0), (1_1, c), (1_1, c\varepsilon), (1_1, c\varepsilon^2)\}.$$

(It is understood that we write any element $(x,y) \in Z_2^2$ as x_y).
The list of differences from the sets D_i's is given by

$$[\{0_0\} \times (\pm < \varepsilon > X_0)] \cup [\{1_0\} \times (\pm < \varepsilon > X_1)] \cup$$
$$\cup [\{0_1\} \times (\pm < \varepsilon > X_2)] \cup [\{1_1\} \times (\pm < \varepsilon > X_3)]$$

where:

$$X_0 = (1, c(\varepsilon - 1)) \qquad X_1 = (a, a-1) \qquad X_2 = (b, b-1) \qquad X_3 = (c, a-b).$$

In view of the choice of the triple (a,b,c), each X_i has exactly one quadratic residue and exactly one non-quadratic residue. In fact, q-1 and $q+1$ $(= 2\frac{q+1}{2})$ are quadratic residues by assumption on q. Then, setting $S = \{\omega^{2i} \mid 0 \le i < t\}$ we have that $\pm < \varepsilon > X_i S = Z_p - \{0\}$ (for i = 0, 1, 2, 3) because $\pm < \varepsilon > S$ is easily seen to be the set of quadratic residues. It follows that the differences from the family $D = (sD_i | s \in S; 1 \le i \le 4)$ cover exactly once $(Z_2^2 \oplus Z_p) - (Z_2^2 \oplus \{0\})$ i.e. D is a $(4p,4,1)$ difference family over $Z_2^2 \oplus Z_p$. The assertion follows. □

From the above theorems we immediately have:
Corollary 2.3. $p \in R(4)$ for any prime $p \equiv 1 \pmod{12}$.

3. Existence of cyclic $(4p,4,1)$-BIBD's for primes $p \equiv 1 \pmod{12}$.

Now we extend Theorem 2.1 to primes $p \equiv 1 \pmod{24}$ via the following results.

Theorem 3.1. $p \in C(4)$ for any prime $p \equiv 1 \pmod{12}$.
Theorem 3.2. If p is a prime and $p \in C(4)$, then $4p \in C(4)$.

The first of the above theorems is due to Chen and Zhu [8], while the latter is a consequence of a result by the author [5,Corollary 3.3]. Combining them we get:

Theorem 3.3. $4p \in C(4)$ for any prime $p \equiv 1 \pmod{12}$.

In spite of Theorem 3.3 an explicit construction of a cyclic $(4p,4,1)$-BIBD for all primes $p \equiv 1 \pmod{24}$ is still missing. In fact, Theorem 3.1 does not give a concrete way for constructing a cyclic $(4p,4,1)$-BIBD for any prime $p \equiv 1 \pmod{24}$. Anyway, using previous constructions by the author ([4, Theorem 4.1] and [5, Theorem 2.1]) we can explicitely get such a cyclic BIBD for all p's such that -3 is not a $2^e th$ power (mod p), 2^e being the largest power of 2 dividing $p-1$.

Question. What about regular $(4p,4,1)$-BIBD's for primes $p \equiv 7 \pmod{12}$?

Acknowledgement. The author wishes to thank Phil Leonard for some helpful discussions on the subject.

References

[1] R.J.R. Abel, *Difference families*, in: The CRC Handboock of Combinatorial Designs, (C.J. Colbourn and J.H. Dinitz, eds.), CRC Press, Boca Raton FL (1996), 270-287.
[2] W. Adams, L.J. Goldstein, *Introduction to the theory of numbers*, Prentice Hall, 1976.
[3] T. Beth, D. Jungnickel and H. Lenz, *Design Theory*, Cambridge University Press, London, 1986.
[4] M. Buratti, *Improving two theorems of Bose on difference families*, J. Combin. Designs 3 (1995), 15-24.
[5] M. Buratti, *From a $(G,k,1)$ difference family to a $(C_k \oplus G,k,1)$ difference family*, Designs, Codes and Cryptography 11 (1997), 5-9.
[6] M. Buratti, *Recursive constructions for difference matrices and relative difference families*, J. Combin. Designs, to appear.
[7] P.L. Check and C.J. Colbourn, *Concerning difference families with block size four*, Discrete Math. 133 (1994), 285-289.
[8] K. Chen and L. Zhu, *Existence of $(q,k,1)$ difference families with q a prime power and $k = 4, 5$*, J. Combin. Designs, to appear.
[9] R. Mathon, *Constructions for cyclic Steiner 2-designs*, Ann. Discrete Math. 34 (1987), 353-362.