DESIGNS FROM CYCLOTOMY

ELIZABETH J. MORGAN, ANNE PENFOLD STREET AND JENNIFER SEBBERRY WALLIS

In this note we use the theory of cyclotomy to help us construct initial blocks from which we can develop balanced and partially balanced incomplete block designs. Our main construction method, using unions of cyclotomic classes, gives us upper bounds on m, the number of associate classes of the design, but not exact values for m; we discuss the possible values of m and the circumstances under which m = 1, so that the design is in fact balanced.

1. INTRODUCTION

In this note we use the theory of cyclotomy to help us construct initial blocks from which we can develop balanced and partially balanced incomplete block designs (BIBD and PBIBD respectively). These initial blocks are usually either difference sets or supplementary difference sets (sds) in the additive group of a finite field.

The theory of cyclotomy has been much used in the construction of difference sets and block designs. Consider the field $GF[p^n]$, where p is prime and n is a positive integer, such that

$$p^n = ef + 1, \qquad e \geq 2, \qquad f \geq 2.$$

Let C_0 denote the set of e^{th} power residues, so that

$$C_0 = \{x^{ae} \mid a = 0, 1, \ldots, f-1\}$$

where x is a primitive root of the field. The original results of Lehmer [4] showed that if C_0 or $C_0 \cup \{0\}$ were a difference set in $GF[p^n]$, then e must be even and f odd. This result has motivated a great deal of work in the evaluation of cyclotomic numbers for e even; relatively little has been done for e odd. However some recent constructions ([10], [11, Lemmas 10 - 15]) have led us to an interest in this case also.

As far as possible, we follows the terminology and notation of Raghavarao [6] with respect to designs, of Storer [9] with respect to cyclotomy and difference sets and of J.S. Wallis [13, part 4] with respect to supplementary difference sets. However in Section 2 some specialised notation is defined and a few computational results are given.

In Section 3, using two somewhat different methods, we construct several series of PBIBDs, by taking unions of cyclotomic classes as initial blocks. These construc-

tion methods give us upper bounds on m, the number of associate classes of the design, but not exact values for m. In Section 4, we discuss these values of m and in particular we consider under what circumstances m = 1, so that the design is in fact a BIBD. Finally in Section 5, we construct a series of Latin Square PBIBD(2)s, starting from one cyclotomic class in GF[p^2].

2. NOTATION AND BASIC COMPUTATIONAL RESULTS

Let $p^n = \alpha\beta\gamma+1$, where p is an odd prime and n, α, β, γ are positive integers with $\alpha,\beta,\gamma \geq 2$. Let $e_1 = \alpha\beta$, $f_1 = \gamma$, $e_2 = \alpha$, $f_2 = \beta\gamma$. Let x be a primitive root of the field GF[p^n] and let C_i, D_i denote the i^{th} cyclotomic class of the field relative to e_2, e_1 respectively, so that

$$C_i = \{x^{a\alpha+i} \mid a = 0,1,\ldots,\beta\gamma-1\}, \qquad i = 0,1,\ldots,\alpha-1$$

and

$$D_i = \{x^{a\alpha\beta+i} \mid a = 0,1,\ldots,\gamma-1\}, \qquad i = 0,1,\ldots,\alpha\beta-1.$$

Note that

$$C_i = \bigcup_{j=0}^{\beta-1} D_{j\alpha+i} \qquad \text{for each } i.$$

Let $i_0 = 0, i_1, \ldots, i_{\alpha-1}$ be a complete set of residues modulo α, where $0 \leq i_h \leq e_1-1$, for $h = 0,1,\ldots,\alpha-1$. Define

$$B_j = \bigcup_{h=0}^{\alpha-1} D_{i_h} + j\alpha, \qquad j = 0,1,\ldots,\beta-1$$

and

$$A_j = \{0\} \cup B_j, \qquad j = 0,1,\ldots,\beta-1.$$

Next we choose some integer t such that $0 < t \leq \alpha\beta$, and t distinct integers $a_1, a_2, \ldots, a_t$ such that $0 \leq a_1 < a_2 < \ldots < a_t \leq \alpha\beta-1$. Define

$$E_i = \bigcup_{h=1}^{t} D_{a_h+i}, \qquad i = 0,1,\ldots,\alpha\beta-1$$

and

$$F_i = \{0\} \cup E_i, \qquad i = 0,1,\ldots,\alpha\beta-1.$$

In addition, we use the following notation as in [6]:

A & B denotes the collection of all the elements of the sets A and B with multiplicities preserved;

A + B denotes the collection of non-zero sums a+b, with $a \in A$, $b \in B$, again with multi-

plicities preserved, and similarly A - B denotes the collection of non-zero differences; nA denotes the collection of n copies of A, so that

$$nA = (n-1)A \;\&\; A;$$

$n \times A$ denotes the set $\{na \mid a \in A\}$.

We let the cyclotomic number (h,k) denote the number of ordered pairs s, t such that

$$x^{es+h} + 1 = x^{et+k},$$

where $0 \leq s, t \leq f-1$, and x is a primitive root of $GF[p^n]$, with $p^n = ef+1$ as usual [9]. If there is any doubt as to which factorisation of p^n-1 we are using, we specify it by writing $(h,k)_e$.

Lemma 1. *(i) If $\beta\gamma$ is even, then $C_i = -C_i$ (or, to be consistent, $C_i = (-1)\times C_i$), so that*

$$C_i - C_i = C_i + C_i = \mathop{\&}_{j=0}^{\alpha-1} (0, j-1)_\alpha C_j,$$

and

$$C_i - C_j = C_i + C_j = \mathop{\&}_{k=0}^{\alpha-1} (j-i, k-i)_\alpha C_k$$

where

$$0 \leq i, j, k \leq \alpha-1.$$

(ii) If $\beta\gamma$ is odd, then $C_i = -C_{i+(\alpha/2)}$, so that

$$C_i - C_i = C_{(\alpha/2)+i} - C_{(\alpha/2)+i} = C_{(\alpha/2)+i} + C_i$$

and

$$C_i - C_j = \mathop{\&}_{k=0}^{\alpha-1} (j-i+(\alpha/2), k)_\alpha C_{i+k},$$

whereas

$$C_j - C_i = \mathop{\&}_{k=0}^{\alpha-1} (j-i+(\alpha/2), k)_\alpha C_{i+k+(\alpha/2)},$$

$$0 \leq i, j, k \leq \alpha-1.$$

(iii) If γ is even, then $D_i = -D_i$, so that

$$D_i - D_i = D_i + D_i = \mathop{\&}_{j=0}^{\alpha\beta-1} (0, j-i)_{\alpha\beta} D_j$$

and

$$D_i - D_j = D_i + D_j = \mathop{\&}_{k=0}^{\alpha\beta-1} (j-i,k-i)_{\alpha\beta} D_k,$$

where

$$0 \leq i,\ j,\ k \leq \alpha\beta-1.$$

(iv) If β *is even,* γ *odd, then*

$$D_i = -D_{i+(\alpha\beta/2)},$$

so that

$$D_i - D_i = D_{(\alpha\beta/2)+i} - D_{(\alpha\beta/2)+i} = D_{(\alpha\beta/2)+i} + D_i$$

and

$$D_i - D_j = \mathop{\&}_{k=0}^{\alpha\beta-1} (j-i+(\alpha\beta/2),k)_{\alpha\beta} D_{k+i},$$

whereas

$$D_j - D_i = \mathop{\&}_{k=0}^{\alpha\beta-1} (j-i+(\alpha\beta/2),k)_{\alpha\beta} D_{k+i+(\alpha\beta/2)},$$

$$0 \leq i,\ j,\ k \leq \alpha\beta-1.$$

Lemma 2. *(i) If* γ *is even, then*

$$B_j = -B_j$$

and

$$B_j - B_j = B_j + B_j = \mathop{\&}_{i=0}^{\alpha\beta-1} k_i D_{i+j\alpha}, \qquad j = 0,1,\ldots,\beta-1,$$

where

$$k_i = \sum_{h=0}^{\alpha-1} (0,i-i_h)_{\alpha\beta} + 2 \sum_{0\leq h<\ell\leq\alpha-1} (i_h-i_\ell,i-i_h)_{\alpha\beta}.$$

(ii) If γ *is even, then*

$$A_j = -A_j$$

and

$$A_j - A_j = A_j + A_j = 2B_j \mathbin{\&} (B_j - B_j) = \mathop{\&}_{i=0}^{\alpha\beta-1} \ell_i D_{i+j\alpha},$$

$$j = 0,1,\ldots,\beta-1,$$

where

$$\ell_i = k_i, \qquad i \neq i_0, i_1, \ldots, i_{\alpha-1},$$

and

$$\ell_i = k_i + 2, \qquad i = i_m, \qquad m = 0, 1, \ldots, \alpha-1.$$

(iii) If β *is even,* γ *odd, then*

$$B_j - B_j = \mathop{\&}_{i=0}^{\alpha\beta-1} K_i D_{i+j\alpha}, \qquad j = 0, 1, \ldots, \beta-1,$$

where

$$K_i = \sum_{h=0}^{\alpha-1} (i-i_h, 0)_{\alpha\beta} + \sum_{0 \le h < \ell \le \alpha-1} (i-i_\ell, i_h-i_\ell)_{\alpha\beta} + \sum_{0 \le h < \ell \le \alpha-1} (i-i_h, i_\ell-i_h)_{\alpha\beta}.$$

(iv) If β *is even,* γ *odd, then*

$$A_j - A_j = B_j \,\&\, B_{j+(\alpha\beta/2)} \,\&\, (B_j - B_j) = \mathop{\&}_{i=0}^{\alpha\beta-1} L_i D_{i+j\alpha},$$

$$j = 0, 1, \ldots, \beta-1,$$

where

$$L_i = K_i, \qquad i \neq i_h, \qquad i \neq i_h + (\alpha\beta/2), \qquad h = 0, 1, \ldots, \alpha-1,$$

and

$$L_i = K_i + 1, \qquad i = i_h, \qquad i = i_h + (\alpha\beta/2), \qquad h = 0, 1, \ldots, \alpha-1.$$

Lemma 3. *Let* $\beta\gamma$ *be even. Then*

(i) $$E_i - E_i = \mathop{\&}_{j=0}^{\alpha\beta-1} d_j D_{j+i},$$

where

$$\sum_{j=0}^{\alpha\beta-1} d_j = t(t\gamma-1).$$

(ii) $$F_i - F_i = \mathop{\&}_{j=0}^{\alpha\beta-1} \delta_j D_{j+i},$$

where

$$\mathop{\&}_{j=0}^{\alpha\beta-1} \delta_j = t(t\gamma+1).$$

We omit the proof of these Lemmas: Lemma 1 follows immediately from the definitions and basic properties of cyclotomic numbers as given in [9, pp.24-26]; Lemma 2(i) is proved in [10, §3(iv)] and is typical of the tedious but straightforward arithmetic required for the remaining proofs.

3. CONSTRUCTION OF SOME PBIBDs

We now use our sets A_j, B_j, E_j, F_j to construct PBIBDs in the following ways, based on Sprott's generalisation [8] of a theorem of Bose and Nair [1].

Theorem 1. *The β sets A_j, $j = 0,1,\ldots,\beta-1$, or the β sets B_j, $j = 0,1,\ldots,\beta-1$, may be used as the initial blocks of a* PBIBD(m), *where $v = p^n$, $b = \beta p^n$, $m \leq \alpha$, and each associate class consists of a cyclotomic class C_i or a union of such classes. The parameters of the design are given in the following table, which includes n_i, λ_i and p_{ij}^k when $m = \alpha$ so that each cyclotomic class is an associate class.*

Initial blocks	k	r	Parity conditions	Parameters when $m = \alpha$		
				n_i	λ_i	p_{ij}^k
(i) B_j	$\alpha\gamma$	$\alpha\beta\gamma$	γ even	$\beta\gamma$	$\sum_{j=0}^{\beta-1} k_{j\alpha+i}$	$(j-i,k-i)_\alpha$
(ii) A_j	$\alpha\gamma+1$	$(\alpha\gamma+1)\beta$	γ even	$\beta\gamma$	$\sum_{j=0}^{\beta-1} \ell_{j\alpha+i}$	$(j-i,k-i)_\alpha$
(iii) B_j	$\alpha\gamma$	$\alpha\beta\gamma$	β even, γ odd	$\beta\gamma$	$\sum_{j=0}^{\beta-1} K_{j\alpha+i}$	$(k-j,i-j)_\alpha = (k-i,j-i)_\alpha$
(iv) A_j	$\alpha\gamma+1$	$(\alpha\gamma+1)\beta$	β even, γ odd	$\beta\gamma$	$\sum_{j=0}^{\beta-1} L_{j\alpha+i}$	$(k-j,i-j)_\alpha = (k-i,j-i)_\alpha$

Proof. The first series, with initial blocks B_j and γ even, is that constructed in [10]; the proofs for the other three series of designs are exactly similar, except for the verification that when β is even and γ odd, we have the equality listed in the last column of the table. Using again the information given in [9, pp.24-26], we have

$$\begin{aligned}(k-j,i-j)_\alpha &= \big(-(j-k),(i-k)-(j-k)\big)_\alpha \\ &= (j-k,i-k)_\alpha = (i-k,j-k)_\alpha \quad \text{since } \beta\gamma \text{ is even} \\ &= \big(-(i-k),(j-k)-(i-k)\big)_\alpha \\ &= (k-i,j-i)_\alpha,\end{aligned}$$

so that $p_{ij}^k = p_{ji}^k$ and we indeed have a design.

We now generalize Theorem 1.

Theorem 2. *Let* $\beta\gamma$ *be even. Then the* β *sets* $E_{j\alpha}$, $j = 0,1,\ldots,\beta-1$, *or the* β *sets* $F_{j\alpha}$, $j = 0,1,\ldots,\beta-1$, *may be used as the initial blocks of* PBIBD(m) *where* $v = p^n$, $b = \beta p^n$, $m \leq \alpha$, *and each associate class consists of a cyclotomic class* C_i *or a union of such classes. The parameters of the design are given in the following table, which includes* n_i, λ_i *and* p_{ij}^k *when* $m = \alpha$ *so that each cyclotomic class is an associate class.*

Initial blocks	k	r	Parameters when $m = \alpha$		
			n_i	λ_i	p_{ij}^k
(i) $E_{j\alpha}$	$t\gamma$	$t\beta\gamma$	$\beta\gamma$	$\sum_{j=0}^{\beta-1} d_{j\alpha+i}$	$(k-j,i-j)_\alpha$
(ii) $F_{j\alpha}$	$t\gamma+1$	$(t\gamma+1)\beta$	$\beta\gamma$	$\sum_{j=0}^{\beta-1} \delta_{j\alpha+i}$	$(k-j,i-j)_\alpha$

Proof. From Lemma 3(i), we have

$$E_k - E_k = \mathop{\&}_{j=0}^{\alpha\beta-1} d_j D_{j+k},$$

where

$$\mathop{\&}_{j=0}^{\alpha\beta-1} d_j = t(t\gamma - 1).$$

Hence

$$\mathop{\&}_{j=0}^{\beta-1} (E_{j\alpha} - E_{j\alpha}) = \mathop{\&}_{j=0}^{\beta-1} \mathop{\&}_{k=0}^{\alpha\beta-1} d_k D_{j\alpha+k}$$

$$= \mathop{\&}_{k=0}^{\alpha\beta-1} d_k \mathop{\&}_{j=0}^{\beta-1} D_{j\alpha+k}$$

$$= \mathop{\&}_{k=0}^{\alpha-1} \left(\sum_{i=0}^{\beta-1} d_{k+\alpha i} \right) C_k.$$

Hence the properties of the first series follows from [8, Theorem 2.1].

The proof for (ii) is analogous.

Now we note that, as in similar work of Sprott [8] and J.S. Wallis [12], further results can be obtained using the fact that $2 \mid (p^n-1)$, and again when $4 \mid (p^n-1)$.

Theorem 3. *Let* $\beta\gamma$ *be even and let* $p^n = 2\alpha\beta\gamma+1$ *be a prime power. Then the* β *sets* $E_{j\alpha}$, $j = 0,1,\ldots,\beta-1$, *or the* β *sets* F_j, $j = 0,1,\ldots,\beta-1$, *may be used as the initial blocks of a* PBIBD(m), *where* $v = p^n$, $b = \beta p^n$, $m \leq \alpha$, *and each associate class consists of a cyclotomic class*

$$C_i = \{x^{a\alpha+i} \mid a = 0,1,\ldots,2\beta\gamma-1\}, \qquad i = 0,1,\ldots,\alpha-1$$

or a union of such classes. The parameters of the design are given in the following table, which includes n_i, λ_i *and* p_{ij}^k *when* $m = \alpha$ *so that each cyclotomic class is an associate class.*

Initial blocks	k	r	Parameters when $m = \alpha$		
			n_i	λ_j	p_{ij}^k
(i) $E_{j\alpha}$	$t\gamma$	$t\beta\gamma$	$2\beta\gamma$	$\sum_{i=0}^{\beta-1} d_{i\alpha+j}$	$(k-j,i-j)_\alpha$
(ii) $F_{j\alpha}$	$t\gamma+1$	$\beta(t\gamma+1)$	$2\beta\gamma$	$\sum_{i=0}^{\beta-1} \delta_{i\alpha+j}$	$(k-j,i-j)_\alpha$

Note: in (i), $\sum_{j=0}^{m-1} \lambda_j = t(t\gamma-1)/2$; in (ii), $\sum_{j=0}^{m-1} \lambda_j = t(t\gamma+1)/2$.

Proof. This is similar to that of Theorem 2.

Next we note that for $e = 2 = \alpha$, $f = 2\beta\gamma$, the cyclotomic array becomes

$$\begin{bmatrix} \beta\gamma-1 & \beta\gamma \\ \beta\gamma & \beta\gamma \end{bmatrix} = \begin{bmatrix} (p^n-5)/4 & (p^n-1)/4 \\ (p^n-1)/4 & (p^n-1)/4 \end{bmatrix}$$

giving the following generalisation of [8, Theorem 3.1].

Corollary. *If* $p^n = 4\beta\gamma+1 = v$ *is a prime power and* $t \leq 4\beta\gamma$ *is a positive integer, then there exists a* PBIBD(2) *with parameters* $v = p^n$, $b = 2t\beta\gamma v$, $r = 2t\beta\gamma k$, $k = t\gamma$; $n_1 = n_2 = 2\beta\gamma$, $\lambda_1+\lambda_2 = t(t\gamma-1)/2$ *(with* $\lambda_j = \sum_{i=0}^{\gamma-1} d_{2i+j}$, *where* d_h *was previously defined) and*

$$p^1 = \begin{bmatrix} (v-5)/4 & (v-1)/4 \\ (v-1)/4 & (v-1)/4 \end{bmatrix}, \qquad p^2 = \begin{bmatrix} (v-1)/4 & (v-1)/4 \\ (v-1)/4 & (v-5)/4 \end{bmatrix}$$

4. NUMBERS OF ASSOCIATION CLASSES IN PBIBDs

We now consider more fully the PBIBDs constructed from the initial blocks B_j in Theorem 1(i). So far, we know that each association class must be a union of complete cyclotomic classes, C_i, with respect to $e_2 = \alpha$, and hence that m, the number of association classes, cannot exceed α. We are particularly interested in the case $m = 1$, that is, in the conditions under which the design is balanced.

The precise value of m depends on the prime power p^n, and on certain sums of cyclotomic numbers for GF[p^n] with respect to $e_1 = \alpha\beta$. Since cyclotomic numbers are known only for certain small orders e, a full treatment of possible values of m for any prime power p^n seems impossible at present.

For any given $p^n = \alpha\beta\gamma+1$, the number of possible different sets of initial blocks $\{B_0,B_1,\ldots,B_{\alpha-1}\}$ must be $\beta^{\alpha-1}$, from the conditions of the Theorem. However, often these different choices give rise to isomorphic PBIBDs, as will become obvious from our proofs.

Lemma 4. *Let* $p^n = \alpha\beta\gamma+1$, *where* p *and* α *are both odd primes. In the notation of Theorem 1, if* $m = \alpha-1$, *then we must have*

$$(0,1)_\alpha = (0,2)_\alpha = \ldots = (0,\alpha-1)_\alpha.$$

Proof. Since $m = \alpha-1$, the association classes must consist of one cyclotomic class each, except for one which consists of $C_s \cup C_t$ for some s, t such that $0 \leq s < t \leq \alpha-1$. By Lemma 1(i), since $\beta\gamma$ is even, we know that

$$C_i - C_i = \sum_{j=0}^{\alpha-1} (0,j-i)_\alpha C_j,$$

and hence by [8, Theorem 2.1] we must have $(0,t-i)_\alpha = (0,s-i)_\alpha$ for every i, $i = 0,1,\ldots,\alpha-1$, $i \neq s,t$. Since α is prime, this implies the Lemma. (Note that a similar argument will work for other values of α, provided that s-t is coprime to α.)

Corollary. *If* $\alpha = 3$ *and* $m = 2$, *then* $p \equiv 2 \pmod 3$ *and* n *is even. If* $\alpha = 5$ *and* $m = 4$, *then* $p \equiv 4 \pmod 5$ *and* n *is even.*

Proof. For $e_2 = \alpha = 3$, the cyclotomic numbers are given by Storer [9, Array 3 and Lemma 7]. Here, $(i,j)_3$ occurs in position (i+1,j+1) of the array

$$\begin{bmatrix} A & B & C \\ B & C & D \\ C & D & B \end{bmatrix},$$

for i,j = 0,1,2, and A, B, C, D are defined by

$$\begin{aligned} 9A &= p^n - 8 + c, \\ 18B &= 2p^n - 4 - c - 9d, \\ 18C &= 2p^n - 4 - c + 9d, \\ 9D &= p^n + 1 + c, \end{aligned}$$

where $4p^n = c^2+27d^2$, $c \equiv 1 \pmod 3$, is the proper representation of $4p^n$. By the Lemma,

if $m = 2$, then $B = C$, which means that $d = 0$ and $4p^n = c^2$. Hence n is even and $p \equiv 2 \pmod 3$.

Similarly, if $\alpha = 5$, the cyclotomic numbers are given by Whiteman [14, p.101] and the condition for $m = 4$ follows from his results.

Lemma 5. *In* $GF[p^{2n}]$, *with* $e_1 = \alpha\beta = p^n+1$, $f_1 = \gamma = p^n-1$, *designs arising from Theorem 1(i) are* BIBDs *(that is,* $m = 1$*) with parameters*

$$(p^{2n},\ \beta p^{2n},\ p^{2n} - 1,\ \alpha\gamma,\ \alpha\gamma - 1).$$

Proof. (i) Since

$$D_0 = GF[p^n] \setminus \{0\},$$

we have

$$D_0 + 1 = \{\{0\} \cup D_0\} \setminus \{1\},$$

so that

$$(0,0)_{e_1} = \gamma - 1$$

and

$$(0,i)_{e_1} = 0 \quad \text{for} \quad i \neq 0.$$

(ii) For $i \neq 0$, D_i is the set of non-zero elements of an additive group (but not a subfield) and $1 \notin D_i$. Hence if $g \in D_i$, we know that $g+1 \notin D_0 \cup D_i$, so that

$$(i,0)_{e_1} = (i,i)_{e_1} = 0, \quad \text{for} \quad i \neq 0.$$

(iii) Suppose that $g, h \in (D_i+1) \cap D_j$. Then

$$g-h \in \{D_i \cap D_j\} \cup \{0\},$$

but since $D_i \cap D_j = \emptyset$, we must have $g-h = 0$ or $g = h$. Hence

$$(i,j)_{e_1} \leq 1.$$

But $\sum_{j=0}^{e_1-1} (i,j)_{e_1} = \gamma$ [9, Lemma 3(d)], and since $(i,0)_{e_1} = (i,i)_{e_1} = 0$, we must have

$$(i,j)_{e_1} = 1 \quad \text{for} \quad i \neq j, \quad i \neq 0.$$

(iv) Now $B_0 = D_0 \cup D_{i_1} \cup \ldots \cup D_{i_{\alpha-1}}$, where

$$\{i_0 = 0, i_1, \ldots, i_{\alpha-1}\}$$

is a complete set of residues modulo α, chosen from $\{0,1,\ldots,\alpha\beta-1\}$. Now

$$B_0 - B_0 = \mathop{\&}_{h=0}^{\alpha-1} (D_{i_h} - D_{i_h}) \;\&\; 2 \mathop{\&}_{0 \le h < \ell \le \alpha-1} (D_{i_h} - D_{i_\ell}).$$

From the first collection of terms in this expansion, we get $(\gamma-1)$ copies of D_{i_h} for $h = 0,1,\ldots,\alpha-1$. The second collection of terms consists of $\alpha(\alpha-1)/2$ collections of differences; $D_{i_h} - D_{i_\ell}$ consists of one copy each of D_i for each $i \neq i_h$ or i_ℓ (by (ii) and (iii) above). Hence D_i occurs $(\gamma-1)+2\{\frac{\alpha(\alpha-1)}{2} - (\alpha-1)\}$ times if $i = i_h$, or $\alpha(\alpha-1)$ times if $i \neq i_h$. Since $B_j = x^j \times B_0$, and since the set $\{i_0 = 0, i_1, \ldots, i_h\}$ forms a complete set of residues modulo α, we find that each D_i occurs altogether $(\gamma-1)+2\{\frac{\alpha(\alpha-1)}{2} - (\alpha-1) + \frac{(\beta-1)\alpha(\alpha-1)}{2}\}$ times, which reduces to $\lambda = \alpha\gamma-1$, since $\alpha\beta = \gamma+2$. This completes the proof.

Example 1. In $GF[11^2]$ with $\alpha = 3$, $\beta = 4$, $\gamma = 10$, so that $e_1 = 11+1$, $f_1 = 11-1$, choose $a \equiv 1 \pmod 3$, $b \equiv 2 \pmod 3$, where $0 \le a, b \le 11$, and consider the set of initial blocks $\{B_j,\ j = 0,1,2,3\}$ where $B_0 = D_0 \cup D_a \cup D_b$, in the notation of Theorem 1(i). Then these blocks generate a BIBD with parameters $(121,484,120,30,29)$. Note that the particular choice $a = 4$, $b = 8$ gives a design constructed by Sprott [7, Series A] but that there are altogether $4^{3-1} = 16$ different choices which will give equivalent designs.

If the cyclotomic numbers of order $e_1 = \alpha\beta$ are known, then conditions on $p^n = \alpha\beta\gamma+1$ and on the initial blocks $\{B_j\}$ can be found, in order that $m = 1$. It will be convenient to make the following definition. Let

$$M_{\alpha,\beta}(a,k) = \sum_{j=0}^{\beta-1} (a, j\alpha+k),$$

where $k = 0,1,\ldots,\alpha-1$, and the cyclotomic numbers are with respect to $e_1 = \alpha\beta$.

Consider the case $\alpha = 2$; one initial block will be $B_0 = D_0 \cup D_a$ where $a = i_1 \equiv 1 \pmod 2$. Since γ is even, $D_i = -D_i$, so that we may consider sums of classes. Now

$$B_0 - B_0 = (D_0+D_0) \;\&\; x^a \times (D_0+D_0) \;\&\; 2(D_0+D_a)$$

$$= \mathop{\&}_{i=0}^{e_1-1} \{(0,i) + (0,i-a) + 2(a,i)\}D_i,$$

so that altogether

$$\mathop{\&}_{j=0}^{\beta-1} (B_j - B_j) = \{\gamma-1+2\sum_{i=0}^{\beta-1} (a,2i)\}C_0 \;\&\; \{\gamma-1+2\sum_{i=0}^{\beta-1} (a,2i+1)\}C_1.$$

To ensure that m = 1, we need these two coefficients to be equal, so we must have

$$\sum_{i=0}^{\beta-1} (a,2i)_{e_1} = \sum_{i=0}^{\beta-1} (a,2i+1)_{e_1}$$

or

$$M_{2,\beta}(a,0) = M_{2,\beta}(a,1).$$

For the cases $\alpha = 2$, $\beta = 3,5,7$ ($e_1 = 6,10,14$), this condition can be worked out more explicitly using the results of Dickson [2], Whiteman [14] and Muskat [5] respectively. We let $B_\beta(i,j)$ denote the Dickson-Hurwitz sums [14, p.97] for $e = \beta$. Also a denotes an odd integer, so that $D_0 \cup D_a$ is one of the possible initial blocks. For β odd, $D_0 \cup D_\beta$ will always generate a BIBD, since it is simply the β-residues of the field [7]. Note that we need not consider $D_0 \cup D_a$ and $D_0 \cup D_{e_1-a}$ separately, because $(i,j) = (e-i,j-i)$ and this, together with the fact that a is odd, implies that

$$M_{2,\beta}(a,0) = M_{2,\beta}(2\beta-a,1)$$

and

$$M_{2,\beta}(a,1) = M_{2,\beta}(2\beta-a,0).$$

So for β odd we need only deal with $a = 1,3,\ldots,\beta-2$, and for β even, with $a = 1,3,\ldots,\beta-1$.

Throughout this section, M is defined by $x^M \equiv 2 \pmod p$; M is taken modulo β. By direct computation using the results of [2], [5] and [14], we find that for $M \equiv k \pmod \beta$, m = 1 if and only if

$$B_\beta(\beta-a-2K,1) = B_\beta(\beta+a-2k,1) \qquad (1)$$

for $\beta = 3,5,7$. We have been unable to discover whether such an equation holds for larger values of β.

To indicate the way in which we proved (1), consider the case $\alpha = 2, \beta = 5, e_1 = 10$, $a = 1$, $M \equiv 1 \pmod 5$. In order to have only one coset class, we need

$$M_{2,5}(a,0) = M_{2,5}(a,1),$$

or

$$\sum_{i=0}^{4} (a,2i)_{10} = \sum_{i=0}^{4} (a,2i+1)_{10}.$$

Since $a = 1$, this becomes

$$(1,0) + (1,2) + (1,4) + (1,6) + (1,8) = (1,1) + (1,3) + (1,5) + (1,7) + (1,9). \qquad (2)$$

The values of the cyclotomic numbers in [14] are expressed in terms of p, x, u, v, w, where

$$\left.\begin{aligned} 16p^n &= x^2 + 50u^2 + 50v^2 + 125w^2, \\ xw &= v^2 - 4uv - u^2, \\ x &\equiv 1 \pmod 5. \end{aligned}\right\} \qquad (3)$$

For instance, when $M \equiv 1 \pmod 5$ we have

$$200(1,6) = 2p^n + 2 + x - 25u - 25v.$$

Substituting these values in (2) reduces it to

$$10p^n - 10 + 75u + 25v - 125w = 10p^n - 10 - 75u - 25v + 125w$$

or

$$3u + v = 5w.$$

Equivalently using equations (4.7) and the results of §6 of [14], we find that

$$B_5(2,1) = B_5(4,1),$$

which is one particular case of (1). Considering each case in turn, we derive (1).

Using equations (3), we may state the conditions equivalent to (1) for $\alpha = 2$, $\beta = 5$ in terms of p, x, u, v, w. These are contained in Table 1.

Table 1.

$\alpha = 2$, $\beta = 5$, $e_1 = 10$.

mod 5	a = 1	a = 3
$M \equiv 0$	$u + 2v = 0$	$2u = v$
$M \equiv 1$	$5w = 3u + v$	$x = 2u + 4v + 5w$
$M \equiv 2$	$4u = x + 2v + 5w$	$3v = u + 5w$
$M \equiv 3$	$2v = x + 4u + 5w$	$u = 3v + 5w$
$M \equiv 4$	$3u + v + 5w = 0$	$5w = x + 2u + 4v.$

Similarly for $\alpha = 2$, $\beta = 3$, $e_1 = 6$, $p^n = A^2+3B^2$, we find that for $M \equiv 0$, 1 or $2 \pmod 3$, if $m = 1$, then

$$p^n = A^2, \qquad B = 0.$$

Example 2. Let $p = 421$. By [3], we find that $M \equiv 1 \pmod 5$. Also $(x,u,v,w) = (-19,8,1,5)$ and $3u+v = 5w$. So $C_0 \cup C_1$ will be one of the initial blocks for a BIBD with parameters (421, 2105, 420, 84, 83).

If $\alpha = 3$, one initial block will be $D_0 \cup D_a \cup D_b$ where $a \equiv 1 \pmod 3$, $b \equiv 2 \pmod 3$. A similar argument shows that, for $m = 1$, we must have

$$\begin{aligned} M_{3,\beta}(a,0) + M_{3,\beta}(b,0) + M_{3,\beta}(b-a,2) &= M_{3,\beta}(a,1) + M_{3,\beta}(b,1) + M_{3,\beta}(b-a,0) \\ &= M_{3,\beta}(a,2) + M_{3,\beta}(b,2) + M_{3,\beta}(b-a,1). \end{aligned}$$

Again we need not consider all possible values of a and b. To see this, we need the following result.

Lemma 6. *(i) If β is even, then*

$$M_{3,\beta}\left(\frac{3\beta}{2}+(3k+1),i\right) = M_{3,\beta}\left(\frac{3\beta}{2}-(3k+1),i+2\right),$$

$$M_{3,\beta}\left(\frac{3\beta}{2}+(3k+2),i\right) = M_{3,\beta}\left(\frac{3\beta}{2}-(3k+2),i+1\right),$$

where $k = 0,1,\ldots,\frac{\beta}{2}-1$, *and* i, i+1, i+2 *are taken modulo* 3.

(ii) If β is odd, then

$$M_{3,\beta}\left(\frac{3\beta+(3k+2)}{2},\ i\right) = M_{3,\beta}\left(\frac{3\beta-(3k+2)}{2},\ i+2\right),$$

where $k = 1,3,\ldots,\beta-4,\beta-2$, *and*

$$M_{3,\beta}\left(\frac{3\beta+(3k+1)}{2},\ i\right) = M_{3,\beta}\left(\frac{3\beta-(3k+1)}{2},\ i+1\right),$$

where $k = 0,2,\ldots,\beta-3,\beta-1$. *In both cases* i, i+1, i+2 *are taken modulo* 3.

Proof. The result follows immediately from the fact that

$$(i,j) = (e-i,j-i).$$

Corollary. *If $B_0 = D_0 \cup D_a \cup D_b$, $a \equiv 1 \pmod 3$, $b \equiv 2 \pmod 3$, as one initial block yields $m = 1$ in Theorem 1(i), then so do the initial blocks $C_0 \cup C_{b-a} \cup C_{3\beta-a}$ and $C_0 \cup C_{3\beta-b} \cup C_{3\beta-(b-a)}$.*

Proof. The Corollary follows by considering the three expressions which are equal if $C_0 \cup C_a \cup C_b$ yields $m = 1$, and then applying the Lemma.

5. LATIN SQUARE DESIGNS FROM CYCLOTOMY

Throughout this Section, we let p be a prime and factor $p+1 = \alpha\beta$, where $\alpha, \beta \geq 2$. We consider the field $GF[p^2]$ and the cyclotomic numbers with respect to α and $\alpha\beta$. Obviously $p^2 = \alpha\beta(p-1)+1 = a\phi+1$, say, where $\phi = \beta(p-1)$. We let C_0 denote the α^{th} power residues of the field, C_i the cyclotomic class $x^i \times C_0$, D_0 the $\alpha\beta^{th}$ power residues and D_i the cyclotomic class $x^i \times D_0$, where x is a generator of the multiplicative group of the field. Notice that

$$C_i = -C_i, \qquad D_i = -D_i,$$
$$C_i = \bigcup_{j=0}^{\beta-1} D_{j\alpha+i}, \tag{4}$$

D_0 is the set of non-zero elements of the sub-field of order p and each D_i consists of the non-zero elements of an additive subgroup of the field.

We have the following result.

Theorem 4. *The set C_0 may be used as the initial block of an $L_\beta(p)$ PBIBD(2), where $b = p^2$, $r = k = \phi$, and (since we have a Latin Square design) the remaining parameters are $v = b$, $n_1 = \phi$, $n_2 = (\alpha-1)\phi$, $\lambda_1 = \beta^2+(\alpha-3)\beta-1 = (0,0)_\alpha$, $\lambda_2 = \beta(\beta-1) = (0,i)_\alpha$ for $i \neq 0$,*

$$P^1 = \begin{bmatrix} \beta^2+(\alpha-3)\beta-1 & (\alpha-1)\beta(\beta-1) \\ (\alpha-1)\beta(\beta-1) & (1-\alpha)\beta\{(1-\alpha)\beta+1\} \end{bmatrix} \text{ and } P^2 = \begin{bmatrix} \beta(\beta-1) & \beta\{(\alpha-1)\beta-1\} \\ \beta\{(\alpha-1)\beta-1\} & (\alpha-1)^2\beta^2+\beta(3-2\alpha)-1 \end{bmatrix}.$$

To prove the Theorem, we need one preliminary result.

Lemma 6. *The cyclotomic numbers with respect to $\alpha\beta$ are as follows:*

$$\begin{aligned} (0,0)_{\alpha\beta} &= p-2; \\ (0,i)_{\alpha\beta} &= 0, \quad i \neq 0; \\ (\alpha s,0)_{\alpha\beta} &= (\alpha s,\alpha s)_{\alpha\beta} = 0, \quad s \neq 0; \\ (\alpha s,i)_{\alpha\beta} &= 1, \quad i \neq 0 \text{ or } \alpha s. \end{aligned}$$

Proof. (i) $D_0 = GF[p] \setminus \{0\}$, so $D_0+1 = GF[p] \setminus \{1\}$. Hence $(0,0)_{\alpha\beta} = p-2$ and $(0,i)_{\alpha\beta} = 0$ for $i \neq 0$.

(ii) $D_{\alpha s}$ consists of the non-zero elements of an additive subgroup of order p, and $1 \notin D_{\alpha s}$ since $1 \in D_0$. Suppose that $y \in D_{\alpha s}$. Then $y+1 \notin D_0 \cup D_{\alpha s}$, so that

$$(\alpha s,0)_{\alpha\beta} = (\alpha s,\alpha s)_{\alpha\beta} = 0 \quad \text{for} \quad s \neq 0.$$

(iii) Finally suppose that $u,v \in (D_{\alpha s}+1) \cap D_i$. Then $u-v \in \{D_{\alpha s} \cap D_i\} \cup \{0\}$, which implies that $u-v = 0$ and $u = v$. Hence $(\alpha s,i)_{\alpha\beta} \leq 1$.

But by [9, Lemma 3(d)], we know that

$$\sum_{i=0}^{\alpha\beta-1} (\alpha s,i)_{\alpha\beta} = p-1,$$

and since $(\alpha s,0)_{\alpha\beta} = (\alpha s,\alpha s)_{\alpha\beta} = 0$, we must have

$$(\alpha s,i) = 1 \quad \text{for each} \quad i \neq 0 \quad \text{or} \quad \alpha s.$$

Corollary. *By the Lemma and (4) we have*

$$(0,0)_\alpha = p - 2 + (\beta-2)(\beta-1) = \beta^2 + (\alpha-3)\beta - 1,$$

and

$$(0,i)_\alpha = (i,0)_\alpha = \beta(\beta-1), \qquad i \neq 0.$$

Proof of the Theorem.

(i) We begin by using the main Theorem of [8] to check the parameters of the design. Certainly if we let $C_0 = B_0$, the initial block, then $B_0-B_0 = C_0-C_0$ and, since $C_0 = -C_0$, we have

$$B_0-B_0 = \{\beta^2+(\alpha-3)\beta-1\}C_0 \,\&\, \beta(\beta-1)\{C_1 \cup C_2 \cup \ldots \cup C_{\alpha-1}\}.$$

Now $G-G = p^2G$, where G denotes $GF[p^2]$, and

$$\begin{aligned} G-C_0 &= \beta(p-1)G = \beta(\alpha\beta-2)G \\ &= (C_0-C_0) \,\&\, (\{C_1 \cup C_2 \cup \ldots \cup C_{\alpha-1}\}-C_0) \,\&\, (\{0\}-C_0) \\ &= (\beta^2+(\alpha-3)\beta-1)C_0 \,\&\, \beta(\beta-1)\{C_1 \cup C_2 \cup \ldots \cup C_{\alpha-1}\} \\ &\qquad \&\, (\{C_1 \cup C_2 \cup \ldots \cup C_{\alpha-1}\}-C_0) \,\&\, C_0. \end{aligned}$$

Hence $\{C_1 \cup C_2 \cup \ldots \cup C_{\alpha-1}\}-C_0 = (\alpha-1)\beta(\beta-1)C_0 \,\&\, \beta[(\alpha-1)\beta-1]\{C_1 \cup C_2 \cup \ldots \cup C_{\alpha-1}\}$.

Similarly $G-\{C_1 \cup C_2 \cup \ldots \cup C_{\alpha-1}\} = (\alpha-1)\beta(\alpha\beta-2)G$

$$\begin{aligned} &= (C_0-\{C_1 \cup C_2 \cup \ldots \cup C_{\alpha-1}\}) \,\&\, (\{C_1 \cup C_2 \cup \ldots \cup C_{\alpha-1}\} - \\ &\qquad -\{C_1 \cup C_2 \cup \ldots \cup C_{\alpha-1}\}) \,\&\, (\{0\}-\{C_1 \cup C_2 \cup \ldots \cup C_{\alpha-1}\}) \\ &= (\alpha-1)\beta(\beta-1)C_0 \,\&\, [\beta\{(\alpha-1)\beta-1\}+1]\{C_1 \cup C_2 \cup \ldots \cup C_{\alpha-1}\} \,\&\, \\ &\qquad (\{C_1 \cup C_2 \cup \ldots \cup C_{\alpha-1}\}-\{C_1 \cup C_2 \cup \ldots \cup C_{\alpha-1}\}). \end{aligned}$$

Hence $\{C_1 \cup C_2 \cup \ldots \cup C_{\alpha-1}\} - \{C_1 \cup C_2 \cup \ldots \cup C_{\alpha-1}\} = (1-\alpha)\beta\{(1-\alpha)\beta+1\}C_0 \& [(\alpha-1)^2\beta^2+\beta(3-2\alpha)-1]$ $\{C_1 \cup C_2 \cup \ldots \cup C_{\alpha-1}\}$.

So the existence of the PBIBD(2) with the given parameters follows by [8].

(ii) To complete the proof, we have to show that in fact we have a Latin square design. That the parameters are those of an $L_\beta(p)$ design follows from [6, p.129].

The first associates of [0,0] are the elements of C_0; in general, the first associates of [i,j] are the elements of C_0+[i,j], where the elements of GF[p^2] are denoted by [i,j], i,j = 0,1,...,p-1. To show that we have a Latin square design, we construct (β-2) mutually orthogonal Latin squares as follows.

We write the elements of GF[p^2] in a $p \times p$ array, with [0,0] in the top left corner, the elements [0,1], [0,2], ..., [0,p-1] of D_0 across the top row, the elements [1,a], [2,2a], ..., [p-1,(p-1)a] of D_α down the left-most column and the elements [i,ia]+[0,j] = [i,ia+j] in the i,j position. Now for each s = 2,3,...,β-1, let L_s be the Latin square with a_1 in the i,j position if and only if an element of $D_{s\alpha} \cup \{0\}$ occupies the i,j position of the array, and a_k in the i,j position if and only if a_1 occupies the i,j-k+1 position. For example, if p = 7, and α = 2, β = 4, then our array of elements of GF[7^2] is

00	01	02	03	04	05	06
14	15	16	10	11	(12)	13
21	22	23	(24)	25	26	20
35	(36)	30	31	32	33	34
42	43	44	45	46	40	(41)
56	50	51	52	(53)	54	55
63	64	(65)	66	60	61	62,

where the elements of D_0 occupy the top row, those of D_2 the left column, those of D_4 are underlined and those of D_6 are circled. The corresponding Latin squares are then

$$L_2 = \begin{bmatrix} a_1 & a_2 & a_3 & a_4 & a_5 & a_6 & a_7 \\ a_2 & a_3 & a_4 & a_5 & a_6 & a_7 & a_1 \\ a_3 & a_4 & a_5 & a_6 & a_7 & a_1 & a_2 \\ a_4 & a_5 & a_6 & a_7 & a_1 & a_2 & a_3 \\ a_5 & a_6 & a_7 & a_1 & a_2 & a_3 & a_4 \\ a_6 & a_7 & a_1 & a_2 & a_3 & a_4 & a_5 \\ a_7 & a_1 & a_2 & a_3 & a_4 & a_5 & a_6 \end{bmatrix}$$

and

$$L_3 = \begin{bmatrix} a_1 & a_2 & a_3 & a_4 & a_5 & a_6 & a_7 \\ a_3 & a_4 & a_5 & a_6 & a_7 & a_1 & a_2 \\ a_5 & a_6 & a_7 & a_1 & a_2 & a_3 & a_4 \\ a_7 & a_1 & a_2 & a_3 & a_4 & a_5 & a_6 \\ a_2 & a_3 & a_4 & a_5 & a_6 & a_7 & a_1 \\ a_4 & a_5 & a_6 & a_7 & a_1 & a_2 & a_3 \\ a_6 & a_7 & a_1 & a_2 & a_3 & a_4 & a_5 \end{bmatrix}$$

To check that these squares are mutually orthogonal, suppose that a_u occupies the (i,j) and (k,ℓ) positions of L_s and that a_v occupies the (i,j) and (k,ℓ) positions of L_t. Without loss of generality, we may assume that $u = 1$, so that $[i,ia+j]$ and $[k,ka+\ell]$ both belong to $D_{\alpha s} \cup \{0\}$. Similarly a_1 appears in the $(i,j-t+1)$ and $(k,\ell-t+1)$ positions of L_t, so $[i,ia+j-t+1]$ and $[k,ka+\ell-t+1]$ both belong to $D_{\alpha t} \cup \{0\}$. But since $D_{\alpha s} \cup \{0\}$ and $D_{\alpha t} \cup \{0\}$ are both subgroups, this means that

$$\begin{aligned} [i,ia+j] - [k,ka+\ell] &= [i-k,(i-k)a+j-\ell] \\ &= [i,ia+j-t+1] - [k,ka+\ell-t+1] \end{aligned}$$

must belong to $[D_{\alpha s} \cup \{0\}] \cap [D_{\alpha t} \cup \{0\}]$ and hence must be zero. That is,

$$i-k = 0 \quad \text{and} \quad (i-k)a+j-\ell = 0,$$

so that $i = k$, $j = \ell$ and L_s, L_t are mutually orthogonal.

REFERENCES

[1] R.C. Bose and K.R. Nair, Partially balanced incomplete block designs, *Sankhya* 4 (1938), 337-372.

[2] L.E. Dickson, Cyclotomy, higher congruences and Waring's problem, *Amer. J. Math.* 57 (1935), 391-424.

[3] C.G.J. Jacobi, *Canon Arithmeticus*, Akademie-Verlag, Berlin (1956).

[4] Emma Lehmer, On residue difference sets, *Canad. J. Math.* 5 (1953), 425-432.

[5] J.B. Muskat, The cyclotomic numbers of order fourteen, *Acta Arith.* XI (1966), 263-279.

[6] Damaraju Raghavarao, *Constructions and combinatorial problems in design of experiments*, (John Wiley and Sons Inc., New York, London, Sydney, Toronto, 1972).

[7] D.A. Sprott, A note on balanced incomplete block designs, *Canad. J. Math.* 6 (1954), 341-346.

[8] D.A. Sprott, Some series of partially balanced incomplete block designs, *Canad. J. Math.* 7 (1955), 369-381.

[9] Thomas Storer, *Cyclotomy and difference sets*, (Markham Publishing Co., Chicago, 1967).

[10] Anne Penfold Street and W.D. Wallis, Nested designs from sum-free sets, *Combinatorial Math. III*, Proc. Third Australian Conf., Lecture Notes in Math. 452, pp.214-226, (Springer-Verlag, Berlin, Heidelberg, New York, 1975).

[11] Jennifer Seberry Wallis, Some remarks on supplementary difference sets, *Colloq. Math. Soc. Janos Bolyai* 10. Infinite and finite sets, Keszthely, Hungary, 1973, pp.1503-1526.

[12] Jennifer Wallis, A note on BIBDs, *J. Austral. Math. Soc.*, 16 (1973), 257-261.

[13] W.D. Wallis, Anne Penfold Street and Jennifer Seberry Wallis, *Combinatorics: Room squares, sum-free sets, Hadamard matrices*, Lecture Notes in Math., 292, (Springer-Verlag, Berlin, Heidelberg, New York, 1972).

[14] A.L. Whiteman, The cyclotomic numbers of order ten, *Proc. Symposia App. Math.*, X (1960), 95-111.

University of Queensland
St. Lucia