A NOTE ON BALANCED INCOMPLETE BLOCK DESIGNS

D. A. SPROTT

1. Introduction. A balanced incomplete block design is defined as an arrangement of v objects in b blocks, each block containing k objects all different, so that there are r blocks containing a given object and λ blocks containing any two given objects. Such designs have been studied for their combinatorial interest, as in **(3)**, and also for their application to statistics, where the objects are usually varieties.

Various methods of construction have been studied by Bose **(1)**, who developed two "Module Theorems" and applied them to form several families of designs. It is the purpose of this note to obtain, using Bose's first Module Theorem, some more general series of designs.

2. Series A

THEOREM 2.1. *If $v = mk + 1 = p^{\alpha}$, where p is prime, then the design with parameters*

$$v = mk + 1,\ b = m(mk + 1),\ r = mk,\ k,\ \lambda = k - 1$$

can be constructed via the initial blocks

$$(x^{i},\ x^{i+m},\ x^{i+2m}, \ldots,\ x^{i+(k-1)m}),$$

where x is a primitive element of $GF(v)$ and i ranges from 0 to $m - 1$.

Proof. All differences are expressible in the form

$$x^{i+(r+s)m} - x^{i+rm} = x^{i+rm}(x^{sm} - 1) = x^{q_s + i + rm}$$

where

$$x^{sm} - 1 = x^{q_s} \qquad (s = 1, 2, \ldots, k - 1;\ r = 0, 1, \ldots, k - 1).$$

Also, such expressions run over all possible differences. The number of such differences, for s fixed is mk. Further, they are all distinct; for otherwise, for $i \neq i'$, $r \neq r'$, we have

$$i + rm \equiv i' + r'm \pmod{mk},$$

$$i - i' \equiv m(r - r') \pmod{mk},$$

$$i - i' \equiv 0 \pmod{m}.$$

Hence $i = i'$, since i and i' are less than m; so

$$r - r' \equiv 0 \pmod{k},$$

and therefore $r = r'$, since r and r' are less than k. This contradiction shows that,

Received June 16, 1953; in revised form November 9, 1953. Some of the results of this paper were obtained while the author was in receipt of a grant from the Research Council of Ontario.

https://doi.org/10.4153/CJM-1954-032-6 Published online by Cambridge University Press

for s fixed, the differences range once over $GF(v)$; hence as s ranges over its $\lambda = k - 1$ values, the differences are symmetrically repeated, each occurring λ times. Thus, by the first Module Theorem, the design can be formed by adding the elements of $GF(v)$ to the initial blocks.

This Series A includes Bose's series α_2 $(k = 4)$, α_4 $(k = 5)$ **(2)**, and part of E_2 $(k = 3)$ **(1)**.

3. Series B

THEOREM 3.1. *If $v = 2m(2\lambda + 1) + 1 = p^{\alpha}$, where p is prime, then the design with parameters*

$$v = 2m(2\lambda + 1) + 1,\ b = mv,\ r = m(2\lambda + 1),\ k = 2\lambda + 1,\ \lambda$$

can be constructed via the initial blocks

$$(x^{i}, x^{i+2m}, x^{i+4m}, \ldots , x^{i+4\lambda m})$$

where x is a primitive element of $GF(v)$ and i ranges from 0 to $m - 1$.

Proof. Here the differences are expressible in the form

$$x^{i+2rm+q_s},$$

where

$$x^{q_s} = x^{2ms} - 1 \qquad (s = 1, 2, \ldots , 2\lambda;\ r = 0, 1, \ldots , 2\lambda).$$

Since x is a primitive element, we have

$$x^{4m\lambda+2m} - 1 = 0, \qquad x^{2m\lambda+m} + 1 = 0,$$
$$x^{2m(2\lambda)} + x^{2m(2\lambda-1)} + \ldots + x^{2m} + 1 = 0.$$

Hence

$$\begin{aligned} x^{q_s} &= (x^{2m} - 1)(x^{2m(s-1)} + x^{2m(s-2)} + \ldots + 1) \\ &= -\ (x^{2m} - 1)(x^{4m\lambda} + x^{4m\lambda-2m} + \ldots + x^{2ms}) \\ &= (x^{2m} - 1)\, x^{2m\lambda+m+2ms}\, (x^{2m(2\lambda-s)} + \ldots + 1) \\ &= x^{2m\lambda+m+2ms}(x^{2m(2\lambda-s+1)} - 1). \end{aligned}$$

Thus, if we set $a = 2\lambda - s + 1$, we have

$$x^{q_a} = x^{q_s-2m\lambda-m-2ms} = x^{q_s+m(2\lambda-2s+1)}.$$

For s fixed, the differences

$$x^{q_s+i+2rm} \text{ and } x^{q_a+i+2rm} = x^{q_s+i+m(2\lambda-2s+2r+1)}$$

range together over $GF(v)$ once. For, if not, there exist i, i', r, r', such that $i = i'$, $r = r'$ do not hold simultaneously and

$$\begin{aligned} i + m(2\lambda - 2s + 2r + 1) &\equiv i' + 2r'm && \pmod{4m\lambda + 2m}, \\ i - i' &\equiv m(2r' - 2\lambda + 2s - 2r - 1) && \pmod{4m\lambda + 2m}, \\ i - i' &\equiv 0 && \pmod{m}, \\ i &= i'. \end{aligned}$$

Thus

$$2r' - 2\lambda + 2s - 2r - 1 \equiv 0 \qquad (\text{mod } 4\lambda + 2),$$

which is impossible. Hence the differences are all distinct; since there are $m(2\lambda + 1)$ of them, they range once over $GF(v)$. As s varies over $1, 2, \ldots, \lambda$, the differences will range λ times over $GF(v)$. Hence, by the first Module Theorem the design can be constructed by adding the elements of $GF(v)$ to the initial blocks.

Series B includes Bose's series S_1 ($m = 1$) **(1)**, α_3 ($\lambda = 2$) **(2)**, and part of T_2 ($\lambda = 1$) **(1)**.

4. Series C

THEOREM 4.1. *If* $v = 2m(2\lambda - 1) + 1 = p^\alpha$, *where p is prime, then the design with parameters*

$$v = 2m(2\lambda - 1) + 1,\ b = mv,\ r = 2m\lambda,\ k = 2\lambda,\ \lambda$$

can be constructed via the initial blocks

$$(0,\ x^i,\ x^{i+2m}, \ldots, x^{i+4(\lambda-1)m}),$$

where x is a primitive element of $GF(v)$ *and* $i = 0, 1, \ldots, m - 1$.

Proof. The differences not involving the zero element are just the differences which arise from the blocks of Series B with λ replaced by $\lambda - 1$; such differences are symmetrically repeated and each occurs $\lambda - 1$ times. The differences involving the zero element are

$$\pm x^i,\ \pm x^{i+2m}, \ldots, \pm x^{i+4(\lambda-1)m}.$$

Since

$$x^{2m\lambda - m} = -1,$$

these can be written as

$$x^i,\ x^{i+2m},\ x^{i+4m}, \ldots, x^{i+4(\lambda-1)m},$$
$$x^{i+m(2\lambda-1)},\ x^{i+m(2\lambda+1)}, \ldots, x^{i+m(2\lambda-3)}.$$

These differences are $2m(2\lambda - 1)$ in number and are all distinct; hence they cover $GF(v)$ once. Thus each difference occurs λ times in all, and the design can be formed by the first Module Theorem.

This series includes Bose's α_1 ($\lambda = 2$) **(2)**. For $m = 1$, one obtains the symmetric series

$$v = b = 4\lambda - 1,\ r = k = 2\lambda,\ \lambda.$$

5. Series D

THEOREM 5.1. *If* $v = 4m(4\lambda + 1) + 1 = p^\alpha$, *where p is prime, and if among the* 2λ *expressions*

$$x^{4ms} - 1 = x^{q_s} \qquad (s = 1, 2, \ldots, 2\lambda)$$

there are λ *even and* λ *odd powers of* x, *where x is a primitive element of* $GF(v)$, *then the design with parameters*

https://doi.org/10.4153/CJM-1954-032-6 Published online by Cambridge University Press

$$v = 4m(4\lambda + 1) + 1,\ b = mv,\ r = m(4\lambda + 1),\ k = 4\lambda + 1,\ \lambda$$

can be constructed via the initial blocks

$$(x^{2i}, x^{2i+4m}, x^{2i+8m}, \ldots, x^{2i+16\lambda m})$$

where i ranges from 0 *to* $m - 1$.

Proof. In a manner similar to that used in Theorem 3.1, it can be shown that, if we set $c = 4\lambda - s + 1$,

$$x^{q_c} = x^{q_s + 2m(4\lambda - 2s + 1)}.$$

Further, the differences are

$$x^{2i+4rm+q_s}, \quad x^{2i+2m(2r+4\lambda-2s+1)+q_s},$$

where s ranges from 1 to 2λ and r ranges from 0 to 4λ. By the method used in Theorem 3.1, it can be shown that, for a fixed s, these differences are all distinct and are $2m(4\lambda + 1)$ in number. Hence they range over half of the non-zero elements of $GF(v)$. Consider now the differences

$$x^{2i+4rm+q_t}, \quad x^{2i+2m(2r+4\lambda-2s+1)+q_t},$$

where q_t is even or odd according as q_s is odd or even. For t fixed, these differences range over the other half of the field $GF(v)$. For, if not, there exist i, i', r, r', such that one of the relations (1), (2), (3), (4), holds.

$$2i + 4rm + q_s \equiv 2i' + 4r'm + q_t \pmod{4m(4\lambda + 1)} \tag{1}$$

$$2i + 4rm + q_s \equiv 2i' + 2m(2r' + 4\lambda - 2s + 1) + q_t \pmod{4m(4\lambda + 1)} \tag{2}$$

$$2i + 2m(2r + 4\lambda - 2s + 1) + q_s \equiv 2i' + 4r'm + q_t \pmod{4m(4\lambda + 1)} \tag{3}$$

$$2i + 2m(2r + 4\lambda - 2s + 1) + q_s \equiv 2i' + 2m(2r' + 4\lambda - 2s + 1) + q_t \pmod{4m(4\lambda + 1)}. \tag{4}$$

Consider the relation (1), for example. If (1) holds, then

$$2(i - i') + 4(r - r')\,m + q_s - q_t \equiv 0 \pmod{4m(4\lambda + 1)},$$

which is impossible, since $q_s - q_t$ is odd. Similarly, it can be shown that relations (2), (3), and (4) are impossible.

Hence, if there exist q_s even and q_t odd, the differences involving this q_s and this q_t range once over $GF(v)$; as s and t vary, the differences will, under the condition in the theorem, range λ times over $GF(v)$. Thus the design can be constructed.

For $\lambda = 1$, this theorem gives Bose's series G_1 **(1)**; in this case, the condition in the theorem simplifies to the requirement that $x^{4m} + 1$ be an odd power of x.

THEOREM 5.2. *If the condition on the exponents q_s in Theorem* 5.1 *is violated by one primitive element of $GF(v)$, then it is violated by all primitive elements of $GF(v)$.*

Proof. $x^{q_a} = x^{q_b}$ implies

$$x^{4ma} = x^{4mb},$$

that is,

$$4ma \equiv 4mb \pmod{4m(4\lambda + 1)},$$
$$a \equiv b \pmod{4\lambda + 1}.$$

Hence, in the exponents q_s, the s may be considered as reduced modulo $4\lambda + 1$.

Let x be replaced by another primitive element $y = x^t$ where t is relatively prime to $4m(4\lambda + 1)$. Then x^{q_w} is replaced by

$$y^{q_w} = y^{4mw} - 1 = x^{4m\,tw} - 1 = x^{q_{w^*}},$$

where $w^* = wt$.

Consider these expressions $x^{q_{w^*}}$; the set of elements w^* can be divided into elements r^* and elements s^*, where $1 \leqslant r^* \leqslant 2\lambda$, $2\lambda < s^* \leqslant 4\lambda$. This subdivision determines a subdivision of the set of elements w into elements r and elements s where $tr = r^*$ and $ts = s^*$. It is clear that every r^* is a w as well as a w^*.

All the w^*'s are different; for if

$$w^* \equiv w_1^* \pmod{4\lambda + 1},$$

then

$$tw \equiv tw_1 \pmod{4\lambda + 1},$$

that is,

$$w \equiv w_1 \pmod{4\lambda + 1}.$$

This is impossible since the elements w are all distinct; hence the r^*'s are all distinct and the s^*'s are all distinct.

Define now s^{**} by the equation

$$s^* + s^{**} = 4\lambda + 1 \equiv 0 \pmod{4\lambda + 1}.$$

Then

$$\begin{aligned} q_{s^*} &= q_{4\lambda+1-(4\lambda+1-s^*)} = q_{4\lambda+1-s^{**}} \\ &= q_{s^{**}} + 2m(4\lambda + 1 - 2s). \end{aligned}$$

Also, since $2\lambda + 1 \leqslant s^* \leqslant 4\lambda$, then $1 \leqslant s^{**} \leqslant 2\lambda$. Hence the s^{**}'s are a subset of the w's; further, they are all distinct.

It can also be shown that the s^{**}'s are all different from the r^*'s; for if $s^{**} \equiv r^* \pmod{4\lambda + 1}$, then

$$4\lambda + 1 - s^* \equiv r^* \pmod{4\lambda + 1},$$
$$s^* + r^* \equiv 0 \pmod{4\lambda + 1},$$
$$t(s + r) \equiv 0 \pmod{4\lambda + 1},$$
$$(s + r) \equiv 0 \pmod{4\lambda + 1}.$$

This is impossible since s and r are at most 2λ and $s \not\equiv 0$. Hence the set of w's has been replaced by sets of elements r^* and s^{**} which are disjoint and have no repeated members, that is,

$$\{r^*\} + \{s^{**}\} = \{w\} = 1, 2, 3, \ldots, 2\lambda.$$

Thus any q_w is replaced either by another q_w or by a q_w plus an even multiple of m, and no w is repeated. So there will be as many odd and even powers of x occurring as occurred originally.

This theorem shows that the "power" condition on Series D need only be checked for one primitive element.

References

1. R. C. Bose, *On the construction of balanced incomplete block designs*, Ann. Eugenics *9* (1939), 353–399.

2. ———, *On some new series of balanced incomplete block designs*, Bull. Calcutta Math. Soc. *34* (1942), 17–31.

3. S. Chowla and H. J. Ryser, *Combinatorial problems*, Can. J. Math. *2* (1950), 93–99.

University of Toronto

https://doi.org/10.4153/CJM-1954-032-6 Published online by Cambridge University Press