The Annals of Mathematical Statistics
1971, Vol. 42, No. 3, 1118-1120

A NEW FAMILY OF BIBD'S

BY E. NEMETH

University of Waterloo

Block designs with parameters $(p^n, \Delta p^n, \Delta((p^n-1)/2), (p^n-1)/2, \Delta((p^n-3)/4))$ are shown to exist whenever p^n, a prime power, can be expressed as $2^m t+1$ with m a positive integer and t an odd integer >1, that is, whenever p^n is not one greater than a power of 2; Δ is equal to 2^{m-1}.

1. Introduction. A balanced incomplete block design, BIBD, defined on a finite set of varieties V is a collection B of subsets of V, called blocks, each of cardinality k such that every pair of distinct elements of V belongs to λ subsets of B. Five parameters (v, b, r, k, λ) are associated with a BIBD:

v = number of varieties,
b = number of blocks,
r = number of replications of each variety,
k = size of the blocks,
λ = number of replications of each pair of distinct varieties.

As discussed in Hall ([1] page 120, ff.) BIBD's may be constructed using a set of difference blocks. A set in which all possible differences comprise each nonzero element of a group G exactly λ times is called a λ-difference set for G. If, instead of a single set, a set of subsets or blocks is such that all possible differences within each subset comprise G–{0} with multiplicity λ, then such a set is called a set of difference blocks for G.

2. The construction. We proceed to form a set of difference blocks for the group G, the Galois field $GF(p^n)$. The form of the blocks and the number of blocks depend on the quantity Δ determined by p^n.

THEOREM. *Let* $p^n = 2^m t+1$ *where* t *is an odd integer* > 1, m *is a positive integer, and* $\Delta = 2^{m-1}$; *further let* x *be a primitive element in* $G = GF(p^n)$. *Then the set*

$$A = \left\{ \begin{matrix} x^0, & x^{2\Delta}, & \cdots, & x^{(2t-2)\Delta}, \\ x, & x^{2\Delta+1}, & \cdots, & x^{(2t-2)\Delta+1}, \\ \vdots & & & \vdots \\ x^{\Delta-1}, & x^{3\Delta-1}, & \cdots, & x^{(2t-1)\Delta-1} \end{matrix} \right\}$$

together with the sets $Ax, Ax^2, \cdots, Ax^{\Delta-1}$ *form a set of* $\Delta((p^n-3)/4)$ *difference blocks for* $GF(p^n)$ *and hence generate a balanced incomplete block design with parameters*

$$\left(p^n, \Delta p^n, \Delta\left(\frac{(p^n-1)}{2}\right), \frac{p^n-1}{2}, \Delta\left(\frac{p^n-3}{4}\right)\right).$$

Received January 27, 1970.

If $\Delta = 1$, then p^n has the form $2t+1$ with t odd and thus is congruent to 3 mod 4. The set $A = \{x^0, x^2, \cdots, x^{p^n-2}\}$ is the set of quadratic residues of p^n and is known to be a $\frac{1}{4}(p^n-3)$–difference set for the group G (see Hall [1] page 141). This set generates the well-known Hadamard designs.

For $\Delta = 2$, that is, $p^n = 4t+1$, the resulting design has the parameters b, r, and λ relatively prime and corresponds to the first member of a $(v, k) = (p^n, (p^n-1)/2)$ family as described in [2].

PROOF. First we consider the following subsets of A,

$$\begin{aligned} B_0 &= \{x^0, x^{2\Delta}, \cdots, x^{(2t-2)\Delta}\}, \\ B_1 &= \{x, x^{2\Delta+1}, \cdots, x^{(2t-2)\Delta+1}\}, \\ &\vdots \\ B_{\Delta-1} &= \{x^{\Delta-1}, x^{3\Delta-1}, \cdots, x^{(2t-1)\Delta-1}\}, \end{aligned}$$

as initial blocks. Sprott has shown in series B of [3] that these blocks are a set of difference blocks corresponding to $\lambda = (t-1)/2$. Thus differences within these initial blocks in each of the sets A, Ax, Ax^2, $\cdots$, $Ax^{\Delta-1}$ account for $\Delta\cdot(t-1)/2$ replications of the group G.

We now consider differences between two of these initial blocks, say B_i and B_j, where $i > j$. The differences may be resolved into classes C_d by letting $d = i-j$ and considering

$$C_d = \{x^i - x^j, x^{2\Delta+i} - x^{2\Delta+j}, \cdots, x^{(2t-2)\Delta+i} - x^{(2t-2)\Delta+j}\}.$$

Each element of C_d contains the nonzero constant factor $(1-x^d)$ which may be divided out of each term, the result still being called C_d. The other $t-1$ classes

$$C_{d+2\Delta}, C_{d+4\Delta}, \cdots, C_{d+2(t-1)\Delta},$$

are identical to C_d except for the common factor $(1-x^{d+2l\Delta})$ where $l = 1, 2, \cdots, t-1$ and $d = 1, 2, \cdots, \Delta-1$. The primitive element x is of order $2t\Delta$ and thus $d+2l$ must be equal to $2t\Delta$ for the common factor to be 0. This is impossible due to the limits of l and d. Hence, we have $t-1$ copies of the resolution class

$$C_d = \{x_i, x^{2\Delta+i}, x^{4\Delta+i}, \cdots, x^{(2t-2)\Delta+i}\}.$$

We now consider the differences generated by the class C_d in Ax, Ax^2, Ax^3, $\cdots$, $Ax^{\Delta-1}$.

These are, in addition to C_d,

$$\begin{array}{lllll} x^{i+1}, & x^{2\Delta+i+1}, & x^{4\Delta+i+1}, & \cdots, & x^{2(t-2)\Delta+i+1}, \\ x^{i+2}, & x^{2\Delta+i+2}, & x^{4\Delta+i+2}, & \cdots, & x^{2(t-2)\Delta+i+2}, \\ \vdots & & & & \\ x^{\Delta+i-1}, & x^{3\Delta+i-1}, & x^{5\Delta+i-1}, & \cdots, & x^{2(t-1)\Delta+i-1}. \end{array}$$

Considering the negatives of these differences, since $-1 = x^{t\Delta}$, we obtain also the group elements

$$\begin{array}{llll} x^{t\Delta+i}, & x^{(t+2)\Delta+i}, & \cdots, & x^{(3t-4)\Delta+i}, \\ x^{t\Delta+i+1}, & x^{(t+2)\Delta+i+1}, & \cdots, & x^{(3t-4)\Delta+i+1}, \\ \vdots & & & \\ x^{(t+1)\Delta+i-1}, & x^{(t+3)\Delta+i-1}, & \cdots, & x^{(3t-1)\Delta+i-1}, \end{array}$$

exponents being reduced modulo $2\Delta t$.

Since the positive differences comprise all elements of the form $x^{l\Delta+i+s}$, where l is even, $s = 0, 1, \cdots, \Delta-1$ and the negative differences comprise all elements of the form $x^{l'\Delta+i+s}$, where l' is odd, $s = 0, 1, \cdots, \Delta-1$, the entire group less the 0 element is replicated exactly once by the differences generated by the resolution class C_d.

Hence the differences between blocks B_i and B_j when considered with respect to $A, Ax, Ax^2, \cdots, Ax^{\Delta-1}$ comprise all of G–$\{0\}$ with multiplicity t.

There are Δ initial blocks B_i to consider and $\binom{\Delta}{2} = \Delta(\Delta-1)/2$ possible distinct pairs. Hence we have the set of difference blocks generating the group GF(p^n)–$\{0\}$

$$\lambda = \frac{\Delta(\Delta-1)}{2}t + \frac{t-1}{2}$$

times. This simplifies to

$$\lambda = \frac{\Delta(t\Delta-1)}{2} = \frac{p^n-3}{4}$$

as desired. The parameters of the design produced by this set of difference blocks are then determined since $|A|$ = block length $k = (p^n-1)/2$ and the variety set is the p^n symbols of GF(p^n).

This then completes the construction.

REFERENCES

[1] HALL, M. JR. (1967). *Combinatorial Theory*. Ginn Blaisdell, New York.

[2] MULLIN, R. C. and STANTON, R. G. (1968). Classification and embedding of BIBD's. *Sankhyā Ser. A* **30** 91–100.

[3] SPROTT, D. A. (1954). A note on balanced incomplete block designs. *Canadian J. Math.* **6** 341–346.