RELATIONS AMONG GENERALIZED HADAMARD MATRICES, RELATIVE DIFFERENCE SETS, AND MAXIMAL LENGTH LINEAR RECURRING SEQUENCES

A. T. BUTSON

1. Introduction. It was established in **(5)** that the existence of a Hadamard matrix of order $4t$ is equivalent to the existence of a symmetrical balanced incomplete block design with parameters $v = 4t - 1$, $k = 2t - 1$, and $\lambda = t - 1$. A block design is completely characterized by its so-called incidence matrix. The existence of a block design with parameters v, k, and λ such that the corresponding incidence matrix is cyclic was shown in **(3)** to be equivalent to the existence of a cyclic difference set with parameters v, k, and λ. For certain values of the parameters, Hadamard matrices, block designs, and difference sets do coexist.

Generalized Hadamard matrices were defined and studied in **(2)**. In this paper it is shown first that the existence of a generalized Hadamard matrix H, containing pth roots of unity where p is a prime, is equivalent to the existence of a matrix E whose elements are in $GF(p)$ and whose "row intersections" satisfy certain restrictions. When $p = 2$, these restrictions are equivalent to requiring that E be the incidence matrix of a symmetrical balanced incomplete block design. Next, the concept of a relative difference set R with parameters m, n, k, and δ is introduced, and the existence of R (when $n + 1 = p$) shown to be equivalent to the existence of a cyclic matrix B whose elements are in $GF(p)$ and whose "row intersections" also satisfy certain restrictions. Then the values of the parameters for which H, R, and B coexist are determined. Next are determined the relations among H, R, and α, a maximal length linear recurring sequence (m-sequence) **(6)**. Using known results concerning the existence of α, the existence of H and R, for certain values of the parameters involved, is established. Finally, some remarks relating R and α to orthogonal arrays are made.

2. Equivalence of H and E. A square matrix H of order h all of whose elements are pth roots of unity is called a *Hadamard matrix* ($H(p, h)$ *matrix*) if $HH^{CT} = hI$. An equivalent requirement is that $H^{CT}H = hI$. When p is a prime, an $H(p, h)$ matrix can exist only for values $h = pt$, where t is a positive integer. A method of constructing $H(p, 2^i p^j)$ matrices for any prime p and any non-negative integers $i \leqq j$ was given in **(2)**. By using the elementary operation of multiplying the elements of a row (or column) by a fixed pth root

Received June 12, 1961.

of unity, it is possible to reduce any $H(p, h)$ matrix to the standard form in which the initial row and column contain only the root 1.

Throughout the remainder of this paper p will denote a fixed prime and H will denote an $H(p, pt)$ matrix in standard form. The matrix obtained by deleting the initial row and column of H will be called the *core* of H and denoted by H_c. Furthermore, it will be assumed that each element of H is expressed in the form γ^x, where γ is a fixed primitive pth root of unity, and $x \in GF(p)$.

Letting $H = (h_{ij})$, $i, j = 0, 1, \ldots, pt - 1$, it is easily seen that the matrix equation $HH^{CT} = ptI$ is equivalent to the following conditions:

$$(2.1)\quad \begin{cases} \gamma^x \text{ occurs exactly } t \text{ times in the row vector } (h_{i0}, h_{i1}, \ldots, h_{i,pt-1}), \\ \text{where } x \in GF(p) \text{ and } i = 1, 2, \ldots, pt - 1; \\ \gamma^x \text{ occurs exactly } t \text{ times in the vector } (h_{i0}h_{j0}^C, h_{i1}h_{j1}^C, \ldots, h_{i,pt-1}h_{j,pt-1}^C), \\ \text{where } x \in GF(p),\ i, j = 1, 2, \ldots, pt - 1, \text{ and } i \neq j. \end{cases}$$

Analogous conditions concerning the columns of H could be stated, but they will not be needed in the sequel.

Now let $\theta(\gamma^x) = x$, for $x \in GF(p)$; and let $E = \theta(H_c) = (\theta(h_{ij}))$, $i, j = 1, 2, \ldots, pt - 1$. Since θ is an isomorphism of the multiplicative group of complex pth roots of unity onto the additive group of $GF(p)$, conditions (2.1) concerning the rows of H are equivalent to the following ones concerning the rows of E:

(2.2)

$$\begin{cases} x \text{ occurs exactly } t \text{ times in row } i,\ x \in GF(p),\ x \neq 0, & i = 1, 2, \ldots, pt - 1; \\ 0 \text{ occurs exactly } t - 1 \text{ times in row } i, & i = 1, 2, \ldots, pt - 1; \\ \sum_{x=0}^{p-1} \lambda_{ij}(x + y, x) = t,\ y \in GF(p),\ y \neq 0, & i, j = 1, 2, \ldots, pt - 1,\ i \neq j; \\ \sum_{x=0}^{p-1} \lambda_{ij}(x, x) = t - 1, & i, j = 1, 2, \ldots, pt - 1,\ i \neq j; \end{cases}$$

where $\lambda_{ij}(x, y)$ is the number of columns of E which contain x in row i and y in row j. Clearly, the following result can now be stated.

THEOREM 2.3. *The existence of H is equivalent to the existence of a matrix E satisfying conditions* (2.2).

When $p = 2$, by noting that t must be even, say $t = 2t_1$, in order that H can exist, it is easy to show that conditions (2.2) are equivalent to requiring that E be the incidence matrix of a symmetrical balanced incomplete block design with parameters $v = 4t_1 - 1$, $k = 2t_1$, and $\lambda = t_1$. When $p > 2$, whether or not a matrix satisfying (2.2) has any significance in the theory of block designs is not known to this author.

3. Equivalence of R and B. Let J_{mn} denote the additive group of integers (mod mn), let $N = \{0, m, 2m, \ldots, (n-1)m\}$, and let $W = \{w: w \in J_{mn}; w \notin N\}$. *A difference set of J_{mn} relative to N* is here defined to be a set $R = \{r_1, r_2, \ldots, r_k\}$ of distinct residues (mod mn) with the following properties:

$$(3.1)\quad \begin{cases} \text{for } w \in W, \text{ there are exactly } \delta \text{ distinct ordered pairs } (r_i, r_j) \text{ of elements} \\ \qquad \text{of } R \text{ such that } r_i - r_j \equiv w (\text{mod } mn); \\ \text{for } w \in N, \text{ there is no pair } (r_i, r_j) \text{ of elements of } R \text{ such that } r_i - r_j \\ \qquad \equiv w (\text{mod } mn). \end{cases}$$

Clearly, the parameters must satisfy $k(k-1) = \delta(mn-n)$. In the sequel, R will be called a relative difference set with parameters m, n, k, and δ. When $n = 1$, R is an ordinary cyclic difference set with parameters m, k, and δ. In general, if D denotes the set obtained by reducing (mod m) the elements of R, it easily follows from (3.1) that D is a cyclic difference set with parameters m, k, and $n\delta$. This result is stated as a theorem.

THEOREM 3.2. *A necessary condition that a relative difference set with parameters m, n, k, and δ exist is that a cyclic difference set with parameters m, k, and $n\delta$ exist.*

From the fact that the complement of a difference set is also a difference set, it follows that the set $Q = \{w: w \in J_m; w \notin D\}$ is a cyclic difference set with parameters m, $m-k$, and $m-2k+n\delta$.

For $j = 0, 1, \ldots, mn-1$, let $R_j = \{r_i + j: r_i \in R\}$, $Q_j = \{q_i + j: q_i \in Q\}$, $S = \bigcup_{j=0}^{n-1} Q_{jm}$, and $S_i = \{s_i + j: s_i \in S\}$; where $r_i + j$, $q_i + j$, and $s_i + j$ are reduced (mod mn). Now each translate R_j is a relative difference set with parameters m, n, k, and δ. Moreover, the collection $\{S_i, R_i, R_{i+m}, \ldots, R_{i+(n-1)m}\}$ is a partition of J_{mn}, $i = 0, 1, \ldots, mn-1$; and the following hold:

$$(3.3)\quad \begin{cases} i \not\equiv j \ (\text{mod } m): & R_i \cap R_j \text{ contains } \delta \text{ elements}, \\ & R_i \cap S_j \text{ contains } k - n\delta \text{ elements}, \\ & S_i \cap S_j \text{ contains } n(m - 2k + n\delta) \text{ elements}; \\ i \equiv j \ (\text{mod } m),\ i \not\equiv j: & R_i \cap R_j \text{ is void}, \\ & R_i \cap S_j \text{ is void}, \\ & S_i \cap S_j \text{ contains } n(m-k) \text{ elements}. \end{cases}$$

Now assume $n + 1 = p$, and let π be a fixed primitive root of p, so that $0, 1, \pi, \pi^2, \ldots, \pi^{p-2}$ are all the elements of $GF(p)$. A matrix $B = (b_{ij})$, $i, j = 0, 1, \ldots, m(p-1)-1$, with elements in $GF(p)$, is now defined. The elements in row i, $i = 0, 1, \ldots, m(p-1)-1$, are determined as follows: for all $j \in S_i$, set $b_{ij} = 0$; for all $j \in R_{i+tm}$, set $b_{ij} = \pi^t$, $t = 0, 1, \ldots, p-2$. This matrix is cyclic and has the following properties:

https://doi.org/10.4153/CJM-1963-005-3 Published online by Cambridge University Press

$$(3.4)\quad \begin{cases} \pi^x \text{ occurs exactly } k \text{ times in each row}, & x = 0, 1, \ldots, p-2, \\ 0 \text{ occurs exactly } (p-1)(m-k) \text{ times in each row}; & \\ i \not\equiv j \pmod m\text{:} \quad \lambda_{ij}(\pi^x, \pi^y) = \delta, & x, y = 0, 1, \ldots, p-2, \\ \qquad\qquad \lambda_{ij}(\pi^x, 0) = k - (p-1)\delta, & x = 0, 1, \ldots, p-2, \\ \qquad\qquad \lambda_{ij}(0, 0) = (p-1)(m-2k+(p-1)\delta); & \\ j - i = tm\text{:} \quad \lambda_{ij}(\pi^{x+t}, \pi^x) = k, & x = 0, 1, \ldots, p-2, \\ \qquad\qquad \lambda_{ij}(\pi^x, 0) = 0, & x = 0, 1, \ldots, p-2, \\ \qquad\qquad \lambda_{ij}(0, 0) = (p-1)(m-k). & \end{cases}$$

It is also noted that

$$(3.5)\quad \pi^t\beta_i = \beta_{i-tm},\ t = 0, 1, \ldots, p-2,\ i = 0, 1, \ldots, (p-1)m-1;$$

where β_i denotes row vector i of B, and $\pi^t\beta_i$ the vector obtained by multiplying each element of β_i by π^t.

Now suppose that B is any cyclic matrix over $GF(p)$ satisfying (3.4) and (3.5). It is obvious that $\{j: b_{0j} = 1\}$ is a relative difference set with parameters m, $p-1$, k, and δ.

THEOREM 3.6. *The existence of a relative difference set R with parameters m, $p-1$, k, and δ is equivalent to the existence of a cyclic matrix B over $GF(p)$ satisfying* (3.4) *and* (3.5).

Although it will not be used in this paper, it should be noted that when $n+1$ is not a prime, the existence of R is equivalent to the existence of a cyclic matrix B' over J_{n+1}. Since in this case it is not possible to express all the elements of J_{n+1} as powers of a fixed primitive root, set $b_{ij}' = 0$ for all $j \in S_i$, and set $b_{ij}' = t+1$ for all $j \in R_{i+tm}$, to obtain the elements in row i of B', $t = 0, 1, \ldots, p-1$, $i = 0, 1, \ldots, nm-1$. This matrix satisfies conditions (3.4) (with π^x replaced by x) but does not satisfy (3.5).

4. Coexistence of R, B, and H. Assume that R is a relative difference set with parameters $m = (p^2\delta - 1)/(p-1)$, $n = p-1$, $k = p\delta$, and δ (m is an integer if and only if δ has the form $(p-1)d+1$, where d is an arbitrary but fixed non-negative integer). Conditions (3.4) for the corresponding matrix B in this case become:

$$(4.1)\quad \begin{cases} \pi^x \text{ occurs exactly } p\delta \text{ times in each row}, & x = 0, 1, \ldots, p-2, \\ 0 \text{ occurs exactly } p\delta - 1 \text{ times in each row}; & \\ i \not\equiv j \pmod m\text{:} \quad \lambda_{ij}(\pi^x, \pi^y) = \delta, & x, y = 0, 1, \ldots, p-2, \\ \qquad\qquad \lambda_{ij}(\pi^x, 0) = \delta, & x = 0, 1, \ldots, p-2 \\ \qquad\qquad \lambda_{ij}(0, 0) = \delta - 1; & \\ j - i = tm\text{:} \quad \lambda_{ij}(\pi^{x+t}, \pi^x) = p\delta, & x = 0\ 1, \ldots, p-2, \\ \qquad\qquad \lambda_{ij}(\pi^x, 0) = 0, & x = 0, 1, \ldots, p-2, \\ \qquad\qquad \lambda_{ij}(0, 0) = p\delta - 1. & \end{cases}$$

It is now an easy matter to verify that the rows of B satisfy conditions (2.2) with $t = p\delta$. Consequently, H exists with $t = p\delta$ and the following properties:

$$(4.2)\quad \begin{cases} H_c \text{ is cyclic;} \\ i \not\equiv j \pmod m : \lambda_{ij}(\gamma^x, \gamma^y) = \delta, \; x, y = 0, 1, \ldots, p-1, \\ \qquad\qquad i, j = 1, 2, \ldots, p^2\delta - 1; \\ (\eta_i)^{\pi^t} = \eta_{i-tm}, \qquad t = 0, 1, \ldots, p-2, \qquad i = 1, 2, \ldots, p^2\delta - 1; \end{cases}$$

where (η_i) denotes row vector i of H, and $(\eta_i)^{\pi^t}$ the vector obtained by raising each element of (η_i) to the power π^t.

Conversely, if, for $t = p\delta$ (where $\delta = (p-1)d + 1$), H exists and satisfies (4.2), then the corresponding matrix E satisfies (3.5) and (4.1); so that R exists with parameters $m = (p^2\delta - 1)/(p-1)$, $n = p - 1$, $k = p\delta$, and δ.

THEOREM 4.3. *A relative difference set R with parameters $m = (p^2\delta - 1)/(p-1)$, $n = p - 1$, $k = p\delta$, and δ; a cyclic matrix B over $GF(p)$ satisfying* (3.5) *and* (4.1)*; and an $H(p, p^2\delta)$ matrix satisfying* (4.2) *coexist.*

It is observed that the trivial relative difference set R with parameters $m = 1$, $n = p - 1$, $k = 1$, and $\delta = 0$, the matrix B whose rows are all the cyclic permutations of the vector $(1, \pi, \pi^2, \ldots, \pi^{p-2})$, and an $H(p, p)$ matrix satisfying (4.2) coexist.

At this point, whether or not any non-trivial relative difference sets ($m > 1$, $n > 1$, $k > 1$, and $\delta > 0$) actually exist remains to be determined. This will be done in the next section.

5. Relations among α, R, and H. Let $f_0, f_1, \ldots, f_u$, with $f_0 f_u \neq 0$, be elements of $GF(p)$. The set $F = F(f_0, f_1, \ldots, f_u)$ of all sequences $\{a_i\}_{i=0}^{\infty}$ with $a_i \in GF(p)$, satisfying

$$f_0 a_i + f_1 a_{i-1} + \ldots + f_u a_{i-u} = 0, \qquad i = u, u+1, \ldots,$$

is called the set of *linear recurring sequences* generated by the $(u+1)$tuple $(f_0, f_1, \ldots, f_u)$. All properties of these sequences used here may be found in **(6)**. It is known that these sequences are periodic with periods not exceeding $r = p^u - 1$; that is, there exists $t \leqq r$ such that $a_{i+t} = a_i$, $i = 0, 1, \ldots$. A sequence with the maximal period r is called an *m-sequence.*

Let $\{a_i\}_{i=0}^{\infty}$ be an m-sequence of period $r = p^u - 1$, and let $\alpha = \{a_i\}_{i=0}^{r-1}$ be its first period. Denote by α_j, $j = 0, 1, \ldots, r-1$, the sequence $\{a_{i-j}\}_{i=0}^{r-1}$, where $i - j$ is reduced (mod r); and let

$$A = \begin{pmatrix} \alpha_0 \\ \alpha_1 \\ \ldots \\ \alpha_{r-1} \end{pmatrix}.$$

Now A is a cyclic matrix, and, by **(6**, Theorem 12**)**, satisfies (4.1) (and consequently (2.2)) with $m = (p^u - 1)/(p-1)$, $n = p - 1$, $k = p^{u-1}$, and

$\delta = p^{u-2}$. By **(6**, Theorem 10**)**, A also satisfies (3.5). By **(6**, Theorem 6**)**, $\alpha_i + \alpha_j$ is either $(0, 0, \ldots, 0)$ or some α_t, $i, j = 0, 1, \ldots, r-1$. Noting that $\alpha_{i-r/2} = -\alpha$, by (3.5), it now follows that there exists an $H(p, p^u)$ matrix whose rows form a group (under the obvious multiplication) and whose core is cyclic. Conversely, the existence of an $H(p, p^u)$ matrix whose rows form a group and whose core is cyclic implies, by **(6**, Theorem 6**)**, the existence of an m-sequence over $GF(p)$ of period $r = p^u - 1$.

THEOREM 5.1. *The existence of an $H(p, p^u)$ matrix whose rows form a group and whose core is cyclic is equivalent to the existence of an m-sequence over $GF(p)$ of period $p^u - 1$.*

THEOREM 5.2. *If an m-sequence over $GF(p)$ of period $p^u - 1$ exists, then there exists a relative difference set with parameters $m = (p^u - 1)/(p - 1)$, $n = p - 1$, $k = p^{u-1}$, and $\delta = p^{u-2}$.*

Since it is known **(6)** that m-sequences over $GF(p)$ of period $p^u - 1$ exist for any prime p and any positive integer u, the following result can be stated.

THEOREM 5.3. *There exist an $H(p, p^u)$ matrix whose rows form a group and whose core is cyclic and a relative difference set with parameters $m = (p^u - 1)/(p - 1)$, $n = p - 1$, $k = p^{u-1}$, and $\delta = p^{u-2}$ for any prime p and any positive integer u.*

When $m = 2^5 - 1$, $n = 1$, $k = 2^4$, and $\delta = 2^3$, there are two non-isomorphic difference sets **(4)**. One is the complement of a projective geometry, and each row of the corresponding matrix B (incidence matrix in this case) is the first period of an m-sequence. The other is the complement of the set of quadratic residues of 31, and no row of the corresponding matrix B is the first period of an m-sequence. This example shows that the converse of Theorem 5.2 is not valid.

6. Remarks. Let B be a matrix satisfying (4.1), and denote row j of B by β_j, $j = 0, 1, \ldots, p^2\delta - 1$. Let B_1 be a matrix whose rows are $\beta_0, \beta_1, \ldots, \beta_{m-1}$, $m = (p^2\delta - 1)/(p - 1)$. Then the matrix B_2, obtained by adjoining an initial column of 0's to B_1, is an orthogonal array of size $p^2\delta$, m constraints, p levels, strength 2, and index δ. The number of constraints is the maximum possible **(1)**, given these values of the other paramaters.

Let A_1 be the matrix whose rows are $\alpha_0, \alpha_1, \ldots, \alpha_{m-1}$, where $m = (p^u - 1)/(p - 1)$, and α is an m-sequence of period $p^u - 1$. The matrix A_2 obtained by adjoining an initial column of 0's to A_1 is an orthogonal array of size p^u, m constraints, p levels, strength s, and index p^{u-s} for any s satisfying $1 \leqq s \leqq u$.

Finally, it is noted that the relative difference set defined and considered in this paper is actually a cyclic relative difference set; and that a relative difference set of an arbitrary group of finite order relative to one of its normal subgroups could be defined.

References

1. R. C. Bose and S. S. Shrikhande, *On the composition of balanced incomplete block designs*, Can. J. Math., *12* (1960), 177–188.
2. A. T. Butson, *Generalized Hadamard matrices*, submitted to Proc. Amer. Math. Soc.
3. S. Chowla and H. J. Ryser, *Combinatorial problems*, Can. J. Math., *2* (1950), 93–99.
4. Marshall Hall, Jr., *A survey of difference sets*, Proc. Amer. Math. Soc., *7* (1956), 975–986.
5. J. A. Todd, *A combinatorial problem*, J. Math. Phys., *12* (1933), 321–333.
6. Neal Zierler, *Linear recurring sequences*, J. Soc. Indust. Appl. Math., *7* (1959), 31–48.

Boeing Airplane Co.