INFORMATION AND CONTROL 15, 196–206 (1969)

Tri-weight Codes and Generalized Hadamard Matrices

P. DELSARTE AND J. M. GOETHALS

MBLE Research Laboratory, Brussels, Belgium

The existence is shown of a set of $(p^m - 1)$ generalized Hadamard matrices $H(p, p^{2m})$ of order p^{2m}, each of which is symmetric and regular. When normalized to become unitary matrices, they form a multiplicative group of order p^m, simply isomorphic to the additive group of $\mathrm{GF}(p^m)$. The rows of these $(p^m - 1)$ matrices are shown to be the image, under the well-known isomorphic mapping relating the pth roots of unity to the elements of $\mathrm{GF}(p)$, of the set of vectors of a given weight in the tri-weight extended-BCH code of length p^{2m}, dimension $3m + 1$, and minimum weight $(p - 1)p^{2m-1} - p^{m-1}$.

LIST OF SYMBOLS

$H(p, h)$	Generalized Hadamard Matrix of order h, over the pth complex roots of unity.
$\mathrm{GF}(q)$	Galois field of q elements.
$T(z)$	The trace of z.
α	A nonzero element of $\mathrm{GF}(q)$.
H_α	The Hadamard matrix corresponding to α.
S	The matrix whose columns are the eigenvectors of H_α.
Δ_α	The diagonal matrix whose elements are the eigenvalues of H_α.
ζ	Primitive complex pth root of unity.
C	Linear code over $\mathrm{GF}(p)$.
$\bar{v}(a_0, a_1, a_2)$	Code vector, corresponding to the parameters a_0, a_1, a_2.
w	Weight of a code vector.
$N(w)$	The number of code vectors of weight w.
A	The incidence matrix of a graph.

1. INTRODUCTION

A square matrix H of order h all of whose elements are complex pth roots of unity is called a *Hadamard matrix* $H(p, h)$ if $HH^* = hI$, where

H^* is the conjugate transpose of H, or in other words, if the matrix $h^{-1/2}H$ is unitary.

Binary Hadamard matrices $H(2, h)$ are known not to exist unless the order h is 2 or a multiple of 4. Although it has been conjectured that $H(2, 4t)$ matrices exist for all integers t, their existence has been established only for a number of specific cases. A survey of results concerning their existence can be found in Hall (1967). Recent improvements were obtained by Goethals and Seidel (1967).

Generalized Hadamard matrices $H(p, h)$ were introduced by Butson (1962) who proved that, when p is a prime, they can only exist for orders $h = pt$. Connections with other combinatorial notions, for instance maximal length recurring sequences (Zierler, 1959), were pointed out by Butson (1963), Shrikhande (1964), Turyn (1967), and Delsarte (1968) among others.

This paper is concerned with the existence of a set of $p^m - 1$ Hadamard matrices $H(p, p^{2m})$ each of which is symmetric and regular.[1] The normalized matrices $p^{-m}H$, together with the unit matrix I, are shown to form a multiplicative group of order p^m, simply isomorphic to the additive group of GF(p^m). Connections with extended-BCH codes of length p^{2m}, dimension $3m + 1$, and minimum weight $(p - 1)p^{2m-1} - p^{m-1}$ over GF(p), are pointed out. Finally, the existence is shown of strongly regular graphs on $v = 2^{3m}$ vertices, whose incidence matrix is constructed by means of the group of $(2^m - 1)$ Hadamard matrices $H(2, 2^{2m})$.

Strongly regular graphs were introduced by Bose (1963). A recent survey of questions concerning their existence and construction was made by Seidel (1968).

The weight distributions of some binary tri-weight codes were studied by Kasami, Lin and Peterson (1967). For a more detailed account of the theory of cyclic codes, see Berlekamp (1968).

For the rest of this paper, p will denote a prime number, and q will stand for p^m.

2. HADAMARD MATRICES $H(p, p^{2m})$

Let T be any linear mapping from GF(q) onto GF(p), for instance *the trace*

[1] The term "regular" is used here with a particular meaning, which arises from graph theory. The incidence matrix of a graph is regular when having a constant row sum. Similarly, a Hadamard matrix having the same property will be said to be regular.

$$T(\alpha) = \sum_{k=0}^{m-1} \alpha^{p^k}. \tag{1}$$

DEFINITION. (Anderson, 1968). By the *T-character* on GF(q) is meant the complex-valued function, defined for the generic element α of GF(q),

$$e(\alpha) = \exp\left(\frac{2\pi i T_\alpha}{p}\right), \tag{2}$$

where T_α is any integer whose residue class modulo p is $T(\alpha)$. It easily follows that

$$e(\alpha + \beta) = e(\alpha)e(\beta), \tag{3}$$

hence proving that e is indeed a character on the additive group of GF(q), that is a homomorphism of the additive group of GF(q) onto the multiplicative group of complex pth roots of unity.

LEMMA 1. *The polynomial* $Z^{q+1} - \alpha$ *has exactly* $(q + 1)$ *distinct roots in* GF(q^2) *when* α *is any nonzero element in* GF(q).

Proof. It is well known that $y^{q-1} - 1$ completely splits into linear factors in GF(q), that is

$$y^{q-1} - 1 = (y - \alpha_1)(y - \alpha_2) \cdots (y - \alpha_{q-1}), \tag{4}$$

where the α_i are the $q - 1$ nonzero elements of GF(q). The same is true for $z^{q^2-1} - 1$ in GF(q^2), and since

$$z^{q^2-1} - 1 = (z^{q+1})^{q-1} - 1, \tag{5}$$

using (4) one deduces

$$z^{q^2-1} - 1 = (z^{q+1} - \alpha_1)(z^{q+1} - \alpha_2) \cdots (z^{q+1} - \alpha_{q-1}). \tag{6}$$

Now, since the left-hand member of (6) completely splits in GF(q^2), the same is true for each factor in the right-hand side, hence proving the result. Q.E.D.

Let α be any nonzero element of GF(q), and let us define a square matrix M_α of order q^2, whose rows and columns are numbered with the elements of GF(q^2). The entry in row x and column y of M_α will be defined as

$$M_\alpha(x, y) = T[\alpha^{-1}(y - x)^{q+1}], \tag{7}$$

where T is the above defined mapping (1).

According to the results of the preceding lemma, one deduces that $(y - x)^{q+1}$ belongs to $GF(q)$ when x and y are any elements of $GF(q^2)$. Thus the elements (7) of M_α belong to $GF(p)$, since T maps $GF(q)$ onto $GF(p)$.

To each nonzero element α of $GF(q)$, let there be attached a square matrix H_α of order q^2, whose entries are the complex pth roots of unity defined by

$$H_\alpha(x, y) = e[\alpha^{-1}(y - x)^{q+1}], \tag{8}$$

where e is the T-character defined in (2).

Let us furter introduce a square matrix S of order q whose entries are

$$S(x, y) = e(xy + x^q y^q), \tag{9}$$

where again e is the T-character (2).

THEOREM 2. *The matrix S is a symmetric Hadamard matrix $H(p, p^{2m})$.*

Proof. Firstly, the entries of S are pth roots of unity, since $xy + (xy)^q$ belongs to $GF(q)$ for xy in $GF(q^2)$, and e maps $GF(q)$ onto the pth roots of unity. Secondly, S obviously is symmetric since, from (9), $S(x, y) = S(y, x)$. Finally, the element $a(x_1, x_2)$ of indices (x_1, x_2) in the matrix product SS^* is easily calculated as

$$a(x_1, x_2) = \sum_{y \in GF(q^2)} e(x_1 y + x_1^q y^q) e(-x_2 y - x_2^q y^q),$$

which, using (3), may be written as

$$a(x_1, x_2) = \sum_{y \in GF(q^2)} e[(x_1 - x_2)y + (x_1 - x_2)^q y^q]. \tag{10}$$

If $x_1 - x_2 = 0$, the above sum reduces to $q^2 e(0)$, that is $a(x_1, x_1) = q^2$, since $e(0) = 1$.

If $x_1 - x_2 \neq 0$, each element of $GF(q)$ appears exactly q times in the expression under brackets, when y runs through $GF(q^2)$, and thus

$$a(x_1, x_2) = q \sum_{\alpha \in GF(q)} e(\alpha),$$

which is known to be zero, since e is a nontrivial character. Q.E.D.

To each nonzero element α of $GF(q)$, let us attach a diagonal matrix Δ_α of order q^2, whose diagonal entries are given by

$$\Delta_\alpha(x, x) = -qe(-\alpha x^{q+1}). \tag{11}$$

THEOREM 3. *The matrix S transforms any matrix H_α into the corresponding diagonal matrix Δ_α, that is*

$$S^{-1}H_\alpha S = \Delta_\alpha .$$

Proof. Let us calculate the element $h_\alpha(x_1, x_2)$ of indices (x_1, x_2) in the matrix product $H_\alpha S$, that is, according to (8) and (9), and using (3),

$$h_\alpha(x_1, x_2) = \sum_{y \in \mathrm{GF}(q^2)} e[\alpha^{-1}(y - x_1)^{q+1} + yx_2 + y^q x_2{}^q].$$

The expression under brackets reduces to

$$\alpha^{-1}z^{q+1} + (x_1x_2 + x_1{}^q x_2{}^q) - \alpha x_2^{q+1}, \tag{12}$$

where $z = y - x_1 + \alpha x_2{}^q$, and thus

$$h_\alpha(x_1, x_2) = e(x_1x_2 + x_1{}^q x_2{}^q)e(-\alpha x_2^{q+1}) \sum_{z \in \mathrm{GF}(q^2)} e(\alpha^{-1}y^{q+1}) \tag{13}$$

Now, according to Lemma 1, z^{q+1} takes $(q + 1)$ times each nonzero value in $\mathrm{GF}(q)$ when z runs through the $q^2 - 1$ nonzero elements of $\mathrm{GF}(q^2)$, and obviously is zero for $z = 0$.

Hence, the sum

$$\sum_{z \in \mathrm{GF}(q^2)} e(\alpha^{-1}z^{q+1}) = (q + 1) \sum_{\alpha \in \mathrm{GF}(q)} e(\alpha) - qe(0), \tag{14}$$

has value $-q$, since e is a nontrivial character, and thus, from (13) and according to (9) and (11),

$$h_\alpha(x_1, x_2) = S(x_1, x_2)\Delta_\alpha(x_2, x_2), \tag{15}$$

hence proving that

$$H_\alpha S = S\Delta_\alpha . \qquad \text{Q.E.D.}$$

THEOREM 4. (i) *The $q - 1$ matrices H_α are symmetric and regular*[1] *Hadamard matrices.*

(ii) *The $(q - 1)$ matrices $-1/q(H_\alpha)$, together with the unit matrix, form a multiplicative group of order q, simply isomorphic to the additive group of* $\mathrm{GF}(q)$.

Proof. From (8), one easily deduces

$$H_\alpha(y, x) = H_\alpha(x, y),$$

hence proving that H_α is symmetric. The sum

$$\sum_{y \in \mathrm{GF}(q^2)} e[\alpha^{-1}(y - x)^{q+1}],$$

of the elements of any row in H_α is easily proved to have value $-q$ using (14), hence proving that H_α is regular.[1]
Now, from Theorem 3, and using the fact that $H_\alpha^* = H_{-\alpha}$, one deduces

$$H_\alpha H_\alpha^* = S\Delta_\alpha\Delta_{-\alpha}S^{-1} = q^2I, \tag{16}$$

hence proving the first part of the theorem, since

$$\Delta_\alpha\Delta_{-\alpha} = q^2I,$$

as it is easily verified.

The second part follows from

$$\Delta_{\alpha_1}\Delta_{\alpha_2} = -q\Delta_{\alpha_1+\alpha_2}, \tag{17}$$

which is easily derived from the definition (11). Indeed, from Theorem 3, this last equation implies

$$\left(-\frac{1}{q}H_{\alpha_1}\right)\left(-\frac{1}{q}H_{\alpha_2}\right) = \left(-\frac{1}{q}H_{\alpha_1+\alpha_2}\right), \tag{18}$$

which proves part (ii) of the theorem. Q.E.D.

3. A CLASS OF TRI-WEIGHT CODES

3.1. Consider the set of polynomials

$$F(a_0, a_1, a_2; y) = a_0 + T[a_1y^{q+1} + a_2y + a_2^qy^q], \tag{19}$$

where a_0, a_1 and a_2 belong, respectively to GF(p), GF(q) and GF(q^2), and where T is the trace (1) from GF(q) to GF(p). Then, the set of vectors

$$\bar{v}(a_0, a_1, a_2) = (v_0, v_1, v_2, \cdots, v_{q^2-1}), \tag{20}$$

where

$$v_i = F(a_0, a_1, a_2; \alpha_i), \qquad \alpha_i \in \text{GF}(q^2), \tag{21}$$

is a linear code C over GF(p), of length $n = q^2$ and dimension $3m + 1$ (Mattson and Solomon (1961), Goethals (1969)).

3.2. Let $a_1 = \alpha^{-1}$, where α is any nonzero element of GF(q), and let a_2 be defined by

$$a_2 = -\alpha^{-1}\beta^q, \tag{22}$$

where β is any element of GF(q^2). Then, if

$$a_0 = T(\alpha^{-1}\beta^{q+1}),$$

the corresponding polynomial (19) can be expressed as

$$F(a_0, a_1, a_2; y) = T[\alpha^{-1}(y - \beta)^{q+1}]. \tag{23}$$

Comparing with (7), one deduces that the corresponding vector

$$\bar{v}(a_0, a_1, a_2),$$

is the row of index β in the matrix M_α. When β runs through $GF(q^2)$ and α through the nonzero elements of $GF(q)$, one obtains $(q - 1)q^2$ vectors (20) of the code C, each of which is a row of some matrix M_α.

Comparing (8) to (7), and using (2), it is easy to see that each element (7) of M_α is the image of the corresponding element (8) of the Hadamard matrix H_α under the well-known isomorphic mapping

$$\zeta^i \to i \pmod p, \quad \zeta \text{ a primitive complex } p\text{th root of unity}, \tag{24}$$

relating the multiplicative group of pth complex roots of unity to the additive group of integers modulo p.

Hence the vectors (20) defined by the set of polynomials (23) can be regarded as the images of the row-vectors of the Hadamard matrices H_α under the mapping (24). The same reasoning will show that the q^2 vectors (20), defined by the set of polynomials (19), with $a_0 = a_1 = 0$, $a_2 = \beta$, that is of the form

$$F(0, 0, \beta; y) = T(\beta y + \beta^q y^q), \tag{25}$$

with β any element of $GF(q^2)$, are the images of the row-vectors of the Hadamard matrix S, (9), under the mapping (24). We thus have the following theorem.

THEOREM 5. *The code C of length p^{2m} and dimension $3m + 1$ over* $GF(p)$, *defined by the set of polynomials* (19), *contains the images, under the well-known isomorphic mapping of the* pth *roots of unity onto* $GF(p)$, *of the row-vectors of a set of p^m Hadamard matrices $H(p, p^{2m})$.*

3.3. The code C contains p^{3m+1} vectors, of which p^{3m} are described in Theorem 5. We shall now prove, in the course of the following theorem, that the remaining $(p - 1)p^{3m}$ vectors are obtained from these by simply adding to each of them the all-one vector multiplied by each of the $(p - 1)$ nonzero elements of $GF(p)$.

THEOREM 6. *The code C is a tri-weight extended-*BCH *code of length p^{2m}, dimension $3m + 1$, and designed distance $(p - 1)p^{2m-1} - p^{m-1}$. Its weight distribution is given in Table 1.*

TABLE 1

WEIGHT-DISTRIBUTION OF CODE C

w	$N(w)$
0	1
$(p-1)p^{2m-1} - p^{m-1}$	$(p-1)(p^m-1)p^{2m}$
$(p-1)p^{2m-1}$	$p(p^{2m}-1)$
$(p-1)(p^{2m-1}+p^{m-1})$	$(p^m-1)p^{2m}$
p^{2m}	$(p-1)$

Proof. The polynomial (19), which can be written as

$$F(a_0, a_1, a_2; y) = a_0 + \sum_{i=0}^{m-1} a_1^{p^i} y^{p^i(p^m+1)} + \sum_{j=0}^{2m-1} a_2^{p^j} y^{p^j}, \quad (26)$$

has degree at most $p^{m-1}(p^m+1)$, and thus cannot have more roots. Consequently, (Mattson and Solomon (1961)), the vector $\bar{v}(a_0, a_1, a_2)$, (20), has weight at least

$$d = p^{2m} - p^{m-1}(p^m+1) = (p-1)p^{2m-1} - p^{m-1}. \quad (27)$$

On the other hand, the only integers u, $1 \leqq u \leqq p^{2m} - 1$, for which the series

$$u, up, up^2, \cdots, up^{2m-1},$$

of integers up^j reduced modulo $p^{2m} - 1$ contains no number greater than $p^{m-1}(p^m+1)$, are $u = 1$ and $u = p^m + 1$, and thus (Mattson and Solomon (1961), Goethals (1967, 1969)) the code C is the extended-BCH code (Berlekamp (1968)) of length p^{2m} and designed distance (27), over GF(p). Consider now the set of vectors (21) of the code C corresponding to the following set of values for a_0, a_1 and a_2:

(i) $a_1 = \alpha^{-1}$, α any nonzero element of GF(q)
a_2 any element of GF(q^2),
$a_0 = T(\alpha^{-1}\beta^{q+1})$, with $\beta = -\alpha a_2^q$.

(ii) $a_0 = a_1 = 0$,
a_2 any nonzero element of GF (q^2).

(iii) $a_0 = a_1 = a_2 = 0$.

Then, according to Theorem 5, the set (i) contains $(p^m - 1)p^{2m}$ vectors each of which is the image of a row-vector of some matrix H_α. Since, from Theorem 4 (i), one has $H_\alpha J = -qJ$, where J is the all-one matrix, one deduces that each row of H_α contains all pth roots of unity, except the element 1, exactly $(p^m + 1)p^{m-1}$ times, and the root 1 exactly $(p^m + 1 - p)p^{m-1}$ times. Since (24) maps 1 onto 0 each vector in (i) has weight $(p - 1)(p^m + 1)p^{m-1}$.

The set (ii) contains $(p^{2m} - 1)$ vectors, each of which is the image of a row-vector of the matrix S, while (iii) only contains the zero vector. These p^{2m} vectors together form the maximum length FSR code, all of whose nonzero vectors have weight $(p - 1)p^{2m-1}$, (Berlekamp (1968)).

It is easily checked that any other vector of the code C is described by a polynomial (26) which only differs by the constant term a_0 from a polynomial in the sets (i), (ii), (iii), hence proving that any other vector is obtained from the preceding ones by adding a fixed multiple of the all-one vector. From the preceding discussion, it clearly appears that:

(1) a set of $(p - 1)(p^m - 1)p^{2m}$ vectors, of weight

$$(p - 1)p^{2m-1} - p^{m-1},$$

is obtained from the set (i),

(2) a further set of $(p - 1)(p^{2m} - 1)$ vectors of weight $(p - 1)p^{m-1}$ from (ii), and

(3) $(p - 1)$ vectors of weight p^{2m} from (iii),

hence proving that C has the weight-distribution given in Table 1.

Q.E.D.

4. A CLASS OF STRONGLY REGULAR GRAPHS

4.1. The adjacency matrix A on an undirected graph without loops and without multiple edges is defined as follows: The diagonal elements A_{ii} are zero, and the off-diagonal entries $A_{ij} = A_{ji}$ are -1 or $+1$ according as the corresponding vertices are adjacent or not. A graph on v vertices is *strongly regular*[2] if and only if there exists integers ρ_0, ρ_1, ρ_2 such that its adjacency matrix A satisfies

$$\begin{aligned}(A - \rho_1 I)(A - \rho_2 I) &= (v - 1 + \rho_1\rho_2)J,\\ AJ &= \rho_0 J,\end{aligned} \tag{28}$$

where J is the all-one matrix, and I the unit matrix.

4.2. Let $p = 2$. Then, according to Theorem 4, there exists, for any m, a set of $2^m - 1$ Hadamard matrices $H(2, 2^{2m})$, each of which is symmetric, regular, and with constant diagonal. Such matrices are involved in various current investigations (see, for instance, Goethals and Seidel (1969)). These $2^m - 1$ matrices H_α, each of which is associated with a

[2] For further details concerning strongly regular graphs, the reader is referred to Bose (1963) and Seidel (1968).

nonzero element α of GF(2^m), furthermore satisfy

$$H_\alpha H_\beta = -qH_\gamma, \quad \text{with} \quad \gamma = \alpha + \beta \quad \text{in} \quad \mathrm{GF}(2^m). \tag{29}$$

On the other hand, from the above properties, one has

$$\begin{aligned} H_\alpha J &= -qJ, \\ H_\alpha^2 &= q^2 I. \end{aligned} \tag{30}$$

Let P_α be the permutation matrix of order 2^m, associated with the element α in the representation of the additive group of GF(2^m) as a regular permutation group of degree 2^m.

THEOREM 7. *The matrix*

$$A = I_q \otimes (I - J) + \sum_{\substack{\alpha \in \mathrm{GF}(q) \\ \alpha \neq 0}} P_\alpha \otimes H_\alpha,$$

is the incidence matrix of a strongly regular graph on $v = q^3$ *vertices. The symbol* $\otimes$ *denotes the Kronecker product,* I_q *is the unit matrix of order* q, I *and* J *are respectively the unit and all-one matrices of order* q^2, *and* $q = 2^m$.

Proof. One easily verifies that A is symmetric, has zero on the diagonal and $+1$ or -1 elsewhere, thus is the incidence matrix of a graph. Now, from the properties (29) and (30), one verifies, by straightforward calculations, that A satisfies:

$$AJ = -(2q^2 - q - 1)J,$$

$$(A - (q + 1)I)(A + (q^2 - q - 1)I) = 2qJ.$$

Hence proving that the graph is strongly regular. Q.E.D.

RECEIVED: April 11, 1969

REFERENCES

ANDERSON, D. R. (1968), A new class of cyclic codes. *Siam J. on Applied Mathematics*. **16**, 181–197.

BERLEKAMP, E. R. (1968), "Algebraic Coding Theory." McGraw-Hill, N.Y.

BOSE, R. C. (1963), strongly regular graphs, partial geometries and partially balanced designs, *Pacific J. Math.* **13**, 389–419.

BUTSON, A. T. (1962), Generalized Hadamard matrices. *Proc. Amer. Math. Soc.* **13**, 894–898.

BUTSON, A. T. (1963), Relations among generalized Hadamard matrices, relative difference sets, and maximal length linear recurring sequences, *Canadian J. Math.* **15**, 42–48.

DELSARTE, P. (1968), Orthogonal matrices over a group and related tactical configurations. Scientific report R90, *MBLE Research Laboratory*, Brussels.

GOETHALS, J. M. (1967), Factorization of cyclic codes, *IEEE Trans. on Information Theory*. **IT-13**, 242–246.

GOETHALS, J. M. (1969), A polynomial approach to linear codes. *Philips Res. Repts.* **24**, 145–158.

GOETHALS, J. M. AND J. J. SEIDEL (1967), Orthogonal matrices with zero diagonal. *Canadian J. Math.* **19**, 1001–1010.

GOETHALS, J. M. AND J. J. SEIDEL (1969), Strongly regular graphs derived from combinatorial designs. *Canadian J. Math.* (to appear).

HALL, M. (1967), "Combinatorial theory." Ginn (Blaisdell), Waltham, Mass.

KASAMI, T., S. LIN AND W. W. PETERSON (1967), Some results on cyclic codes which are invariant under the affine group and their applications. *Inform. Control* **11**, 475–496.

MATTSON, H. F. AND G. SOLOMON (1961), A new treatment of Bose-Chandhuri codes. *J. Siam*, **9**, 654–669.

SEIDEL, J. J. (1968), Strongly regular graphs. *Proc. 3d Waterloo Conf. Combin.* (to appear).

SHRIKHANDE, S. S. (1964), Generalized Hadamard matrices and orthogonal arrays of strength two. *Canadian J. Math.* **16**, 736–740.

TURYN, R. (1968), Sequences with small correlation, *In* "Error-Correcting Codes," Proc. Symposium Univ. Wisconsin (H. B. Mann ed.). J. Wiley, N.Y.

ZIERLER, N. (1959), Linear recurring sequences. *J. Siam* **7**, 31–48.