JOURNAL OF COMBINATORIAL THEORY (A) 16, 313-333 (1974)

Hadamard Matrices, Baumert-Hall Units, Four-Symbol Sequences, Pulse Compression, and Surface Wave Encodings

R. J. TURYN

Raytheon Company, Equipment Division, Sudbury, Massachusetts 01776

Communicated by Marshall Hall, Jr.

Received September 11, 1972

If a Williamson matrix of order $4w$ exists and a special type of design, a set of Baumert-Hall units of order $4t$, exists, then there exists a Hadamard matrix of order $4tw$. A number of special Baumert-Hall sets of units, including an infinite class, are constructed here; these give the densest known classes of Hadamard matrices. The constructions relate to various topics such as pulse compression and image encodings.

1. INTRODUCTION

The main purpose of this paper is the construction of some new Hadamard matrices. The particular approach here is the construction of sets of Baumert-Hall units; these are combinatorial designs first constructed by Baumert and Hall in [1] for $t = 3$. Given a Williamson matrix (an Hadamard matrix of quaternion type) of order h and a set of Baumert-Hall units of order $4t$, an Hadamard matrix of order th can be constructed. The fact that the Paley Hadamard matrices of order $2(q + 1)$, q a prime power $\equiv 1 \pmod 4$, can be put in the quaternion form (see [6]) means that every construction of a set of Baumert-Hall units with t odd constructs $c\pi(n)$ Hadamard matrices of order $\equiv 4 \pmod 8$ and $\leqslant n$, $c > 0$. (If the Baumert-Hall units are of order $4t$, i.e., $4t \times 4t$ matrices, $c = 1/4t$.) The only other known construction of Hadamard matrices which yields as many as $c\pi(n)$ Hadamard matrices is that of Paley for the matrices of order $q + 1$, q a prime power $\equiv -1 \pmod 4$. The constructions presented here depend on theorem 2 which uses a theorem of Goethals and Seidel [2], as well as an idea common in the fields of radar pulse compression and very recent work in surface wave encodings. Briefly, the construction depends on certain quadruples of sequences whose autocorrelation functions (when the sequences are viewed as periodic, i.e., functions on a finite cyclic group) add up to 0. Such quadruples are constructed here by requiring that the non-periodic autocorrelations (i.e., as functions on Z) add up to zero, a more stringent requirement. A number of such quadruples are constructed here, some possible forms are suggested, and one infinite class is presented. Some other Baumert-Hall units are constructed and a composition for them is proved. It seems very probable that there is some construction of Hadamard matrices of all orders $4t$ which is very analogous to the matrices discussed here: Williamson matrices exist of all orders $4t$ for $t \leqslant 31$, $t = 9^s$ and $t = (q+1)/2$, q a prime power $\equiv 1 \pmod 4$. The theorem in [2] removes the necessity for the symmetry of the individual matrices for the construction of an Hadamard matrix; finally, we present here constructions both for the Hadamard matrices and the Baumert-Hall units which depend on various quadruples of commuting ± 1 matrices of order t which satisfy

$$AA' + BB' + CC' + DD' = 4tI, \tag{1}$$

and it seems likely that such quadruples exist for all t, e.g., with A, B, C, D multicirculants.

Pairs of ± 1 sequences (x_i), (y_i) which satisfy

$$c_j(x) + c_j(y) = \sum_{1}^{n-j} (x_i x_{i+j} + y_i y_{i+j}) = 0, \qquad j \not\equiv 0 \pmod n,$$

were discussed in connection with spectrometry and radar pulse compression (see [3] and [5]). Since $c_j(x) + c_{n-j}(x) = a_j(x) = \sum_1^n x_i x_{i+j}$, two ± 1 sequences which satisfy the non-periodic condition $c_j(x) + c_j(y) = 0$ for all $j > 0$ will certainly satisfy the periodic condition $a_j(x) + a_j(y) = \sum_1^n x_i x_{i+j} + y_i y_{i+j} = 0$. (If X is the circulant with first row (x_i), $a_j(x)$ is the $(m, m+j)$ entry of XX' for all m; a similar statement applies to multicirculants.) Quadruples of ± 1 sequences which satisfy

$$c_j(x) + c_j(y) + c_j(z) + c_j(w) = 0$$

had been used by Golay (see [3]) in applications to spectrometry, and n-tuples of sequences which satisfy $\sum_{k=1}^{n} c_j(x^{(k)}) = 0$ have recently been considered in connection with surface wave encodings. It is interesting that the original Golay applications, described in [3], used the sequences for spacial encoding; the more recent ones use the sequences for phase encoding of waveforms. A pair of sequences (x_i), (y_i) which satisfies $\sum_1^m x_i x_{i+j} + y_i y_{i+j} = 0$ for all $j \not\equiv 0 \pmod m$ will yield a quadruple of such sequences of length $m/2$ for $m > 1$. ($\left[\begin{smallmatrix} X & -Y \\ Y' & X' \end{smallmatrix}\right]$ is an Hadamard matrix and thus m is even. The quadruple arises from the odd and even subscript subsequences of x and y; cf. [5] and Lemma 6 below.)

I want to express my gratitude to Dr. L. D. Baumert for many helpful comments.

2. Baumert-Hall Units

Williamson ([9], see also [4]) considered Hadamard matrices of order $4t$ which are constructed by means of a quadruple of symmetric commuting ± 1 matrices of order t which satisfy equation (1) above. (It is only necessary to assume that A, B, C, D satisfy the six equations $XY' = YX'$ but aside from a few examples, two mentioned in [7], all the known examples of such quadruples have A, B, C, D symmetric.) Williamson used symmetric commuting circulants; his construction is $A \times I + B \times i + C \times j + D \times k$, where I, i, j, k are the 4×4 matrices which correspond to the quaternion units. A generalization of this construction which removes symmetry requirements, but not the commutativity condition, was given by Goethals and Seidel in [2], by exhibiting the matrix

$$\begin{matrix} M_1 & M_2R & M_3R & M_4R \\ -M_2R & M_1 & -M_4'R & M_3'R \\ -M_3R & M_4'R & M_1 & -M_2'R \\ -M_4R & -M_3'R & M_2R' & M_1 \end{matrix} \tag{2}$$

where (see [8]) R is a monomial matrix which satisfies

$$R' = R$$

and

$$RM_iR = M_i' \tag{3}$$

$$(\text{or } RM_i = M_i'R).$$

For circulant or multicirculant M_i, R can be taken as the matrix which reverses the order of coordinates. If the M_i are ± 1 matrices and commute, the matrix (2) is Hadamard. This is a generalization of the statement in [2].

The Baumert-Hall units arise from the idea (see [1]) of using quadruples of symmetric A, B, C, D satisfying (1) to form other Hadamard matrices by finding matrices of the form

$$H = A \times e_1 + B \times e_2 + C \times e_3 + D \times e_4 \tag{4}$$

where the e_i are matrices of order $4t$ which are supplementary, in the sense that the entries of the e_k are $0, +1, -1$ and for each pair i, j precisely one of the four is not 0, i.e.,

$$\sum_{k=1}^{4} |(e_k)_{ij}| = 1, \qquad \text{all } i, j,$$

and finally that the matrix H in (3) satisfy

$$HH' = t(A^2 + B^2 + C^2 + D^2)\, I \tag{5}$$

for A, B, C, D symmetric. One such set was constructed in [1] for $t = 3$; since then, a very interesting set was constructed by Welch for $t = 5$. J. Wallis found some for $t = 7, 9, 11$ independently of this paper. If such a set of order $4t$ exists, and a Williamson matrix (A, B, C, D commuting, symmetric) of order n exists, then the matrix in (4) is Hadamard.

THEOREM 1. *e_1, e_2, e_3, e_4 are a set of Baumert-Hall units if and only if they are supplementary and*

$$e_i e_i' = tI,$$
$$e_i e_j' + e_j e_i' = 0, \qquad i \neq j.$$

It follows from these two conditions that the matrices $e_j e_1'/t$ form a quaternion basis. The proof is completely straightforward (see [8]).

The next theorem is the key to the constructions in this paper. To motivate it, the proof being completely elementary, we offer the following comments: We wish to construct a square matrix of order $4t$ whose elements are $\pm A$, $\pm B$, $\pm C$, $\pm D$ and which satisfies (5). The Goethals-Seidel construction (2) suggests that we need only find four circulants of order t whose entries are $\pm A \cdots \pm D$, whose autocorrelation functions add up to zero and which together contain in any row precisely t terms $\pm X$ for $X = A, B, C, D$. The second condition can be satisfied automatically if we think of the four circulants as a sequence of four-dimensional vectors, whose components are $\pm A$, $\pm B$, $\pm C$, $\pm D$, and we require each letter to occur once in each vector. We now restrict ourselves to a subset of eight of these $4! \times 2^4 = 384$ vectors: Let the vector (A, B, C, D) correspond to $Q = A + Bi + Cj + Dk$, where $1, i, j, k$ are the quaternion units, and consider the eight vectors obtained by multiplying Q by one of the eight quaternion units. Thus,

$$\begin{array}{ll} Q : (A, B, C, D) & -Q : (-A, -B, -C, -D) \\ Qi : (-B, A, D, -C) & -Qi : (B, -A, -D, C) \\ Qj : (-C, -D, A, B) & -Qj : (C, D, -A, -B) \\ Qk : (-D, C, -B, A) & -Qk : (D, -C, B, -A) \end{array}$$

It is clear that $Qv_1 \cdot Qv_2 = 0$ if $v_1 \neq \pm v_2$, and $Qv_1 \cdot Q(uv_2) = u(A^2 + B^2 + C^2 + D^2)$ if $u = \pm 1$. For simplicity of notation, we write ± 1 for $\pm Q$, etc.

The preceding discussion (which depends on the Goethals-Seidel construction), immediately suggests Baumert-Hall units of orders 12 and 20: It is clear that the two sequences of vectors

$$1, i, j$$
$$1, i, i, j, -j$$

give rise to two quadruples of sequences (of lengths 3 and 5, respectively) with terms $\pm A$, $\pm B$, $\pm C$, $\pm D$ whose autocorrelation functions add up to zero. Specifically, these are, e.g.,

$$\begin{array}{rrr} A, & -B, & -C \\ B, & A, & -D \\ C, & D, & A \\ D, & -C, & B \end{array}$$

and

$$\begin{array}{rrrrr} A, & -B, & -B, & -C, & C \\ B, & A, & A, & -D, & D \\ C, & D, & D, & A, & -A \\ D, & -C, & -C, & B, & -B \end{array}$$

We summarize the preceding in

LEMMA 1. *If there exists a circulant or multicirculant of order t whose terms are ± 1, $\pm i$, $\pm j$, $\pm k$, subject to the rules $m^2 = 1$, $m \cdot (-m) = -1$ and $mn = 0$ for $m \neq \pm n$ and $a_j = 0$ for $j \neq 0$, then there exists a set of Baumert-Hall units of order $4t$.*

We shall refer to sequences whose terms are $\pm v_j$ where the v_j are any of n orthonormal vectors ($n = 4$ above) as n-symbol sequences. Thus, ordinary binary sequences (terms ± 1) would be called one-symbol sequences.

Quadruples of sequences such as those above must clearly have the property that the sum of the four autocorrelation functions is zero if we replace each of A, B, C, D by $+1$ or -1 (independently); if we replace each of A, B, C, D by $+1$, the eight vectors we use are precisely those four-dimensional vectors with all components ± 1 which have an even number of the components $+1$, or, equivalently, for which the product of the components is $+1$. Replacing one or three of A, B, C, D by -1 would simply require the product to be -1. (This applies to 4-dimensional vectors, i.e., quadruples of sequences. In general, an m-symbol sequence can be realized as a sequence of n-dimensional vectors, with components ± 1, i.e., n sequences, where $n \geqslant m$ and there are m orthogonal vectors with components ± 1 of dimension n. In general, assuming the truth of the Paley conjecture that there are Hadamard matrices of all orders $\equiv 0 \pmod 4$, $n = 4\,[m + 3/4]$ if $m > 2$; $n = 2$ if $m = 2$.)

The preceding motivates the following theorem, whose proof is trivial:

THEOREM 2. *Let* M_1, M_2, M_3, M_4 *be four commuting matrices of order* t *with entries* ± 1 *which are symmetrized by* R (*i.e.*, M_i, R *satisfy* (3)) *which satisfy* (1) *and such that* $\sum_1^4 M_i$ *has all entries* $0, \pm 4$. *Then there exists a set of Baumert-Hall units of order* $4t$.

The construction has been described above. The four matrices e_i are all of the form (2). The explicit formulas are as follows: Let M_i be the four commuting $t \times t$ matrices, and let

$$(\overline{M}_1, \overline{M}_2, \overline{M}_3, \overline{M}_4) = \tfrac{1}{4}(M_1, M_2, M_3, M_4) \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & -1 & -1 & 1 \\ 1 & 1 & -1 & -1 \end{bmatrix}$$

Then (specifying the e_i by the first rows of the form (2))

$$\begin{array}{llllll} e_1: & [\overline{M}_1 & -\overline{M}_2 R & -\overline{M}_3 R & -\overline{M}_4 R] \\ e_2: & [\overline{M}_2 & \overline{M}_1 R & \overline{M}_4 R & -\overline{M}_3 R] \\ e_3: & [\overline{M}_3 & -\overline{M}_4 R & \overline{M}_1 R & \overline{M}_2 R] \\ e_4: & [\overline{M}_4 & \overline{M}_3 R & -\overline{M}_2 R & \overline{M}_1 R] \end{array} \tag{6}$$

are a set of Baumert-Hall units, and the Baumert-Hall matrix is $Ae_1 + Be_2 + Ce_3 + De_4$. It is immediate that the $\overline{M}_i$ have $0, \pm 1$ entries and are supplementary.

3. n-SYMBOL δ CODES

We now turn to the construction of other sets of Baumert-Hall units, based on Theorem 2. Our discussion depends on the elementary properties of various convolution algebras, most often functions defined on Z with values in Z^4 or Z^2; we do not reprove well-known elementary properties.

We shall now define an n-symbol δ code of length m as a sequence V of length m of vectors, each of which is $\pm v_j$, where the v_j are a set of n orthonormal vectors and such that $c_j(V) = 0$ for $j \neq 0$. For $n = 2$ or 4, such a set of vectors can be realized with components ± 1. Thus a 2-symbol δ code corresponds to a pair of binary sequences X and Y such that $c_j(X) + c_j(Y) = 0$ for $j \neq 0$; these were called complementary sequences by Golay. Some properties of such pairs were rediscovered by Welti; all this is discussed in [5]. It is interesting that Welti approached the subject from the point of view of two orthonormal vectors, each corresponding to one of two orthogonal waveforms. Golay and Welti independently proved the theorem (also discovered by the late

Arthur Kohlenberg; as he was then editor of *PGIT*,[1] he would not allow mention of his name in [5]) which states that, if there is a 2-symbol δ code of length m, there is also one of length $2m$. The proof can be stated as follows: If X, Y are the two binary sequences, then $X; Y$ (X followed by Y) and $X; -Y$ will also have the complementary property. We can restate this elegantly by saying that the sequence of length $2m$ is X written in terms of ± 1 followed by Y in terms of $\pm k$ (k a symbol orthogonal to 1). In this paper, we are concerned with δ codes of odd length.

LEMMA 3. *If there is an n-symbol δ code of length m, then there is also an $(n + 1)$-symbol δ code of length $m + 1$.*

This lemma is proved trivially by following the length m code by one new orthogonal symbol. Together with the theorem alluded to above, and the results of the previous section, this gives Baumert-Hall units of all orders $4 \cdot (2^k + 1)$, since 2-symbol δ codes of length 2^k exist for all k. (I do not believe even Hadamard matrices of all these orders were known previously.) We can extend this result. We first make the following definition: If S is a sequence, we will say the sequence T is an orthogonal complement of S if $S^*T = 0$. S^*T is the correlation function: $S^*T(v) = \sum_w S(w)\, T(v + w)$. We are mainly interested in the case of S, T sequences of vectors with all components ± 1, i.e., S, T n-tuples of binary sequences. In the "engineering" literature, orthogonal complements are called "mates" of S.

LEMMA 4. *An n-symbol sequence S (n even) has at least one n-symbol orthogonal complement.*

Arrange the symbols in pairs: (v_1, v_2), (v_3, v_4), etc. To construct T, we first write S backwards, and then interchange the symbols by the monomial permutation which generalizes the quaternion units: $v_{2i-1} \to v_{2i}$, $v_{2i} \to -v_{2i-1}$. It can be verified immediately that T is an orthogonal complement. This gives, in fact, several such (for $n > 2$) since the n symbols can be paired in different ways. It would be interesting to find a family of more than two orthogonal sequences ($S_i * S_j = 0$ for $i \neq j$). In terms of binary (real) sequences, if we have n sequences, n even

$$\begin{matrix} X_1 \\ X_2 \\ \vdots \\ X_n \end{matrix}$$

[1] Professional Group Information Theory.

then an orthogonal complement is

$$\begin{array}{c} -X_2^* \\ X_1^* \\ -X_4^* \\ X_3^* \\ \vdots \\ X_{n-1}^* \end{array}$$

where X^* denotes X backwards: $X^*(w) = X(-w)$. This, of course, yields an orthogonal complement even when S is not an n-symbol sequence, and is a δ code if S is.

Golay proved that, if A, B and X, Y are two pairs of complementary sequences of lengths m_1 and m_2, then $A \times X$; $B \times Y$ and $A \times Y^*$; $-B \times X^*$ are also complementary, of length $2m_1m_2$. We improve on this theorem.

LEMMA 5. *If U is an n-symbol δ code of length m_1, n even and W is a 2-symbol δ code of length m_2, there is an n-symbol δ code of length m_1m_2.*

To prove the lemma, we fix one orthogonal complement of U, say V. We then replace the occurrences of one of the two symbols in W by U, and of the other by V. In terms of binary sequences, e.g., for $n = 2$, if A, B are complementary of length m_1 and X, Y are complementary of length m_2, we have

$$A \times \left(\frac{X+Y}{2}\right) - B^* \times \left(\frac{X-Y}{2}\right), \qquad B \times \left(\frac{X+Y}{2}\right) + A^* \times \left(\frac{X-Y}{2}\right)$$

as the two complementary pairs.

COROLLARY. *There exist complementary binary sequences (two-symbol δ codes) of length $2^a 10^b 26^c$ for all $a, b, c, \geqslant 0$.*

By Lemma 5, we need only exhibit such codes of lengths 2, 10, 26. Using 1 and k as the two orthogonal symbols, we have 1, k of length 2 and

$$1, -1, -1, k, -1, k, -1, -k, -k, k \quad \text{or} \quad 1, k, 1, k, -k, 1, 1, -k, -1, k$$

(Golay, [10])

$$1, 1, 1, -1, -1, 1, 1, 1, -1, 1, -1, -1, k, -1, k, -k, k, -k, -k, k, k, -k, k, k, k, k$$

(Golay [11], also [12]).

The proof of Lemma 5 is suggested by the composition theorems for complex Hadamard matrices [7, 8].

THEOREM 3. *There are three-symbol* δ *codes of all lengths* $2^a 10^b 26^c + 1$ *and, therefore, Baumert-Hall units of orders* $4(2^a 10^b 26^c + 1)$.

This summarizes Lemma 5 and the corollary, in view of Theorem 2. It is interesting that Theorem 3 represents a sort of "bordering" of one Hadamard matrix to get one of size $m + 4$ from one of size m.

Our main interest is in Baumert-Hall units of order $4t$ with t odd. In passing, we mention several constructions with t even. (Theorem 4 was also discovered by Plotkin [18].)

THEOREM 4. *If there are four commuting, symmetrized by R matrices of order t with entries* ± 1 *which satisfy* (1), *then there is a set of Baumert-Hall units of order* $8t$. *If the matrices are circulants of order t whose first rows satisfy* $c_j(A) + c_j(B) + c_j(C) + c_j(D) = 0$, *there are such matrices of order* $2t$ *which form a four-symbol* δ *code.*

The second part of the theorem follows from the quadruple:

$$\begin{array}{l} A;\ \ \ B \\ A; -B \\ C;\ \ \ D \\ C; -D \end{array}$$

((A, C) written in $1, i$ followed by (B, D) written in j, k) for which the product of corresponding elements is clearly 1. The first part follows from the analogous construction

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

which are symmetrized by $\left[\begin{smallmatrix} R & 0 \\ 0 & R \end{smallmatrix}\right]$.

COROLLARY. *There exist Baumert-Hall units of order* $2(q + 1)$ *or* $4(q + 1)$ *if q is a prime power* $\equiv -1$ *or* $+1$ (mod 4), *respectively.*

The four matrices can be taken as circulants if $q \equiv 1$ (mod 4) or 3 (mod 8) and as skew circulants whenever $q \equiv 3$ (mod 4) (see [8]). The construction is not of much interest for Hadamard matrices since, if H is any Hadamard matrix of order $h > 1$, not necessarily of the Williamson type, and q is a prime power, then there are Hadamard matrices of order $(q + 1)\,h$ or $(q + 1/2)\,h$ as $q \equiv 1$ or -1 (mod 4). This follows from the existence of complex Hadamard matrices of order $q + 1$ or $(q + 1)/2$, respectively [8].

THEOREM 5. *For $k = 2, 3, 4$, if there is a k-symbol δ code of length m then m can be expressed as a sum of k squares. In particular, there are no three-symbol codes if $m \equiv -1 \pmod 8$.*

For $k = 2$, this is well known and follows from the identity $(\sum x_i)^2 + (\sum y_i)^2 = 2n + \sum_{j>0} \sum_i (x_i x_{i+j} + y_i y_{i+j})$ so that the non-periodic condition is not necessary. For $k = 3$ or 4, replace the orthogonal vectors by the quaternion vectors with ± 1 components. Then if (x_i), (y_i), (z_i), (w_i) are the four sequences of length m we have

$$\left(\sum x_i\right)^2 + \left(\sum y_i\right)^2 + \left(\sum z_i\right)^2 + \left(\sum w_i\right)^2 = 4m$$

or

$$\left(\sum \frac{x_i + y_i + z_i + w_i}{4}\right)^2 + \left(\sum \frac{x_i - y_i - z_i + w_i}{4}\right)^2 + \left(\sum \frac{x_i - y_i + z_i - w_i}{4}\right)^2 + \sum \left(\frac{x_i + y_i - z_i - w_i}{4}\right)^2 = m.$$

By the definition of a four-symbol code, the terms in parentheses are integers. If we had a three-symbol code, we can assume we do not use the vector (1, 1, 1, 1) in which case two of the four terms x_i, y_i, z_i, w_i are always $+1$, the other two -1, so that $x_i + y_i + z_i + w_i = 0$ for all i. Of course, the conclusion that m is a sum of four squares does not depend on the existence of a δ code. Again, only the periodic conditions $a_j = 0$ are necessary.

We have now produced an infinite number of Baumert-Hall sets. These come from three-symbol codes, and the above theorem shows that there cannot be such codes of orders 7, 15, 23... . We now present some simple theorems and hand computations to produce other sets.

We first produce four-symbol δ codes of length 13. One such is to be found in [3]; it can be verified that the product of corresponding terms of the four binary sequences on p. 471 is -1. The sequence is: $1, i, j, k, 1, 1, -i, 1, -1, -j, j, j, -k$. Another can be derived from the following lemma:

LEMMA 6. *If there is a two-symbol δ code of length $m > 1$, then there is a four-symbol δ code of length $m/2$.*

It is clear that m must be even. It is known that, if $x_n = \pm 1$, then x_{m-n+1} is $\pm k$, where 1 and k are the two orthogonal vectors. (In terms of binary sequences (x_i) and (y_i), we have $x_i x_{m+1-i} y_i y_{m+1-i} = -1$.) This is very easily checked; it does not extend to three-symbol δ codes, as for example in $1, i, j, -i, j$. If we have a two-symbol δ code S, decompose it as

S_o and S_e, the odd index and even index terms. ($S = S_o/S_e$). Then (S_o, S_e^*) is a δ code; the terms are $(\pm 1, \pm k)$ or $(\pm k, \pm 1)$ so that we have four orthogonal vectors and their negatives. The δ code of length 13 derived in this way is: $1, 1, -1, 1, -1, -1, i, i, j, -i, j, i, j$.

The converse of Lemma 6 cannot be true, since there are four-symbol δ codes of length 6.

Because the discussion of the following point is not quite complete in [5], we point out that a two-symbol δ code of length m is equivalent to a pair of complementary binary sequences of length m and implies the existence of a doubled or interleaved two-symbol δ code of length $2m$ where doubled means $1 \cdot X;\ k \cdot Y$ with X, Y binary and interleaved means $1 \cdot X/k \cdot Y$: $1x_1, ky_1, 1x_2, ky_2, \ldots$. A two-symbol δ code of length m is equivalent to a binary sequence of length $2m$ with $c_{2j} = 0$ for all $j > 0$; the sequence corresponds to X/Y with X, Y the two binary sequences.

LEMMA 7. *If X is a binary sequence of odd length m, then $c_{2j-1}(X) = 0$ for all $j > 0$ if and only if, with $X = X_o/X_e$, the odd-length sequence of X_o, X_e is symmetric and the other one skew.*

By symmetric, we mean $y_j = y_{n+1-j}$, and by skew $y_j = -y_{n+1-j}$, where n is the length of the sequence in question. The lemma is known and straightforward (the proof is analogous to part of Theorem 6).

THEOREM 6. *Suppose there are two binary sequences X and Y of length $m+1$ and two of length m, Z and W, such that $c_j(X) + c_j(Y) + c_j(Z) + c_j(W) = 0$ for all $j > 0$. Then there is a four-symbol δ code of length $2m+1$, and*

$$\begin{aligned} x_j x_{m+2-j} &= y_j y_{m+2-j}, \qquad & 2 \leqslant j \leqslant m, \\ z_j z_{m+1-j} &= w_j w_{m+1-j}, \qquad & 1 \leqslant j \leqslant m. \end{aligned}$$

The theorem assumes the existence of a δ code of length $m+1$ in which the vectors are not necessarily orthogonal and all but the last have components ± 1; the last has two components 0.

The four-symbol δ code of length $2m+1$ can be realized as (X, Y) written in ± 1, $\pm i$ followed by (Z, W) written in $\pm j$, $\pm k$; for example, as the quadruple of binary sequences

$$\begin{matrix} X; & Z \\ X; & -Z \\ Y; & W \\ Y; & -W \end{matrix} \qquad \text{or also} \qquad \begin{matrix} X/\ Z \\ X/-Z \\ Y/\ W \\ Y/-W \end{matrix}$$

where it is clear that the product of corresponding terms is 1.

The sequences produced in this way are analogous to the "doubled" sequences mentioned above, in that they are of the form $A; B$ where the symbol sets in A and B are disjoint.

The proof of the second assertion is standard; we use the fact that, if the u_i are all ± 1, then $\sum_1^{2t} u_i = 0$ implies

$$\prod_1^{2t} u_i = (-1)^t.$$

We have the equation for c_j, $1 \leqslant j \leqslant m-1$,

$$\sum_1^{m+1-j} (x_i x_{i+j} + y_i y_{i+j}) + \sum_1^{m-j} (z_i z_{i+j} + w_i w_{i+j}) = 0, \tag{7}$$

which involves $2(2(m-j)+1)$ terms, so that, letting

$$\bar{x}_i = x_i x_{m+2-i} y_i y_{m+2-i}, \qquad \bar{z}_i = z_i z_{m+1-i} w_i w_{m+1-i},$$

we get

$$\prod_1^{m+1-j} \bar{x}_i \prod_1^{m-j} \bar{z}_i = -1, \qquad 1 \leqslant j \leqslant m-1, \tag{8}$$

since (7) involves, e.g., the first and last $m+1-j$ of the x_i. We also have from $x_1 x_{m+1} + y_1 y_{m+1} = 0$ that $\bar{x}_1 = -1$. Multiplying two successive equations (8), and using $\bar{x}_1 = -1$ with (8) for $j = m-1$

$$\bar{x}_{i+1} \bar{z}_i = 1, \qquad 1 \leqslant i \leqslant m-1. \tag{9}$$

Since $\bar{x}_i = \bar{x}_{m+2-i}$, $\bar{z}_i = \bar{z}_{m+1-i}$, we get from (9)

$$\bar{x}_{m+1-j} \bar{z}_{m+1-j} = 1, \qquad 1 \leqslant j \leqslant m-1,$$

or (10)

$$\bar{x}_i \bar{z}_i = 1, \qquad 2 \leqslant i \leqslant m.$$

Comparison of (9) and (10) shows $\bar{z}_1 = \bar{z}_2 = \cdots = \bar{z}_m$, and thus the $\bar{x}_i$ are also equal for $2 \leqslant i \leqslant m$. Finally, we note that, if m is even, $m = 2t$, $\bar{x}_{t+1} = x_{t+1}^2 y_{t+1}^2 = 1$, while, if m is odd, $m = 2t-1$, $\bar{z}_t = z_t^2 w_t^2 = 1$, so that in either case $\bar{z}_i = 1 = \bar{x}_{i+1}$, $1 \leqslant i \leqslant m-1$, the second assertion of the theorem.

COROLLARY. *If there are binary sequences X, Z, W of length m, such that $2c_j(X) + c_j(Z) + c_j(W) = 0$ for all $j > 0$, then there are four-symbol δ codes of length $2m+1$.*

We have the sequences $X; 1$, $X; -1$ of length $m+1$ and Z, W of length m which satisfy the conditions of Theorem 6. This is also an example of

Theorem 4, with $X = A = C$, $Z = B$, $W = D$ followed by one new symbol as in Theorem 3.

THEOREM 7. *Suppose X, Y, Z, W are as in Theorem 6, and that*

(a) for *m even, X is symmetric and Z is skew*;
(b) for *m odd, X is skew and Z is symmetric.*

Then there is a four-symbol δ code of length $4m + 3$ and

(a) *if m is even, $2m + 1$ is a sum of two squares*;
(b) *if m is odd, $2m - 1$ is a sum of two squares.*

Proof. By Lemma 7, the sequence X/Z has $c_j = 0$ for j odd. The required δ code then is X/Z; $iY/jW; k$, where iY denotes the binary sequence Y written in terms of $\pm i$ instead of ± 1. The quadruple of binary sequences is

$$\begin{array}{l} X/Z;\quad Y/W\ \ ;\quad 1 \\ X/Z;\quad Y/-W; -1 \\ X/Z; -Y/-W;\quad 1 \\ X/Z; -Y/W\ \ ; -1 \end{array}$$

The proof of the second part is again a simple application of the sum of squares identity

$$\left(\sum_1^n x_i\right)^2 = \sum x_i^2 + \sum_1^{n-1} (c_j(x) + c_{n-j}(x)).$$

If m is even Z and, by Theorem 6, W are skew so that $z_i + z_{m+1-i} = 0$, and $\sum z_i = \sum w_i = 0$. Therefore,

$$\left(\sum x_i\right)^2 + \left(\sum y_i\right)^2 + \left(\sum z_i\right)^2 + \left(\sum w_i\right)^2 = 2(m + 1) + 2m + \sum 0$$

so that $2(2m + 1) = (\sum x_i)^2 + (\sum y_i)^2$, and therefore $2m + 1$ is a sum of two squares. If m is odd, X is skew and, by Theorem 6, $y_i = -y_{m+2-i}$ for $2 \leqslant i \leqslant m$, so that $\sum x_i = 0$, $\sum y_i = 2y_1$, and we have

$$4 + \left(\sum w_i\right)^2 + \left(\sum z_i\right)^2 = 2(2m + 1),$$

and

$$2(2m - 1) = \left(\sum w_i\right)^2 + \left(\sum z_i\right)^2.$$

Theorems 6 and 7 provide an easy means of calculating four-symbol δ codes of small lengths. The two smallest multiples of 4 for which

Hadamard matrices are not known are $188 = 4.47$ and $236 = 4.59$. A construction of a four-symbol δ code of length 47 by Theorem 7 is impossible since then $m = 11$ and $2m - 1 = 21$ is not a sum of two squares. However, a construction of a four-symbol δ code of length 59 is given below. Construction of quadruples of sequences satisfying the conditions of Theorem 7 is facilitated by the following considerations: We can reverse any of the sequences and multiply any of them by -1. If m is even, we have X symmetric, and $y_1 = -y_{m+1}$, so that $y_2 = y_m$ is equal to either y_1 or y_{m+1}, and we can, by reversing Y if necessary, assume that $x_1 = y_1 = y_2 = z_1 = w_1 = 1$. The same is true if m is odd. Then $c_{m-1} = 0$ shows that $x_2 = 1$. The equations which the sequences must satisfy can be halved in length by using the symmetry relations of Theorem 6, and the reduced equations can be used to extract product relations (as in the proof of Theorem 6) which are not independent, so that some relations are apparent immediately. The remaining conditions can be satisfied by various forms of trial and error, including the appeal to the sum of squares relations. As examples, using the normalizations $x_1 = y_1 = y_2 = z_1 = w_1 = 1$, and $x_2 = 1$ proved above, we have the following examples for small m (note that for $m \leqslant 4$ the constructions are now immediate or almost immediate):

+−	+++	++−−	++−++	+++−−−
++	++−	++−+	++++−	++−+−+
+	+−	+++	++−−	++−++
+	+−	+−+	+−+−	++−++

+++−+++	++−+−+−−
++−−−+−	++++−−−+
++−+−−	+++−+++
++−+−−	+−−+−−+

The above examples construct four-symbol δ codes by Theorem 6 for length $\leqslant 15$ and by Theorem 7 for length $\equiv -1 \pmod 4$ and $\leqslant 31$. Theorem 3 exhibits such codes of lengths 17, 21. We now have different constructions for several lengths, e.g., 11, 15, 27. The Theorem 6 set of length 13 ($m = 6$) is identical to the one derived from the complementary sequence of length 26. The following example gives δ codes of lengths 29 and 59 (by Theorems 6 and 7, respectively). (This gives the first known example of an Hadamard matrix of order $4.59 = 236$.)

++−+++−+−+++−++
+++−++−−−++−++−
++++−−+−++−−−−
+−−−−+−+−++++−

4. Remarks

It seems very likely that four-symbol δ codes of all lengths exist. This would require proof only for odd length. Theorems 6 and 7 suggest some possible forms for such codes. Theorem 7, of course, cannot give examples for all m, as shown by the second part of the theorem. $m = 8$ and 9, lengths 35 and 39, are not ruled out by Theorem 7 but no such codes of those lengths exist; this is very simple to verify using the method of computation described.

The construction of Theorem 6 seems most promising. It can be viewed as finding a complementary pair of two-symbol sequences of lengths m and $m + 1$, respectively, to form a δ code of length $2m + 1$. It is analogous in this sense to Theorem 3, which uses a two-symbol δ code of length n and a length 1 code to form a three-symbol δ code of length $n + 1$. We now consider other possible analogous ways of forming δ codes. As in Theorem 6, we consider two pairs of binary sequences X and Y of length $n > m$ and Z and W of length m, with $p = n - m$ odd, (in Theorem 6, $p = 1$), such that the resulting quadruple has $c_j = 0$ for $j > 0$. As in Theorem 6, we define

$$\bar{x}_i = x_i x_{n+1-i} y_i y_{n+1-i} \,,$$

$$\bar{z}_i = z_i z_{m+1-i} w_i w_{m+1-i} \,,$$

and we note that $\bar{x}_i = \bar{x}_{n+1-i}$, $\bar{z}_i = \bar{z}_{m+1-i}$.

Theorem 8. *If X, Y, Z, W are binary sequences such that $c_j = 0$ for the sequence of four vectors, with X, Y of length n, Z, W of length m, $n - m = p$ odd, $p > 1$, then $m = kp + 1$, $n = (k + 1)p + 1$.*

We remark that, for an arbitrary collection of binary sequences with $c_j = 0$ for all $j > 0$, it is trivial that the number of sequences of each length is even. Other theorems analogous to Theorem 8 can be proved similarly; two pairs and p odd are the only case which interests us here. (In general, adding quadruples of sequences of the same length will not affect the conclusions.)

We have the equations

$$\sum_{1}^{n-j} (x_i x_{i+j} + y_i y_{i+j}) = 0, \qquad m \leqslant j \leqslant n - 1,$$

$$\sum_{1}^{n-j} (x_i x_{i+j} + y_i y_{i+j}) + \sum_{1}^{m-j} (z_i z_{i+j} + w_i w_{i+j}) = 0, \qquad 1 \leqslant j \leqslant m - 1,$$

from which we deduce, as in Theorem 6,

$$\prod_1^{n-j} \bar{x}_i = (-1)^{n-j}, \qquad m \leqslant j \leqslant n-1, \tag{11}$$

$$\prod_1^{n-j} \bar{x}_i \prod_1^{m-j} \bar{z}_i = (-1)^{2(m-j)+p} = -1, \qquad 1 \leqslant j \leqslant m-1. \tag{12}$$

Equation (11) with $j = n - 1$, is

$$\bar{x}_1 = -1$$

and then the product of two successive equations (11) gives

$$\bar{x}_i = -1, \qquad 1 \leqslant i \leqslant n - m = p. \tag{13}$$

(If we disregard z and w, we have derived the condition on two-symbol δ codes alluded to earlier.)

Since we have, e.g., $\prod_1^{n-1} \bar{x}_i = \prod_1^{n-1} x_i y_i \prod_2^n x_j y_j = \bar{x}_1$, we also get from (12)

$$\begin{aligned} \bar{x}_1 \bar{z}_1 &= -1, \\ \bar{x}_{n+1-i}\bar{z}_{m+1-i} = \bar{x}_i \bar{z}_i &= 1, \qquad 2 \leqslant i \leqslant m-1. \end{aligned} \tag{14}$$

However, we get from (12), with $k = m - j$,

$$-1 = \prod_1^{n-j} \bar{x}_i \prod_1^{m-j} \bar{z}_i = \prod_1^{p} \bar{x}_i \prod_{p+1}^{p+k} \bar{x}_i \prod_1^{k} \bar{z}_i, \tag{15}$$

valid for $1 \leqslant k \leqslant m - 1$. Since we have $\bar{x}_i = -1$ for $1 \leqslant i \leqslant p$, $\pi_1{}^p \bar{x}_i = -1$. Thus

$$\bar{x}_{k+p}\bar{z}_k = 1, \qquad 1 \leqslant k \leqslant m-1. \tag{16}$$

We can now see that

$$\begin{aligned} &\bar{z}_{jp+1} = 1, && jp + 1 < m, \\ &\bar{z}_{jp+i} = -1 = \bar{x}_{jp+i}, && (jp + i) < m, 2 \leqslant i \leqslant p, \\ &\bar{x}_{jp+1} = 1, && jp + 1 < m, j > 0. \end{aligned} \tag{17}$$

We have already seen this for $j = 0$ in equations (13) and (14), and we showed $\bar{x}_{p+1} = 1$ above. By induction on j, we have for $1 < jp + i < m-p$

$$\begin{aligned} \bar{z}_{jp+i} &= \bar{z}_{m-jp-i+1} \\ &= \bar{x}_{m-jp-i+1} \qquad \text{by (14)} \\ &= \bar{x}_{n+1-(m-jp-i+1)} = \bar{x}_{(j+1)p+i} \\ &= \bar{z}_{(j+1)p+i} \qquad \text{by (14).} \end{aligned}$$

This proves equations (17). It is now clear that $m \equiv 1 \pmod p$. In fact, if this is not true, let r be the largest integer $\equiv 1 \pmod p$ and less than m. Then $m - r < p$, and (17) shows $\bar{z}_r = 1$, so $\bar{z}_{m-r+1} = 1$. Since $m - r + 1 \leqslant p$, this contradicts (17), proving the theorem.

The theorem actually reveals something of the structure of such sequences (equations (17)). As an example, we have for $p = 3$, $m = 4$, $n = 7$, the quadruples

$$\begin{array}{l} 1\ 1\ -w\ -w\ w\ -1\ 1 \\ 1\ 1\ -w\ -1\ -w\ 1\ -1 \\ 1\ w\ 1\ w \\ 1\ w\ -1\ w \end{array}$$

with $w = \pm 1$.

COROLLARY. *A quadruple of sequences satisfying the conditions of Theorem* 8 *satisfies* $\bar{x}_i = -1$, $i \leqslant p$, *and equations* (17).

Theorem 8 shows that the variety of doubled four-symbol δ codes of length t depends on the factorization of $t - 2$. It seems that the form suggested by Theorem 6 is the most likely form for the doubled codes.

The corollary of Theorem 6 suggests another possible form (quadruples of the form X, X, Y, Z of length t which yield four-symbol δ codes of length $2t + 1$). This is possible only when $4t = 2x^2 + y^2 + z^2$ with x, y, z of the same parity as t, so it is impossible, for example, for $t = 14$. However, it is easy to show that there are no such quadruples of length 6. We use the transformation $A : v_i \to (-1)^i v_i$ applied to the three sequences. This leaves invariant the δ code property (also the four-symbol property). We then see that we must have

$$4t = 2(x_1 + x_2)^2 + (y_1 + y_2)^2 + (z_1 + z_2)^2,$$
$$4t = 2(x_1 - x_2)^2 + (y_1 - y_2)^2 + (z_1 - z_2)^2,$$

where, e.g., x_1, x_2 are the sums of the even subscript and odd subscript terms of X, x_i, y_j, z_i must have the parity of $t/2$ when t is even, or be even and odd in pairs when t is odd. For $t = 6$, it is easy to verify there is no such decomposition.

The transformation A exhibits some interesting forms of δ codes gotten by the method of Theorem 6 from sequences satisfying the conditions of Theorem 7. The transformation will preserve the symmetry of the odd length sequences but will change the skew sequences of even length into symmetric sequences (if the length is n, and the sequence w_i, by symmetry we now mean $w_i = w_{n+1-i}$). The four-symbol code of length $2m + 1$

obtained by the method of Theorem 6 from the four sequences obtained by applying A to the sequences satisfying the conditions of Theorem 7 will then clearly be symmetric about the center of symmetry of the odd length sequences except at the one point corresponding to the end-points of the original two sequences of length $m + 1$. This applies to both of the constructions

$$\begin{array}{ll} X; & Z \\ X; & -Z \\ Y; & W \\ Y; & -W \end{array} \quad \text{and} \quad \begin{array}{ll} X/ & Z \\ X/ & -Z \\ Y/ & W \\ Y/ & -W \end{array}$$

Williamson [9] has shown that a four-symbol δ code cannot be symmetric: if the four binary sequences are symmetric and $x_0 = y_0 = z_0 = w_0 = 1$, then $x_i y_i z_i w_i = -1$ for $i \neq 0$.

By analogy with the theorem for two symbol δ codes, i.e., complementary sequences, we mention that a set of n sequences with $c_j = 0$ is equivalent (by interleaving) to a single sequence with $c_{jn} = 0$. Orthogonal complements translate into sequences whose cross-correlation with the original is 0 at all multiples of n. Finally, much of this has been phrased for functions on Z but is valid for finite Abelian groups. For example, in the next theorem, we need a four-symbol code but $c_j = 0$ can be replaced by correlation zero on a finite Abelian group.

We might also consider the possibility of constructing a four-symbol δ code from more than two pairs of sequences as in Theorems 6 and 8. The four-symbol condition then implies we must restrict ourselves to four sequences X, Y, Z, W of lengths m, m, n, p, respectively, such that the 6-tuple of sequences X, Y, Z, Z, W, W has $c_j = 0$ for $j > 0$, and we ask that $m + n + p$ be odd. It is then easy to verify, proceeding as in Theorem 6, that the only such constructions are those of Theorem 3 for $m < n$ (Z, W complementary, $m = 1$), the construction of the corollary to Theorem 6 ($m = n, p = 1$) or when $m = n, p = m - 1$, which are an example of Theorem 8 ($k = 1$, the four sequences are $Z; W$, $Z; -W$, X, Y). Examples of the last construction are ($m = 4, 6, 8$)

X	$+-+-$	$+-++-+$	$+--+---+$
Y	$+---$	$+++--+$	$+++----+$
Z	$+--+$	$+-+++-$	$+z++--z-$
W	$+++$	$+----$	$+++-+++$

with z either $+1$ or -1.

The statements about the possibilities of constructions are proved as in

Theorem 8. If m, n, p are all > 1, then $c_1 = 0$ shows $\bar{x}_1 = 1$, and thus either $m = n, m > p$ or $n = p, m < n$. In the latter case, we conclude that $\bar{x}_i = -1$ (assuming $m + n + p$ is odd, so $m = 2t + 1$) for $i > 1$ so $\bar{x}_{t+1} = -1$, which is impossible. If $m = n$, $m > p$, we have, as in Theorem 8, that $\bar{x}_i = -1$ for $i < p$, whereas $\bar{x}_i = 1$ for $i \geqslant p$, so $p = m - 1$.

The method of calculation described after Theorem 6 is applicable whenever the reflection coefficients

$$t_i t_{s+1-i}$$

with s the length of the sequence (t_i) are known for each of the four sequences X, Y, Z, W. In that case, we can use Theorem 6 to construct the δ code. To fill the gap $t = 25$ in our examples, the following was derived with a somewhat arbitrarily chosen set of reflection coefficients:

$$\begin{array}{l} ++-+-+++-+-++ \\ +++--------++- \\ ++a-++-++a-- \\ +-a+-+---a+- \end{array}$$

By a construction analogous to Theorem 3, we can prove another composition theorem. Welch has exhibited a very elegant set of Baumert-Hall units of order 20. To exhibit it, let $\bar{N}$ denote the matrix N with the sign of the diagonal changed. We define four circulants by their first rows

$$\begin{aligned} N_1 &= -D, \quad B, -C, -C, -B \\ N_2 &= \quad C, \quad A, -D, -D, -A \\ N_3 &= -B, -A, \quad C, -C, -A \\ N_4 &= \quad A, -B, -D, \quad D, -B \end{aligned}$$

Then the Welch construction is

$$\begin{array}{cccc} N_1 & N_2 & N_3 & N_4 \\ -N_2' & N_1' & -N_4' & N_3' \\ \bar{N}_3' & -\bar{N}_4' & -\bar{N}_1 & \bar{N}_2 \\ \bar{N}_4 & \bar{N}_3 & -\bar{N}_2' & -\bar{N}_1' \end{array}$$

The only point which concerns us here is that we have a four-by-four matrix whose elements are multicirculants (here 5×5 circulants) in $\pm A, \ldots, \pm D$. The matrix is $Ae_1 + Be_2 + Ce_3 + De_4$ with e_i the Baumert-Hall units.

THEOREM 9. *Assume there exists a four-symbol δ code of length t (not necessarily non-periodic; a finite Abelian group of order t is allowable) and* *a Baumert-Hall matrix which is partitioned as a* 4×4 *matrix of* $s \times s$ *multicirculants in* $\pm A, \ldots, \pm D$. *Then there exists a set of Baumert-Hall units of order* $4st$.

If the four-symbol code is defined on the Abelian group G_t and the special Baumert-Hall matrix is $[W_{mn}]$, $1 \leqslant m, n \leqslant 4$, with the W_{mn} defined on the finite Abelian group G_s, we construct four multicirculants X_m on $G_t \times G_s$ as follows: X_m, $1 \leqslant m \leqslant 4$ is defined by substituting in the four-symbol code W_{m1}, W_{m2}, W_{m3}, W_{m4}, for 1, i, j, k, respectively, with 1, i, j, k the four symbols. Then it is clear that the X_i satisfy

$$\sum_{1}^{4} X_i X_i' = ts(A^2 + B^2 + C^2 + D^2)\, I$$

and therefore can be used to form a Baumert-Hall matrix using the construction (2). We need only that the $s \times s$ matrices W_{ij} and their transposes all commute and be symmetrizable by R_s.

We summarize our results:

THEOREM 10. *Four-symbol* δ *codes of length* t *exist for* t *odd when* $t \leqslant 33$, $t = 59$, *and for* $t = 1 + 2^a 10^b 26^c$, $a, b, c, \geqslant 0$. *If a four-symbol* δ *code of length* t *exists, then sets of Baumert-Hall units of orders* $4t$ *and* $20t$ *exist. Thus, Hadamard matrices of orders* $4tw$ *and* $20tw$ *exist with* t *as above and* $w \leqslant 31$, $w = 43$, $w = (q + 1)/2$, q *a prime power* $\equiv 1 \pmod 4$ *and* $w = 9^j$.

Since it depends on some *ad hoc* constructions and on prime powers, the theorem is most effective for small orders. It gives examples (with $w = 1$) of Hadamard matrices of orders 4.59 and 4.101 which, I believe, were previously unknown. The smallest orders not covered by the theorem are 4.47, 4.67, 4.71, 4.73, 4.83, 4.89, 8.47 and 4.103; of these 4.71 and 4.83 are covered by the Paley construction of order $q + 1$, q a prime power $\equiv 3$ (mod 4). The density statement shows there are many new Hadamard matrices constructed.

REFERENCES

1. L. D. BAUMERT AND M. HALL, JR., A new construction for Hadamard matrices, *Bull. Amer. Math. Soc.* **71** (1965), 169–170.
2. J. M. GOETHALS AND J. J. SEIDEL, A skew Hadamard matrix of order 36, *J. Austral. Math. Soc.*, **11** (1970), 343–344.
3. M. J. E. GOLAY, Static multislit spectrometry and its application to the panoramic display of infrared spectra, *J. Opt. Soc. Amer.* **41** (1951), 468–472.

4. M. Hall, Jr., "Combinatorial Theory," Blaisdell, Waltham, Mass., 1967.
5. R. J. Turyn, Ambiguity functions of complementary sequences, *IEEE Trans. Information Theory* **IT-9** (1963), 46–47.
6. R. J. Turyn, An infinite class of Williamson matrices, *J. Combinatorial Theory Sect. A* **12** (1972), 319–321.
7. R. J. Turyn, Complex Hadamard Matrices, "Combinatorial Structures and Their Applications," Gordon and Breach, New York, 1969.
8. R. J. Turyn, Hadamard matrices, algebras and composition theorems, to appear.
9. J. Williamson, Hadamard's determinant theorem and the sum of four squares, *Duke Math. J.* **11** (1944), 65–81.
10. M. J. E. Golay, Complementary series, *IRE Trans. Information Theory* **IT-6** (1960), 400–408.
11. M. J. E. Golay, Note on Complementary Series, *Proc. IRE* **50** (1962), 84.
12. S. Jauregui, Jr., Complementary sequences of length 26, *IRE Trans. Information Theory* **IT-8** (1962), 323.
13. J. B. Kruskal, Golay's complementary series, *IRE Trans. Information Theory* **IT-7** (1961), 273–276.
14. W. D. Squire, H. J. Whitehouse, and J. M. Alsup, Linear signal processing and ultrasonic transversal filters, *IEEE Trans. Microwave Theory and Technol.* **MIT-17** (1969), 1020–1039.
15. Y. Taki, *et al.*, Even-shift orthogonal sequences, *IEEE Trans. Information Theory* **IT-15** (1969), 295–300.
16. C.-C. Tseng, Signal multiplexing in surface-wave delay lines using orthogonal pairs of Golay's complementary sequences, *IEEE Trans. Sonics and Ultrasonics* **SU-18** (1971), 103–107.
17. G. R. Welti, Quaternary codes for pulsed radar, *IRE Trans. Information Theory* **IT-6** (1960), 82–87.
18. M. Plotkin, Decomposition of Hadamard matrices, *J. Combinatorial Theory Sect. A* **13** (1972), 127–130.