SUGGESTED STANDARD FORMS FOR - CERTAIN REAL HADAMARD MATRICES*

Keith W. Henderson

Stanford Linear Accelerator Center Stanford University, Stanford, California 94305

ABSTRACT

Any Hadamard matrix constructed by methods of R.E.A.C. Paley can be converted easily by one or two elementary matrix operations to a form sharing at least four desirable properties with standard forms of Walsh matrices: symmetry, zero trace, normal form, and the same number of 1's as -1's in every row and column except the <u>O</u>th row and Oth column.

The matrices thus converted are suggested as tentative standard forms for engineering purposes.

This report, prepared especially for publication in the <u>IEEE</u> <u>Transactions on Computers</u>, is largely a summary of the author's much more detailed SLAC-PUB-1740.

*Work supported by the Energy Research and Development Administration.

I. INTRODUCTION

For engineering purposes three standard forms of the Walsh matrix W (of order 2^{ν} , where ν is a positive integer) have been proposed [1] and are widely used.

Although known forms of the more general Hadamard matrix H (of order $4\mu \neq 2^{\nu}$, where μ is a positive integer) have been classified as being symmetric or skew-symmetric, or as having a constant principal diagonal [8], no standard form of H for engineering purposes has yet been proposed.

Paley established and tabulated methods for constructing H (he called it U) of all orders up to 200 except six then unknown orders 92, 116, 156, 172, 184, and 188, all of which have since then been discovered and constructed by other methods [2-4,7].

The author has shown elsewhere [5] that each Paley matrix can be converted easily by one or two elementary matrix operations to a form that shares at least the following four properties with the standard forms of W:

- 1. It is symmetric.
- 2. Its trace is zero (i.e., it has the same number of 1's as -1's on its principal diagonal).
- It is of normal form (i.e., all elements in its <u>0</u>th row and <u>0</u>th column are
 1).
- 4. It has the same number of 1's as -1's in every row and every column except the 0th row and 0th column.

Although not trivial, property 4 is superfluous in the sense that it is a direct consequence of property 3 and the orthogonality of the matrix.

Adoption of this form as a tentative standard for engineering purposes

- 2 -

would widen the applicability of (non-Walsh) Hadamard matrices to practical problems, unify their notation, and simplify communication among engineers using them.

II. EXAMPLES

Of the four properties listed, Paley's illustrative matrix A of order 12 (Fig. 1) possesses only 3 and 4. However, the submatrix obtained by deleting the <u>0</u>th row and <u>0</u>th column is symmetric with respect to its own secondary diagonal, and the number of -1's on this secondary diagonal is just one greater than the number of 1's. Consequently, since all elements in the <u>0</u>th row and <u>0</u>th column of A are 1, then if the sequence of all the rows (columns) of A except the <u>0</u>th row (column) is reversed, the resulting matrix will also be symmetric with zero trace, and will thus possess all four properties.

This matrix was constructed by Paley's lemma 2, with

$$m = 4\mu = p+1 ; \mu = 3, p = 11 \cong 3 \pmod{4}$$
, (1)

where p denotes a prime number. But neither the matrix nor the method is unique. Other matrices of the same order can be constructed by Paley's lemma 3, with

$$m = 4\mu = 2(p+1)$$
; $\mu = 3$, $p = 5 \cong 1 \pmod{4}$, (2)

first constructing an orthogonal, but non-Hadamard, B matrix of order 6 (Fig. 2), then making the substitutions

$$\begin{bmatrix} + \end{bmatrix} \rightarrow \begin{bmatrix} + & + \\ + & - \end{bmatrix}; \begin{bmatrix} - \end{bmatrix} \rightarrow \begin{bmatrix} - & - \\ - & + \end{bmatrix}; \begin{bmatrix} 0 \end{bmatrix} \rightarrow \begin{bmatrix} + & - \\ - & - \end{bmatrix}$$
(3)

to obtain a Hadamard matrix H of order 12. Here B, unlike A in the preceding example, is already symmetric, and the submatrix obtained by deleting its <u>0</u>th row and <u>0</u>th column is doubly symmetric, so we have the two options of either making the substitutions directly in B, or else first reversing the sequence of all but the <u>0</u>th row and <u>0</u>th column and then making the substitutions. In either case the substitution for 0 in $B_{0,0}$ makes $H_{0,1} = H_{1,0} = -1$, so it is necessary to multiply the <u>1</u>th row and <u>1</u>th column of H by -1 to normalize it. Whichever option is chosen, the resulting matrix H will possess all four properties.

_	_	_	-	_			_			_	
+	+	+	+	+	+	+	+	+	+	÷	+
+	-	+		+	+	+	-	-	-	+	-
+	-	-	+		+	+	+	-	-	-	+
+	+	_		+	_	+	+	+	-	-	-
+	-	+		-	+	-	+	+	+	-	-
+	-	-	+	-	-	+	-	+	+	+	-
+	-	_		+		-	+	-	+	+	+
+	+	-	-	-	÷	-		+	-	+	+
+	+	+		-	-	+	-	-	+	-	+
+	+	÷	+	_	_	-	+		-	+	
+	-	+	+	+		-	-	+	-	-	+
+	+	-	+	+	÷	-	-	-	÷	-	-

Fig. 1--Paley A matrix of order 12, and submatrix obtained by deleting <u>0th</u> row and 0th column.

0	+	+	+	+	+
+	0	+		-	+
+	+	0	+	-	-
+	-	+	0	+	-
+	-	~	+	0	+
+	+	-	-	+	0

Fig. 2--Paley B matrix of order 6, and submatrix obtained by deleting <u>0</u>th row and 0th column.

III. STANDARD FORMS

As implied in Section I, the author has proved rigorously [5] that the possibility of so modifying the Paley matrices to obtain forms possessing all four desirable properties is quite general. The rules for doing so are quite simple: 1. If $p \cong 3 \pmod{4}$ or $p^h \cong 3 \pmod{4}$, where h is a positive integer,

a. construct a Paley A matrix using Paley's lemma 2 or 4 respectively;

b. reverse the sequence of all but the 0th row (column).

2. If $p \cong 1 \pmod{4}$ or $p^h \cong 1 \pmod{4}$,

- a. construct a Paley B matrix using Paley's lemma 3 or a combination of
 3 and 4 respectively;
- b. reverse the sequence of all but the 0th row (column) or not, as desired;
- c. make the substitutions (3);

d. multiply the 1th row and 1th column of the resulting matrix by -1.

Of course, it is not necessary to actually construct the Paley matrix and then reverse the rows (columns). In either case steps a and b can be merged into a single step and the desired matrix constructed more directly, either by suitably relabeling the row (column) index in Paley's element formulas, except for the <u>Oth</u> row (column), or by simply reversing the numbering of all but the Oth row (column).

The now well-known Kronecker product (Paley's lemma 1) can be used to obtain matrices of orders that are powers-of-2 times that of a matrix constructed by these rules, and it is sometimes necessary.

The resulting matrices are not necessarily unique, in either method of construction or form, and, unlike the Walsh matrices widely used by engineers, are not all neatly related by Kronecker products and/or permutations of rows (columns). For example, Paley matrices of order 24 can be constructed in three distinct ways, using his:

1. lemma 2, since

24 = 23 + 1 and $23 \cong 3 \pmod{4}$;

2. lemmas 2 and 1 (in that order), since

 $24 = [11 + 1] \times 2 \text{ and } 11 \cong 3 \pmod{4};$

3. lemmas 3 and 1 (in that order), since

 $24 = [2(5+1)] \times 2 \text{ and } 5 \cong 1 \pmod{4};$

where p+1 implies direct construction of an A matrix, 2(p+1) implies construction of a B matrix and the substitutions (3), and $[\ldots] \times 2^k$ implies a Kronecker product of order 2^k . Thus, there are four possible standard forms of order 24, one each for cases 1 and 2, and two for case 3 according as the row (column) sequence of B is or is not reversed before the substitutions (3).

IV. EQUIVALENCE CLASSES

Hadamard matrices of the same order but different constructions that cannot be converted one into another by negating and/or permuting rows and/or columns are said to be Hadamard-inequivalent, and to belong to different equivalence classes [9]. The number of classes for each order of Hadamard (including Walsh) matrix is a complicated subject not within the scope of the research reported herein.

Although there are many equivalence classes for higher orders of Walsh matrices as well as for the more general Paley and other Hadamard matrices, all three standard forms of the Walsh matrix of any order [1] belong to the same equivalence class, and in general engineers have not been concerned about the existence or possible utility of others.

Which class or classes of the suggested standard forms engineers will prefer will depend upon experience in their application and the discovery and dissemination of other useful properties. (For example, it can be shown that the submatrix obtained by deleting the <u>0</u>th row and <u>0</u>th column of the A matrix constructed by Paley's lemma 2, as in Fig. 2, is always circulant, and consequently that that of the resulting standard matrix will always be back-circulant.)

V. NOTATION

Experience in practical applications will lead to different ideas for notation. Whatever symbol is used to denote the modified Paley matrix, say P, a particular matrix can be indicated conveniently and unambiguously by a double subscript, of which the first numeral specifies the order and the second the prime number used in the construction, with a tilde (or other mark) over the latter to indicate row (column) sequence reversal of the submatrix. For example,

- 6 -

 $P_{24,23}$, $P_{24,11}$, $P_{24,5}$, and $P_{24,5}$ suffice to distinguish among the four possible standard forms of order 24.

In these matrices the individual functions (rows) are not neatly identifiable by sequency as are those in the Walsh matrices. However, a particular function can be indicated conveniently and unambiguously by the same double subscript as the matrix, plus a single or double argument specifying the row or row and column respectively. For example, pal_{24} , 23(i) or pal_{24} , 23(i, j) suffices to distinguish among the rows or the rows and columns of P_{24} , 23.

As suggested in [1], pal and Pal can be used to distinguish between continuous and discrete functions.

VI. SUMMARY AND CONCLUSIONS

Any Hadamard matrix obtained by Paley's lemmas 1 to 4 can be converted easily to one possessing the four desirable properties listed in Section I, which it then shares with the three standard forms of Walsh matrix defined and illustrated in [1].

Although the more general Hadamard matrices (of order $4\mu \neq 2^{\nu}$) differ markedly from the Walsh matrices in other properties, use of the standard forms suggested herein for engineering purposes will encourage a more widespread and uniform practical application of them, and facilitate a clearer understanding of them.

It is not yet known whether the non-Paley type matrices [2-4, 7] can be converted into a form possessing all four desirable properties.

REFERENCES

- N. Ahmed, H. H. Schreiber, and P. V. Lopresti, "On notations and definitions of terms related to a class of complete orthogonal functions," IEEE Transactions on Electromagnetic Compatibility, Vol. EMC-15, pp. 75-80; May 1973.
- 2. L. D. Baumert, "Hadamard Matrices of Orders 116 and 232," Bulletin of American Mathematical Society, Vol. 72, p. 237; 1966.
- 3. L. D. Baumert and M. Hall, Jr., "Hadamard Matrices of the Williamson Type," Mathematics of Computation, Vol. XIX, pp. 442-447; 1965.
- 4. S. W. Golomb and L. D. Baumert, "The Search for Hadamard Matrices," American Mathematical Monthly, Vol. 70, pp. 12-17; January 1963.
- 5. K. W. Henderson, "Tentative Standard Forms for Real Hadamard Matrices," Stanford Linear Accelerator Center, Stanford University, Stanford, California, SLAC-PUB-1740, April 1976. (Single copies available at no charge upon request to Publications Dept., SLAC, P.O. Box 4349, Stanford, CA 94305. This reference includes some tutorial background for engineers not well acquainted with residue and Galois theory.)
- R.E.A.C. Paley, "On Orthogonal Matrices," Journal of Mathematics and Physics, Vol. 12, pp. 313-320; 1933.
- R. J. Turyn, "Hadamard Matrices, Baumert-Hall Units, Four-Symbol Sequences, Pulse Compression, and Surface Wave Encodings," Journal of Combinatorial Theory, Vol. 16, pp. 313-333; 1974.
- J. S. Wallis, "Hadamard Matrices," in Lecture Notes in Mathematics, A. Dold and B. Eckmann, eds., Vol. 292, <u>Combinatorics: Room Squares</u>, <u>Sum-Free Sets, Hadamard Matrices</u>, Part 4, Appendices A, B, D, E, and H; Springer-Verlag, Berlin/Heidelberg/New York, 1972.
- 9. Ibid., Part 4, Chapter X.