ERRATA TO SLAC-PUB-1740 Rev.

p. 20: In the third column of the second line of the heading the label should be "$m = f[2(p+1)]$". See heading on p. 19.

p. 20: In the last column of the second line of the heading the label should be "$m = f[2(p^h+1)]$". See heading on p. 19.

p. 20: In the third line of the heading the congruency sign "$\cong$" has been omitted. See heading on p. 19.

p. 22: The sentence should read "...to perform this research."

SLAC-PUB-1740
April 1976
Revised January 1978

TENTATIVE STANDARD FORMS FOR REAL HADAMARD MATRICES*

Keith W. Henderson
Stanford Linear Accelerator Center
Stanford University, Stanford, California 94305

ABSTRACT

Any non-Walsh Hadamard matrix obtained by methods of R. E. A. C. Paley, including all but six orders less than 200, plus infinitely many higher orders, can be converted easily to one sharing at least for desirable properties with standard forms of Walsh matrices: symmetry, the same number of 1's as -1's on the principal diagonal (zero trace), all 1's in the 0th row and 0th column (normal form), and the same number of 1's as -1's in every row and column except the 0th row and 0th column.

To widen the applicability of (non-Walsh) Hadamard matrices to practical problems, unify their notation, simplify communication among engineers using them, and promote further research, the matrices thus converted are proposed as tentative standard forms for engineering purposes, comparable to standard forms of Walsh matrices.

*Work supported by the Department of Energy.

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 [26], no standard form of H for engineering purposes has yet been proposed.

Paley established and tabulated methods for constructing H of all orders less than or equal to 200, except six then unknown orders (92,116,156,172, 184 and 188) [14], all of which have since been discovered and constructed by other methods [4,5,9,22].

We can show that each Paley matrix H either is already of a form, or simply by one or two elementary matrix operations can be converted to a form, that shares at least the following four properties with the standard forms of W:

1. H is symmetric.
2. It has the same number of 1's as -1's on its principal diagonal (and consequently zero trace).
3. All elements in its 0th row and 0th column are 1 (and thus it is of so-called normal form [2]).
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.

Adoption of this form as a tentative standard for engineering purposes would widen the applicability of (non-Walsh) Hadamard matrices to practical problems, unify their notation, simplify communication among engineers using

them, and promote further research.

Of the four properties listed, Paley's illustrative matrices of order 12 (Fig. 1) and 28 [16] possess only 3 and 4. In either case, however, the submatrix obtained by deleting the 0th row and 0th column of the complete matrix 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 0th row and 0th column of the complete matrix are 1, if the sequence of all the rows (columns) of the complete matrix except the 0th row (column) is reversed, the resulting matrix (Fig. 2) possesses all four properties.

Thus our task is to demonstrate the generality of these features of the Paley matrices, and to examine its ramifications.

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. Therefore it will be sufficient herein to show that the modified Paley matrix possesses properties 1 to 3.

+	+	+	+	+	+	+	+	+	+	+	+
+	-	+	-	+	+	+	-	-	-	+	-
+	-	-	+	-	+	+	+	-	-	-	+
+	+	-	-	+	-	+	+	+	-	-	-
+	-	+	-	-	+	-	+	+	+	-	-
+	-	-	+	-	-	+	-	+	+	+	-
+	-	-	-	+	-	-	+	-	+	+	+
+	+	-	-	-	+	-	-	+	-	+	+
+	+	+	-	-	-	+	-	-	+	-	+
+	+	+	+	-	-	-	+	-	-	+	-
+	-	+	+	+	-	-	-	+	-	-	+
+	+	-	+	+	+	-	-	-	+	-	-

Fig. 1--Paley matrix of order 12, showing submatrix obtained by deleting 0th row and 0th column.

+	+	+	+	+	+	+	+	+	+	+	+
+	-	+	-	-	-	+	+	+	-	+	-
+	+	-	-	-	+	+	+	-	+	-	-
+	-	-	-	+	+	+	-	+	-	-	+
+	-	-	+	+	+	-	+	-	-	+	-
+	-	+	+	+	-	+	-	-	+	-	-
+	+	+	+	-	+	-	-	+	-	-	-
+	+	+	-	+	-	-	+	-	-	-	+
+	+	-	+	-	-	+	-	-	-	+	+
+	-	+	-	-	+	-	-	-	+	+	+
+	+	-	-	+	-	-	-	+	+	+	-
+	-	-	+	-	-	-	+	+	+	-	+

Fig. 2--Matrix obtained by reversing sequence of all rows (columns) except 0th row (column).

II. NOTATION

To avoid confusion we shall employ Paley's notation insofar as feasible. However, it will not suffice to refer merely to his U-matrix, because we shall alter it by means of elementary matrix operations and matrix products, and we shall also refer often to the submatrix discussed in Section I. To distinguish clearly among the different forms, let:

- A and B denote Paley matrices, $A_{i,j}$ and $B_{i,j}$ their respective elements, and A' and B' the submatrices obtained by deleting the 0th row and 0th column of A and B respectively;
- $\overline{A}$ and $\overline{B}$ denote new matrices obtained by reversing the sequence of all but the 0th row (column) of A and B respectively, and $\overline{A}_{i,j}$ and $\overline{B}_{i,j}$ their respective elements;
- $\overline{\overline{A}}$ denote another new matrix obtained by multiplying the 1th row and 1th column of $\overline{A}$ by -1;
- $\hat{A}$ denote either A or $\overline{A}$ where it is not necessary to distinguish between them because of specified common properties, and $\hat{A}_{i,j}$ its elements;
- $\hat{\hat{A}}$ denote a new matrix obtained by multiplying the 1th row and 1th column of $\hat{A}$ by -1;
- $\widetilde{A}$ denote a new matrix obtained as a Kronecker product of a Walsh matrix W and $\overline{A}$, and $\widetilde{\overline{A}}$ another new matrix obtained as a Kronecker product of a Walsh matrix W and either $\overline{\overline{A}}$ or $\hat{\hat{A}}$.

Other notation herein will be either identically the same as Paley's or else clearly defined in the text.

III. PALEY'S LEMMA 1

Paley's lemma 1 is simply a demonstration of the now well-known Kronecker product [3,11,19,27], also called direct product [19] and tensor product [10], and of the construction of Walsh matrices of all orders. For our purpose herein it is not of interest by itself, but it can be used in combination with his lemmas 2 to 4 to generate (non-Walsh) Hadamard matrices of higher orders.

IV. PALEY'S LEMMA 2

In this case

$$m = 4\mu = p + 1 ; \qquad p \cong 3 (\text{mod } 4) \tag{1}$$

where p is any prime number satisfying the constraint, in which the congruency symbol implies that the remainder of p/4 is 3.

The elements of Paley's matrix A are

$$A_{i,0} = A_{0,j} = 1 ; \quad 0 \leq i \leq p, \quad 0 \leq j \leq p \tag{2}$$

$$A_{i,j} = \chi(j-i) ; \quad 1 \leq i \leq p, \quad 1 \leq j \leq p, \quad i \neq j \tag{3}$$

$$A_{i,i} = -1 ; \quad 1 \leq i \leq p \tag{4}$$

where χ denotes the Legendre symbol [12,24]:

$$\chi(j-i) = \frac{j-i}{p} = \begin{Bmatrix} 1 \\ -1 \end{Bmatrix} \text{ if } j-i \text{ is a quadratic } \begin{Bmatrix} \text{residue} \\ \text{nonresidue} \end{Bmatrix} \text{ of } p$$

$$= \begin{Bmatrix} 1 \\ -1 \end{Bmatrix} \text{ if } (j-i)^{\frac{\phi(p)}{2}} \begin{Bmatrix} \cong \\ \ncong \end{Bmatrix} 1 (\text{mod } p) \tag{5}$$

where $\phi(p)$ is the Euler totient function [23].

Although A possesses property 3 of Section I by (2), it does not possess property 2, since by (2) and (4) all elements on the principal diagonal except $A_{0,0}$ are identical.

Nor does it possess property 1, for we can show easily that A is not symmetric. It is well-known [25,28] that if

$$p \cong 3 \pmod 4 \tag{6}$$

as specified by (1), then

$$\chi[-f(p)] = -\chi[f(p)] \tag{7}$$

where f(p) denotes simply the argument of χ in functional form. In the submatrix A' (defined in Section II) the element symmetrically opposite $A_{i,j}$ with respect to the principal diagonal of A' (and of A) is $A_{j,i}$. By (3) and (7),

$$A_{j,i} = \chi(i-j) = \chi[-(j-i)] = -\chi(j-i) = -A_{i,j} \tag{8}$$

Thus A' is skew-symmetric, and consequently A is not symmetric.

However, in A the element symmetrically opposite $A_{i,j}$ with respect to the secondary diagonal of A is $A_{p-j,p-i}$. In A' the element symmetrically opposite $A_{i,j}$ with respect to the secondary diagonal of A' must be one row below and one column to the right of $A_{p-j,p-i}$, and is therefore $A_{p-j+1,p-i+1}$. By (3) and (7),

$$A_{p-j+1,p-i+1} = \chi[(p-i+1) - (p-j+1)] = \chi(j-i) = A_{i,j} \tag{9}$$

Thus A' is symmetric with respect to its own secondary diagonal. Consequently if the sequence of all but the 0th row (column) of A is reversed, the new matrix $\bar{A}$ is symmetric with respect to its principal diagonal, and thereby possesses property 1.

The elements on the secondary diagonal of A' are $A_{i,p+1-i}$. By (3),

$$A_{i,p+1-i} = \chi[(p+1-i) - i] \tag{10}$$

Since the order of A is p+1, that of A' is p. Since p, a prime number, is always odd, so is the number of elements on the secondary diagonal of A', one of which must be also on the principal diagonal of A. With this one exception,

then, for every element defined by (10), there is another element $A_{p+1-i,i}$ (i.e., one with the row and column indices simply interchanged). By (3), (7), and (10),

$$A_{p+1-i,i} = \chi[i - (p+1-i)] = -\chi[(p+1-i) - i] = -A_{i,p+1-i} . \tag{11}$$

By the foregoing reasoning and (4), the excepted element is

$$A_{\frac{p+1}{2},\frac{p+1}{2}} = -1 \tag{12}$$

Thus the number of -1's on the secondary diagonal of A' is just one greater than the number of 1's. But by (2),

$$A_{0,0} = 1 \tag{13}$$

Consequently if the sequence of all but the 0th row (column) of A is reversed, the new matrix $\overline{A}$ has the same number of 1's as -1's on its principal diagonal, and thereby possesses property 2.

Finally, by (2), all elements in the 0th row and 0th column of A are 1. Reversing the sequence of all but the 0th row (column) of A alters neither its 0th row nor 0th column. Consequently the new matrix $\overline{A}$ is of normal form, and thereby possesses property 3.

V. PALEY'S LEMMA 3

In this case

$$m = 4\mu = 2^k(p+1) ; \; k = 1 , \; p \cong 1 (\mathrm{mod}\ 4) \tag{14}$$

where k is (in general) a positive integer, and p is any prime number satisfying the constraint, in which the congruency symbol implies that the remainder of p/4 is 1.

Paley first obtains a matrix B of order p+1, whose elements (corresponding to, but not exactly the same as, (2) - (4)) are

$$B_{i,0} = B_{0,j} = 1;\ 1 \le i \le p,\ 1 \le j \le p \tag{15}$$

$$B_{i,j} = \chi(j-i);\ 1 \le i \le p,\ 1 \le j \le p,\ i \neq j \tag{16}$$

$$B_{i,i} = 0;\ 0 \le i \le p \tag{17}$$

where χ again denotes the Legendre symbol [12,24]. He shows that B, whose order is a multiple of 2, but not of 4, is orthogonal. It is not a Hadamard matrix, though, because some of its elements are 0. By definition, each element of a Hadamard matrix is either 1 or -1. He then proves that the substitutions

$$[1] \rightarrow \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \tag{18}$$

$$[-1] \rightarrow \begin{bmatrix} -1 & -1 \\ -1 & 1 \end{bmatrix} \tag{19}$$

$$[0] \rightarrow \begin{bmatrix} 1 & -1 \\ -1 & -1 \end{bmatrix} \tag{20}$$

result in a Hadamard matrix A of order 2(p+1), a multiple of 4.

In this case we have two options. The matrix B is already symmetric, for it is well known [25,28] that if

$$p \cong 1 (\text{mod } 4) \tag{21}$$

as specified by (14), then, contrary to (7),

$$\chi[-f(p)] = \chi[f(p)] \tag{22}$$

and by (15), (16), and (22),

$$B_{j,i} = B_{i,j};\quad 0 \le i \le p,\quad 0 \le j \le p \tag{23}$$

Alternatively, however, by exactly the same reasoning as in Section IV, in the submatrix B' (defined in Section II) the element symmetrically opposite $B_{i,j}$ with respect to the secondary diagonal of B' is $B_{p-j+1,p-i+1}$. By (16) and (22), exactly as in (9),

$$B_{p-j+1,p-i+1} = \chi[(p-i+1) - (p-j+1)] = \chi(j-i) = B_{i,j} \tag{24}$$

Thus B' is symmetric with respect to its own secondary diagonal. Consequently if the sequence of all but the 0th row (column) of B is reversed, the new matrix $\overline{B}$ is symmetric with respect to its principal diagonal.

By the substitutions (18) - (20), either a Paley matrix A of order 2(p+1) can be obtained from B, or a new matrix $\overline{A}$ of order 2(p+1) can be obtained from $\overline{B}$. Although A and $\overline{A}$ are not identical, we can show that both possess all of the desired properties, and in the remainder of this section $\hat{A}$ (defined in Section II) represents either A or $\overline{A}$.

Since the substitution matrices (18) - (20) are all symmetric, $\hat{A}$ is symmetric with respect to its principal diagonal, and thereby possesses property 1.

Since each of these substitution matrices has the same number of 1's as -1's on its principal diagonal, $\hat{A}$ does so also, and thereby possesses property 2.

Property 3 does not occur spontaneously in this case, but can be realized by an additional elementary matrix operation. From (15) and (18) we can deduce that in $\hat{A}$

$$\hat{A}_{i,0} = \hat{A}_{0,j} = 1 \; ; \; 2 \leq i \leq p \; , \; 2 \leq j \leq p \tag{25}$$

and from (17) and (20) that

$$\hat{A}_{0,0} = 1 \tag{26}$$

but that

$$A_{1,0} = A_{0,1} = -1 \tag{27}$$

Multiplication of both the 1th row and 1th column by -1 removes this discrepancy, resulting in a new matrix $\hat{\hat{A}}$ (defined in Section II) that does possess property 3. However, we must now verify that $\hat{\hat{A}}$ still possesses properties 1 and 2.

Since the ordinal number of the row and that of the column multiplied by -1 are identical, the symmetry of $\hat{\hat{A}}$ is preserved, so $\hat{\hat{A}}$ still possesses property 1.

Since $\hat{\hat{A}}_{1,1}$ is multiplied by -1 twice in the process, its sign is not changed, so the equality of the number of 1's and -1's on the principal diagonal is preserved, and $\hat{\hat{A}}$ still possesses property 2.

Thus $\hat{\hat{A}}$ possesses all of the desired properties.

VI. PALEY'S LEMMA 4

In this case

$$m = 4\mu = 2^k(p^h + 1)\,;\ k = 0,\ p^h \cong 3 \pmod 4 \tag{28}$$

where k is (in general) a nonnegative integer, h is a positive integer, and p is any prime number satisfying the constraint, in which the congruency symbol implies that the remainder of $p^h/4$ is 3.

The elements of Paley's matrix A are

$$A_{i,0} = A_{0,j} = 1\,;\ 0 \le i \le p^h\,,\ 0 \le j \le p^h \tag{29}$$

$$A_{i,j} = \chi(\xi_j - \xi_i)\,;\ 1 \le i \le p^h,\ 1 \le j \le p^h,\ i \ne j \tag{30}$$

$$A_{i,i} = -1\,;\ 1 \le i \le p^h \tag{31}$$

where the ξ's in (30) denote not numerals, but polynomials, and χ denotes not the Legendre symbol, but the quadratic characters of a finite Galois field [6, 13,20,29]

$$GF[\xi_q(x)] = GF(p^h)[\text{mod } p, \text{mod } P(x)];\ q = 1,2,\ldots,p^h \tag{32}$$

where x is a real variable, $F[\xi_q(x)]$ is a set of p^h polynomials, conveniently written in matrix form as

$$\xi_q(x)] = [\alpha_{q,r}] \cdot x^r]\,;\ q = 1,2,\ldots,p^h\,;\ r = h-1,h-2,\ldots,0 \tag{33}$$

in which the p^h-by-h coefficient matrix $[\alpha_{q,r}]$ is simply a conventional pnary

table listing all p^h possible combinations of the integers

$$\alpha_{q,r} = 0,1,\ldots,p-1 \tag{34}$$

taken h at a time, and P(x) is an irreducible polynomial of degree h, which by definition cannot be divided without a remainder by any polynomial of degree less than h but greater than 0 [21]. Irreducible polynomials have been tabulated for all values of $p \leq 31$ and $h \leq 9$ for which $p^h < 1000$ [7,8].

In (32) some engineers and mathematicians write [mod p, mod P(x)] more compactly as [modd p, P(x)].

As indicated by Paley, the $\xi_q(x)$ are called the marks of the field. Some engineers and mathematicians call them elements instead of marks [6,13,20, 29], but we avoid this terminology herein to prevent confusion with the elements of matrices. The first p marks in any field defined by (33) are constants (polynomials of degree 0), whose values are specified by (34), called the integral marks of the field.

In the theory of Galois fields it is shown that every difference $\xi_j - \xi_i$ in (30) is uniquely equal to some other field mark, say ξ_v $(1 \leq v \leq p^h)$, and subject to the constraint

$$P(x) = 0 \tag{35}$$

reduces to a unique power of x, say x^w $(1 \leq w \leq p^h)$, so analogous to (5),

$$\chi(\xi_j - \xi_i) = \chi(\xi_v) = \chi(x^w)$$

$$= \begin{Bmatrix} 1 \\ -1 \end{Bmatrix} \text{ if } x^w \text{ is a quadratic } \begin{Bmatrix} \text{residue} \\ \text{nonresidue} \end{Bmatrix} \text{ of } GF(p^h) \tag{36}$$

By definition

$$\chi(x^w) = \begin{Bmatrix} 1 \\ -1 \end{Bmatrix} \text{ if } x^w \begin{Bmatrix} = \\ \neq \end{Bmatrix} y^2 \; ; \; y \in GF(p^h) \tag{37}$$

where y is a real variable. To satisfy the equality

$$x^w = y^2 \tag{38}$$

in (37), and to be a field mark as specified by the constraint in (37), it is necessary that

$$y = x^{\frac{w}{2}} \tag{39}$$

be an integral power of x. Since $x^{\frac{w}{2}}$ (w even) is either a mark, or congruent to a mark, of GF(p^h), while $x^{\frac{w}{2}}$ (w odd) is not, then

$$\chi(\xi_j - \xi_i) = \begin{Bmatrix} 1 \\ -1 \end{Bmatrix} \text{ if w is } \begin{Bmatrix} \text{even} \\ \text{odd} \end{Bmatrix} ; \quad w = 1,2,\ldots,p^h-1 \tag{40}$$

As in Section IV, although A possesses property 3 of Section I by (29), it does not possess property 2, since by (29) and (31) all elements on the principal diagonal except $A_{0,0}$ are identical.

Nor does it possess property 1, for we can show easily that A is not symmetric. Corresponding to (6) and (7), if

$$p^h \cong 3 (\text{mod } 4) \tag{41}$$

as specified by (28), then

$$\chi[-f(p^h)] = -\chi[f(p^h)] \tag{42}$$

where $f(p^h)$ denotes simply the argument of χ in functional form. In the submatrix A' (defined in Section II) the element symmetrically opposite $A_{i,j}$ with respect to the principal diagonal of A' (and of A) is $A_{j,i}$. By (30) and (42),

$$A_{j,i} = \chi(\xi_i - \xi_j) = \chi[-(\xi_j - \xi_i)] = -\chi(\xi_j - \xi_i) = -A_{i,j} \tag{43}$$

Thus A' is skew-symmetric, and consequently A is not symmetric.

However, in A the element symmetrically opposite $A_{i,j}$ with respect to the secondary diagonal of A is A_{p^h-j,p^h-i}. In A' the element symmetrically opposite $A_{i,j}$ with respect to the secondary diagonal of A' must be one row below and one column to the right of A_{p^h-j,p^h-i}, and is therefore A_{p^h-j+1,p^h-i+1}. By (30),

$$A_{p^h-j+1,p^h-i+1} = \chi(\xi_{p^h-i+1} - \xi_{p^h-j+1}) \tag{44}$$

Considering the modular nature of GF(p^h), we can readily deduce from (33) that for any value of q,

$$\xi_{p^h} = \xi_q + \xi_{p^h-q+1} \; ; \; q = 1,2,\ldots,p^h \tag{45}$$

Then by (45), with q replaced by i or j as required, we can rewrite (44) as

$$A_{p^h-j+1,\,p^h-i+1} = \chi\,[(\xi_{p^h} - \xi_i) - (\xi_{p^h} - \xi_j)] = \chi\,(\xi_j - \xi_i) = A_{i,j} \tag{46}$$

Thus A' is symmetric with respect to its own secondary diagonal. Consequently if the sequence of all but the 0th row (column) of A is reversed, the new matrix $\bar{A}$ is symmetric with respect to its principal diagonal, and thereby possesses property 1.

The elements on the secondary diagonal of A' are A_{i,p^h+1-i}. By (30),

$$A_{i,p^h+1-i} = \chi\,(\xi_{p^h+1-i} - \xi_i) \tag{47}$$

Since the order of A is p^h+1, that of A' is p^h. Since p, a prime number, is always odd, so is the number of elements on the secondary diagonal of A', one of which must be also on the principal diagonal of A. With this one exception, then, for every element defined by (47), there is another element $A_{p^h+1-i,i}$ (i.e., one with the row and column indices simply interchanged). By (30), (42), and (47),

$$A_{p^h+1-i,i} = \chi\,(\xi_i - \xi_{p^h+1-i}) = -\chi\,(\xi_{p^h+1-i} - \xi_i) = -A_{i,p^h+1-i} \tag{48}$$

By the foregoing reasoning and (31), the excepted element is

$$A_{\frac{p^h+1}{2},\,\frac{p^h+1}{2}} = -1 \tag{49}$$

Thus the number of -1's on the secondary diagonal of A' is just one greater

than the number of 1's. But by (29),

$$A_{0,0} = 1 \tag{50}$$

Consequently if the sequence of all but the 0th row (column) of A is reversed, the new matrix $\overline{A}$ has the same number of 1's as -1's on its principal diagonal, and thereby possesses property 2.

Finally, by (29), all elements in the 0th row and 0th column of A are 1. Reversing the sequence of all but the 0th row (column) of A alters neither its 0th row nor 0th column. Consequently the new matrix $\overline{A}$ is of normal form, and thereby possesses property 3.

VII. COMBINATION OF PALEY'S LEMMAS 3 AND 4

Under his lemma 4 Paley does not explain what to do if, instead of (28),

$$m = 4\mu = 2^k(p^h + 1)\ ;\ k = 0,\ p^h \cong 1 (\mathrm{mod}\ 4) \tag{51}$$

In this case we can employ somewhat the same method as under his lemma 3.

First we obtain a matrix B of order $p^h + 1$, whose elements (corresponding to, but not exactly the same as, (29) - (31)) are

$$B_{i,0} = B_{0,j} = 1\ ;\ 1 \leq i \leq p^h\ ,\ 1 \leq j \leq p^h \tag{52}$$

$$B_{i,j} = \chi(\xi_j - \xi_i)\ ;\ 1 \leq i \leq p^h\ ,\ 1 \leq j \leq p^h\ ,\ i \neq j \tag{53}$$

$$B_{i,i} = 0\ ;\quad 0 \leq i \leq p^h \tag{54}$$

where again, as in Section VI, the ξ's denote the marks, and χ the quadratic characters, of a finite Galois field as defined by (32) - (40). We can then prove by Paley's methods [18] or others (see Appendix) that B, whose order is a multiple of 2 but not of 4, is orthogonal, although not a Hadamard matrix, and that the substitutions (18) - (20) result in a Hadamard matrix of order $2(p^h+1)$, a multiple of 4.

As in Section V, in this case again we have two options. The matrix B is already symmetric. Corresponding to (21) and (22), if

$$p^h \cong 1 \pmod 4 \tag{55}$$

as specified by (51), then contrary to (42),

$$\chi[-f(p^h)] = \chi[f(p^h)] \tag{56}$$

and by (52), (53), and (56),

$$B_{j,i} = B_{i,j}; \quad 0 \leq i \leq p^h, \quad 0 \leq j \leq p^h \tag{57}$$

Alternatively, however, by exactly the same reasoning as in Section IV, in the submatrix B' (defined in Section II) the element symmetrically opposite $B_{i,j}$ with respect to the secondary diagonal of B' is B_{p^h-j+1,p^h-i+1}. By (53),

$$B_{p^h-j+1,p^h-i+1} = \chi(\xi_{p^h-i+1} - \xi_{p^h-j+1}) \tag{58}$$

Then, as in Section VI, by (45) with q replaced by i or j as required, we can rewrite (58) as

$$B_{p^h-j+1,p^h-i+1} = \chi[(\xi_{p^h} - \xi_i) - (\xi_{p^h} - \xi_j)] = \chi(\xi_j - \xi_i) = B_{i,j} \tag{59}$$

corresponding to (46). Thus B' is symmetric with respect to its own secondary diagonal. Consequently if the sequence of all but the 0th row (column) of B is reversed, the new matrix $\overline{B}$ is symmetric with respect to its principal diagonal, and thereby possesses property 1.

Then, as in Section V, by the substitutions (18) - (20), either a Paley matrix A of order $2(p^h+1)$ can be obtained from B, or a new matrix $\overline{A}$ of order $2(p^h+1)$ can be obtained from $\overline{B}$. Although A and $\overline{A}$ are not identical, we can show that both possess all of the desired properties, and in the remainder of this section $\hat{A}$ (defined in Section II) represents either A or $\overline{A}$.

Since the substitution matrices (18) - (20) are all symmetric, $\hat{A}$ is symmetric with respect to its principal diagonal, and thereby possesses property 1.

Since each of these substitution matrices has the same number of 1's as -1's on its principal diagonal, $\hat{A}$ does so also, and thereby possesses property 2.

As in Section V, property 3 does not occur spontaneously in this case, but can be realized by an additional elementary matrix operation. From (18) and (52) we can deduce that in $\hat{A}$,

$$\hat{A}_{i,0} = \hat{A}_{0,j} = 1 \; ; \; 2 \leq i \leq p^h \; , \; 2 \leq j \leq p^h \tag{60}$$

and from (20) and (54) that

$$\hat{A}_{0,0} = 1 \tag{61}$$

but that

$$\hat{A}_{1,0} = \hat{A}_{0,1} = -1 \tag{62}$$

corresponding to (25) - (27). Multiplication of both the $\underline{1}$th row and $\underline{1}$th column by -1 removes this discrepancy, resulting in a new matrix $\hat{\hat{A}}$ that does possess property 3, and that also, as in Section V, still possesses properties 1 and 2.

VIII. OTHER VALUES OF THE PARAMETERS

In Section V, if the constraint in (14) is changed so that

$$k > 1 \tag{63}$$

the modification implies an application of Paley's lemma 1 to the matrix $\hat{\hat{A}}$ of order 2(p+1), to obtain another new matrix

$$\tilde{\hat{A}} = W \times \hat{\hat{A}} \tag{64}$$

of order $2^k(p+1)$, where $\times$ denotes a Kronecker product, and W is a Walsh matrix of order 2^{k-1}.

Also in Section V, if the constraint in (14) is changed so that

$$k \geq 1 \ , \quad p \cong 3 (\text{mod } 4) \tag{65}$$

the modification implies an application of Paley's lemma 1 to the matrix $\overline{A}$ of order p+1 obtained in Section IV, to obtain another new matrix

$$\widetilde{A} = W \times \overline{A} \tag{66}$$

of order $2^k(p+1)$, where W is of order 2^k.

In Section VI, if the constraint in (28) is changed so that

$$k \geq 1 \tag{67}$$

the modification implies an application of Paley's lemma 1 to the matrix $\overline{A}$ of order p^h+1, to obtain a second new matrix

$$\widetilde{A} = W \times \overline{A} \tag{68}$$

of order $2^k(p^h+1)$, where W is of order 2^k.

Finally, in Section VII, if the constraint in (51) is changed so that

$$k \geq 1 \tag{69}$$

the modification implies an application of Paley's lemma 1 to the matrix $\hat{\hat{A}}$ of order $2(p^h+1)$, to obtain another new matrix

$$\widetilde{\widetilde{A}} = W \times \hat{\hat{A}} \tag{70}$$

of order $2^k(p^h+1)$, where W is of order 2^{k-1}.

In each of these cases W is of the type Paley uses for illustration[17], one of natural or Hadamard ordering in the terminology of standard forms of Walsh matrices [1].

Observe carefully that whenever a row (column) sequence reversal is involved, we must perform this operation before forming the Kronecker product. We know from the fundamental nature of the Kronecker product that $\widetilde{\widetilde{A}}$ in (64) and (70), and $\widetilde{A}$ in (66) and (68), possess all of the desired properties listed in Section I. But if we form the Kronecker product of W and A of Section IV or VI,

or that of W and B of Section V or VII, we know again from the fundamental nature of the Kronecker product, or can easily verify by an example, that neither of the submatrices obtained by deleting the 0th row and 0th column of W x A or W x B can ever be fully symmetric with respect to its own secondary diagonal, and therefore can never fulfill one of the essential conditions upon which our method is based. For a specific example, compute the Kronecker product of W of order 2 and Paley's matrix of order 12 (Fig. 1), and examine the submatrix obtained by deleting the 0th row and 0th column of the product matrix of order 24.

This precaution if not necessary in the cases where the already symmetric matrix B is used withour row (column) sequence reversal.

IX. SUMMARY AND CONCLUSIONS

Any Hadamard matrix obtained by Paley's lemmas 2 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 matrices defined and illustrated in [1].

Paley matrices of most orders are not constructed uniquely, however. Table I is an updating and extension of Paley's Table I [15], indicating the Paley lemma or lemmas, in the order of their application if a combination of them is required, by which each Paley matrix can be constructed. In this table $p + 1$ implies direct construction of an A matrix, $2(p + 1)$ implies construction of a B matrix and the substitutions (18 - 20), and $[\ldots] \times 2^k$ implies a Kronecker product of order 2^k.

We have neither discussed nor utilized Paley's lemma 5, simply because it is unnecessary for any matrix of practicable size. Paley obviously did not utilize it in compiling his own Table I, for none of the equations in that table is of the form defined by his lemma 5.

TABLE I

Paley Matrices Convertible to Proposed Standard Forms

Order m	Lemma 2 m=f(p + 1) $p \cong 3 \pmod 4$	Lemma 3 m=f[2(p + 1)] $p \cong 1 \pmod 4$	Lemma 4 m=f(p^h + 1) $p^h \cong 3 \pmod 4$	Lemmas 3 & 4 m=f[2(p^h + 1)] $p^h \cong 1 \pmod 4$
12	11 + 1	2(5 + 1)		
20	19 + 1			$2(3^2 + 1)$
24	23 + 1	[2(5 + 1)]×2		
	[11 + 1]×2			
28		2(13 + 1)	$3^3 + 1$	
36		2(17 + 1)		
40	[19 + 1]×2			$[2(3^2 + 1)]\times 2$
44	43 + 1			
48	47 + 1	$[2(5 + 1)]\times 2^2$		
	[23 + 1]×2			
	$[11 + 1]\times 2^2$			
52				$2(5^2 + 1)$
56		[2(13 + 1)]×2	$[3^3 + 1]\times 2$	
60	59 + 1	2(29 + 1)		
68	67 + 1			
72	71 + 1	[2(17 + 1)]×2		
76		2(37 + 1)		
80	79 + 1			$[2(3^2 + 1)]\times 2^2$
	$[19 + 1]\times 2^2$			
84	83 + 1	2(41 + 1)		
88	[43 + 1]×2			
96	[47 + 1]×2	$[2(5 + 1)]\times 2^3$		
	$[23 + 1]\times 2^2$			
	$[11 + 1]\times 2^3$			
100				$2(7^2 + 1)$
104	103 + 1			$[2(5^2 + 1)]\times 2$

TABLE I
(Cont'd)

Order m	Lemma 2 m=f(p + 1) p ≡ 3(mod 4)	Lemma 3 m=f 2(p + 1) p ≡ 1(mod 4)	Lemma 4 m=f(p^h + 1) p^h ≡ 3(mod 4)	Lemmas 3&4 m=f 2(p^h + 1) p^h ≡ 1(mod 4)
108	107 + 1	2(53 + 1)		
112		$[2(13 + 1)]\times 2^2$	$[3^3 + 1]\times 2^2$	
120	$[59 + 1]\times 2$	$[2(29 + 1)]\times 2$		
124		2(61 + 1)		
132	131 + 1			
136	[67 + 1]×2*			
140	139 + 1			
144	$[71 + 1]\times 2$	$[2(17 + 1)]\times 2^2$		
148		2(73 + 1)		
152	151 + 1	$[2(37 + 1)]\times 2$		
160	$[79 + 1]\times 2$			$[2(3^2 + 1)]\times 2^3$
	$[19 + 1)]\times 2^3$			
164	163 + 1			$2(3^4 + 1)$
168	167 + 1	$[2(41 + 1)]\times 2$		
	$[83 + 1]\times 2$			
176	$[43 + 1]\times 2^2$			
180	179 + 1	2(89 + 1)		
192	191 + 1	$[2(5 + 1)]\times 2^4$		
	$[47 + 1]\times 2^2$			
	$[23 + 1]\times 2^3$			
	$[11 + 1]\times 2^4$			
196		2(97 + 1)		
200	199 + 1			$[2(7^2 + 1)]\times 2$

*In Paley's original table [14] this entry was incorrect, duplicating there the correct entry for m = 152.

Although the more general Hadamard matrices II (of order $4\mu \neq 2^{\nu}$) differ markedly from the Walsh matrices in properties other than those listed in Section I, adoption of the form proposed herein as a tentative standard for engineering purposes will encourage a more widespread and uniform application of them, facilitate a clearer understanding of them, and promote further investigation of them.

As shown in Sections V and VII, in the case of lemma 3 or a combination of lemmas 3 and 4, the matrix B is already symmetric, thus making the row (column) sequence reversal optional, and leading to two possible desired forms. Perhaps both forms should be adopted as tentative standards for engineering purposes, just as more than one standard form of Walsh matrix has been defined [1].

Undoubtedly by appropriate changes of variables Paley's formulas could be modified for more direct construction of the desired form, eliminating the necessity of first constructing the Paley matrix and then applying the appropriate elementary matrix operations.

Other areas for fruitful research are possible additional properties common among and/or unique to the converted matrices, properties of their row (column) vectors, and whether the more recently discovered types of non-Walsh Hadamard matrices also can be converted to the desired form.

X. ACKNOWLEDGEMENTS

Special acknowledgements are due Raymond S. Larsen and Carl W. Olson of the Stanford Linear Accelerator Center, Stanford University, Stanford, California, for enabling the author to perform this.

REFERENCES

1. 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, "Codes with Special Correlation," in Digital Communications with Space Applications (S. W. Golomb, ed.), p. 54; Prentice-Hall, Englewood Cliffs, N. J., 1964.

3. Ibid., p. 55.

4. L. D. Baumert, "Hadamard Matrices of Orders 116 and 232," Bulletin of the American Mathematical Society, Vol. 72, p. 237; 1966.

5. L. D. Baumert and M. Hall, Jr., "Hadamard Matrices of the Williamson Type," Mathematics of Computation, Vol. XIX, pp. 442-447; 1965.

6. B. Benjauthrit and I. S. Reed, "Galois switching functions and their applications," IEEE Transactions on Computers, Vol. C-25, pp. 78-86; January 1976.

7. W. H. Bussey, "Galois field tables for $p^n \leq 169$," Bulletin of the American Mathematical Society, Vol. XII, pp. 22-38; October 1905.

8. W. H. Bussey, "Galois field tables of order less than 1000," Bulletin of the American Mathematical Society, Vol. XVI, pp. 188-206; January 1910.

9. S. W. Golomb and L. D. Baumert, "The Search for Hadamard Matrices," American Mathematical Monthly, Vol. 70, pp. 12-17; January 1963.

10. Ibid., p. 14.

11. H. J. Harmuth, Transmission of Information by Orthogonal Functions, 2nd ed., pp. 30-31; Springer-Verlag, New York/Heidelberg/Berlin, 1972.

12. G. James and R. C. James, Mathematics Dictionary, 3rd ed., p. 213; Van Nostrand, New York, 1968.

13. K. S. Menger, Jr., "A Transform for Logic Networks," IEEE Transactions on Computers, Vol. C-18, pp. 241-250; March 1969.

14. R. E. A. C. Paley, "On Orthogonal Matrices," Journal of Mathematics and Physics, Vol. 12, pp. 313-320; 1933.

15. Ibid., p. 317.

16. Ibid., pp. 313 and 316.

17. Ibid., p. 312.

18. Ibid., pp. 314 and 315.

19. W. W. Pease III, Methods of Matrix Algebra, p. 322; Academic Press, New York/London, 1965.

20. W. W. Peterson and E. J. Weldon, Jr., Error-Correcting Codes, 2nd ed., Chap. 6: "Polynomial Rings and Galois Fields"; MIT Press, Cambridge, Mass./London, 1972.

21. Ibid., p. 148.

22. R. J. Turyn, "Hadamard Matrices, Baumert-Hall Units, Four-Symbol Sequences, Pulse Compression, and Surface Wave Encodings," Journal of Comboinatorial Theory, Vol. 16, pp. 313-333; 1974.

23. U. S. Dept. of Commerce, Natl. Bur. Stand., Applied Mathematics Series, Vol. 55, Handbook of Mathematical Functions, p. 826 (definitions) and pp. 840-843 (tables); U. S. Govt. Printing Office, Washington, D. C., 1964.

24. I. M. Vinogradov, Elements of Number Theory, p. 81; Dover Publications (reprint), New York, 1954.

25. Ibid., p. 82.

26. W. D. Wallis, A. P. Street, and J. S. Wallis, Lecture Notes in Mathematics, A. Dold and B. Eckmann, eds., Vol. 292, Combinatorics: Room Squares, Sum-Free Sets, Hadamard Matrices, Appendices A, B, D, E, and H; Springer-Verlag, Berlin/Heidelberg/New York, 1972.

27. Ibid., p. 18.

28. Ibid., p. 9.

29. Ibid., pp. 7-9.

APPENDIX

1. Proof of orthogonality of matrix B in Section VII

For any two rows i_1 and i_2 other than the 0th row,

$$\sum_{j=0}^{p^h} B_{i_1,j} B_{i_2,j} = B_{i_1,0} B_{i_2,0} + \sum_{j=1}^{p^h} B_{i_1,j} B_{i_2,j} ;$$

$$1 \le i_1 \le p^h, \quad 1 \le i_2 \le p^h, \quad i_1 \ne i_2 \qquad \text{(A-1)}$$

By substituting (52) and (53), we can rewrite (A-1) as

$$\sum_{j=0}^{p^h} B_{i_1,j} B_{i_2,j} = 1 + \sum_{j=1}^{p^h} \chi(\xi_j - \xi_{i_1}) \chi(\xi_j - \xi_{i_2}) \qquad \text{(A-2)}$$

Subtracting and adding ξ_{i_1} in the argument of the second χ in the summation, we can rewrite (A-2) as

$$\sum_{j=0}^{p^h} B_{i_1,j} B_{i_2,j} = 1 + \sum_{j=1}^{p^h} \chi(\xi_j - \xi_{i_1}) \chi(\xi_j - \xi_{i_1} + \xi_{i_1} - \xi_{i_2}) \qquad \text{(A-3)}$$

Since the difference (or sum) of any two marks of a finite Galois field is uniquely equal or congruent to some other mark of the field, and since ξ_j varies over all the marks ($1 \le j \le p^h$), we can let

$$\xi_j - \xi_{i_1} = \bar{\xi}_j \qquad \text{(A-4)}$$

$$\xi_{i_1} - \xi_{i_2} = \xi_\sigma \qquad \text{(A-5)}$$

where σ is a constant, and rewrite (A-3) as

$$\sum_{j=0}^{p^h} B_{i_1,j} B_{i_2,j} = 1 + \sum_{j=1}^{p^h} \chi(\bar{\xi}_j) \chi(\bar{\xi}_j + \xi_\sigma) \qquad \text{(A-6)}$$

By the constraint in (A-1),

$$i_1 \ne i_2 \qquad \text{(A-7)}$$

so in (A-5)

$$\xi_{i_1} \neq \xi_{i_2} \tag{A-8}$$

and consequently

$$\xi_\sigma \neq 0 \tag{A-9}$$

It is shown in [26] that if ξ_σ is nonzero, as in (A-9), then the summation on the right side of (A-6) reduces to -1, from which it follows that

$$\sum_{j=0}^{p^h} B_{i_1,j} B_{i_2,j} = 1 - 1 = 0 ; \quad i_1 \neq i_2 \tag{A-10}$$

Now, if i_1 denotes the 0th row and i_2 denotes any other row, then, corresponding to (A-1),

$$\sum_{j=0}^{p^h} B_{0,j} B_{i_2,j} = B_{0,0} B_{i_2,0} + \sum_{j=1}^{p^h} B_{0,j} B_{i_2,j} ; \; 1 \leq i_2 \leq p^h \tag{A-11}$$

By substituting (52) and (54), we can rewrite (A-11) as

$$\sum_{j=0}^{p^h} B_{0,j} B_{i_2,j} = \sum_{j=1}^{p^h} B_{i_2,j} \tag{A-12}$$

By substituting (53) and (54) and recognizing that $\chi(0)$ is not defined, we can rewrite (A-12) as

$$\sum_{j=0}^{p^h} B_{0,j} B_{i_2,j} = \sum_{j=1}^{i_2-1} \chi(\xi_j - \xi_{i_2}) + B_{i_2,i_2} + \sum_{j=i_2+1}^{p^h} \chi(\xi_j - \xi_{i_2}) \tag{A-13}$$

By (54), the second term on the right side vanishes. Then by substituting (A-4), we can rewrite (A-13) as

$$\sum_{j=0}^{p^h} B_{0,j} B_{i_2,j} = \sum_{j=1}^{i_2-1} \chi(\bar{\xi}_j) + \sum_{j=i_2+1}^{p^h} \chi(\bar{\xi}_j) \tag{A-14}$$

Since p, a prime number, is always odd, so is p^h, so the two summations on the right side, taken together, contain an even number of terms, exactly half of which are quadratic residues and half of which are quadratic nonresidues, whose quadratic characters are, by (36), 1 and -1 respectively. It follows that (A-14) reduces to

$$\sum_{j=0}^{p^h} B_{0,j} B_{i_2,j} = \frac{p^h-1}{2} - \frac{p^h-1}{2} = 0 \qquad \text{(A-15)}$$

Consequently, by (A-10) and (A-15), B is orthogonal, Q.E.D.

2. Proof of orthogonality of matrix A in Section VII

Consider any two rows R_{i_1} and R_{i_2} ($i_1, i_2 = 0, 1, \ldots, p^h$; $i_1 \neq i_2$) of B. Since B is orthogonal, with each element either 1 or -1, except on its principal diagonal, where each element is 0, then R_{i_1} and R_{i_2} must contain the same number of pairs of like elements (both 1 or both -1) as of unlike elements (one 1 and the other -1) in the columns in which R_{i_1} and R_{i_2} do not intersect the principal diagonal. In any two of these columns, one containing a like pair and the other an unlike pair of elements, the result of the substitutions (18) and (19) is an orthogonal submatrix of order 4 of A.

Thus we need consider further only the two columns C_{j_1} and C_{j_2} ($j_1, j_2 = 1, 2, \ldots, p^h$; $j_1 \neq j_2$) of B in which R_{i_1} and R_{i_2} do intersect the principal diagonal. For this purpose we can write

$$R_{i_1} = \ldots\ldots 0 \qquad \ldots\ldots B_{i_1,j_2} \ldots\ldots \qquad \text{(A-16)}$$

$$R_{i_2} = \ldots\ldots B_{i_2,j_1} \ldots\ldots 0 \qquad \ldots\ldots \qquad \text{(A-17)}$$

In these two columns the result of substituting (18) - (20) is again a submatrix of order 4 of A, which, however, may or may not be orthogonal. By

making the substitutions we can readily verify that it is orthogonal if

$$B_{i_1,j_2} = B_{i_2,j_1} = 1 \text{ or } -1 \tag{A-18}$$

but not if

$$B_{i_1,j_2} = -B_{i_2,j_1} = 1 \text{ or } -1 \tag{A-19}$$

Thus A is orthogonal if and only if (A-18) is an identity. By (53),

$$B_{i_1,j_2} = \chi(\xi_{j_2} - \xi_{i_1}) \; ; \; i_1 \neq j_2 \tag{A-20}$$

$$B_{i_2,j_1} = \chi(\xi_{j_1} - \xi_{i_2}) \; ; \; i_2 \neq j_1 \tag{A-21}$$

But by (A-16), (A-17), and (54), the elements of R_{i_1} and R_{i_2} on the principal diagonal of B are

$$B_{i_1,j_1} = B_{i_1,i_1} = 0 \tag{A-22}$$

$$B_{i_2,j_2} = B_{i_2,i_2} = 0 \tag{A-23}$$

from which it follows that

$$j_1 = i_1 \tag{A-24}$$

$$j_2 = i_2 \tag{A-25}$$

Therefore we can rewrite (A-20) and (A-21) as

$$B_{i_1,j_2} = B_{i_1,i_2} = \chi(\xi_{i_2} - \xi_{i_1}); \; i_1 \neq i_2 \tag{A-26}$$

$$\begin{aligned} B_{i_2,j_1} &= B_{i_2,i_1} = \chi(\xi_{i_1} - \xi_{i_2}) \\ &= \chi[-(\xi_{i_2} - \xi_{i_1})]; \; i_2 \neq i_1 \end{aligned} \tag{A-27}$$

Finally, by (55) and (56), we can rewrite (A-27) as

$$B_{i_2,j_1} = \chi(\xi_{i_2} - \xi_{i_1}) = B_{i_1,j_2} \tag{A-28}$$

thus verifying that (A-18) is an identity, and consequently that A is orthogonal, Q.E.D.