25. Some New Series of Hadamard Matrices

By Mieko YAMADA
Department of Mathematics, Tokyo Women's Christian University

(Communicated by Shokichi IYANAGA, M. J. A., March 12, 1987)

1. Statement of the results. In this note we shall show that the following theorems hold.

Theorem 1. *If* $q\equiv 1 \pmod 8$ *is a prime power and there exists an Hadamard matrix of order* $(q-1)/2$, *then we can construct an Hadamard matrix of order* $4q$.

Theorem 2. *If* $q\equiv 5 \pmod 8$ *is a prime power and there exists a skew-Hadamard matrix of order* $(q+3)/2$, *then we can construct an Hadamard matrix of order* $4(q+2)$.

Theorem 3. *If* $q\equiv 1 \pmod 8$ *is a prime power and there exists a symmetric C-matrix of order* $(q+3)/2$, *then we can construct an Hadamard matrix of order* $4(q+2)$.

The particular cases of Theorems 2, 3 when $(q+3)/2$ is a prime power, were given (without proof) as Theorem 9.18 by Kiyasu [2]. In a private communication, he showed that Theorems 2, 3 can be proved by using KSW array. In this note we prove all these three Theorems by using an adaptation of generalized quaternion type array and relative Gauss sums.

We have the following 39, 36 and 8 new orders $4n$ for $n\leqq 10000$, of Hadamard matrices from Theorems 1, 2, and 3 respectively, which are not found in the list of Geramita and Seberry [1].

(1) New orders obtained from Theorem 1.
n: 233, 809, 953, 1193, 1889, 2393, 2417, 2441, 2729, 2953, 3209, 3593, 3617, 3881, 4049, 4217, 4721, 4889, 5657, 5849, 6073, 6089, 6113, 6257, 6449, 6473, 6569, 6977, 7177, 7417, 7433, 7753, 7793, 8297, 8369, 8609, 8713, 8761, 9833.

(2) New orders obtained from Theorem 2.
n: 103, 127, 151, 655, 879, 1231, 1951, 1999, 2209, 2271, 2559, 2799, 2839, 2959, 3039, 3183, 3583, 3679, 4359, 4735, 4863, 4911, 5079, 5311, 5503, 5815, 5983, 6199, 6639, 7519, 8119, 8223, 8679, 9279, 9631, 9903.

(3) New orders obtained from Theorem 3.
n: 579, 2019, 3043, 4443, 6339, 7419, 8523, 9819.

2. The following notations will be used in this note.

q: a power of a prime p; $F=GF(q)$: a finite field with q elements
$K=GF(q^t)$: an extension of F of degree $t\geqq 2$
$S_{K/F}$: the relative trace from K to F; ξ: a primitive element of K
A^*: the transpose of a matrix A; I_m: the unit matrix of order m

J_m: the matrix of order m with every element $+1$
$\otimes$: tensor product of matrices
$J_m(x)=1+x+\cdots+x^{m-1}$.

3. From our arguments in [3], we easily obtain the following theorem which gives special Hadamard matrices of order $4(n+1)$.

Theorem 4. *Let*

$$L=\begin{pmatrix} 1 & -1 & -1 & -1 \\ -1 & 1 & -1 & -1 \\ -1 & -1 & 1 & -1 \\ -1 & -1 & -1 & 1 \end{pmatrix}, \quad M=\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & -1 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & 1 & -1 \end{pmatrix}$$

and $N=-LM/2$. *Note that* L, M, N *are Hadamard matrices of order* 4. *Now*

$$H=\begin{pmatrix} A & B & C & D \\ -B^* & A^* & -D^* & C^* \\ -C^* & D & A^* & -B \\ -D^* & -C & B^* & A \end{pmatrix}$$

is a matrix of order $4n$ *if* A, B, C, D *are the matrices of order* n. *Moreover suppose that the component matrices* A, B, C, D *satisfy the following conditions*:

(i) A, B, C, D *are normal matrices of order* n *whose elements are from* $\{1, -1\}$,

(ii) $AB=BA$, $AC=CA$, $AD=DA^*$, $BC=C^*B$, $BD^*=DB^*$, $CD=DC$, $A^*B=BA^*$, $A^*D^*=D^*A$, $CB=BC^*$, $B^*D=D^*B$, $C^*D=DC^*$,

(iii) $AA^*+BB^*+CC^*+DD^*=4(n+1)I_n-4J_n$

(iv) $Ae=2e$, $Be=Ce=De=0$ *where* e *is the column vector of length* n *with every element* $+1$.

Then

$$\begin{pmatrix} 1\otimes L & e^*\otimes N \\ e\otimes M^* & H \end{pmatrix}$$

is an Hadamard matrix of order $4(n+1)$.

If A, B, C, D are circulant matrices, then the matrix H is the right regular representation matrix of a particular element in a nonassociative quaternion extension ring over the generalized quaternion ring. So we may regard the matrix H as an adaptation of generalized quaternion type array.

4. Let χ be a character of K such that $\chi(\xi)=\zeta_{q-1}$ where ζ_{q-1} is a primitive $(q-1)^{\text{th}}$ root of unity. We define the number z_m by

$$\chi\left(\frac{S_{K/F}\xi^m}{2\xi^m}\right)=\zeta_{q-1}^{z_m} \quad \text{for} \quad m\not\equiv\frac{(q+1)}{2} \pmod{q+1},$$

and let

$$f(x)\equiv\sum_{\substack{m=0 \\ m\neq(q+1)/2}}^{q} x^{z_m} \pmod{x^{q-1}-1}.$$

Lemma 1. *For the polynomial* $f(x)$, *we have*

(1) *$f(x)$ contains every x^{2m} exactly twice except for $x^0=1$,*

(2) $f(x)f(x^{-1})\equiv q+(q+1)J_{q-1}(x)-2J_{(q-1)/2}(x^2) \pmod{x^{q-1}-1}$.

Lemma 1 is derived from the norm relation of a certain character sum which is obtained from the additive formula [3, 4, 5] of the relative Gauss sum associated with χ.

Lemma 2. *Put $f(x)\equiv f_0(x^2)+xf_1(x^2) \pmod{x^{q-1}-1}$. By replacing x^2 by x in the polynomials $f_0(x^2)$ and $f_1(x^2)$, we define the polynomials*

$$\varphi_0(x)\equiv f_0(x)-J_{(q-1)/2}(x) \pmod{x^{(q-1)/2}-1},$$
$$\varphi_1(x)\equiv f_1(x)-J_{(q-1)/2}(x) \pmod{x^{(q-1)/2}-1}.$$

Then all the coefficients of $\varphi_0(x)$ and $\varphi_1(x)$ are from $\{1, -1\}$ and we have

$$\varphi_0(x)\varphi_0(x^{-1})+\varphi_1(x)\varphi_1(x^{-1})\equiv q-2J_{(q-1)/2}(x) \pmod{x^{(q-1)/2}-1}.$$

This Lemma follows from Lemma 1.

5. We assume that $q\equiv 1 \pmod 4$ and put $n=(q+1)/2$. We let i be a primitive fourth root of unity and denote by ψ the quadratic character of F. We define the polynomial $g(x)$ by

$$g(x)\equiv\sum_{m=0}^{q}\psi(S_{K/F}\xi^m)i^m x^m \pmod{x^n-1}.$$

Since n is odd, we can write $g(x)$ in following form

$$g(x)\equiv\sum_{m=0}^{n-1}\psi(S_{K/F}\xi^{4m})x^m+i^n\sum_{m=0}^{n-1}\psi(S_{K/F}\xi^{4m+n})x^m \pmod{x^n-1}.$$

Moreover we define the polynomials

$$\alpha(x)\equiv\sum_{m=0}^{n-1}\psi(S_{K/F}\xi^{4m})x^m \pmod{x^n-1},$$
$$\beta(x)\equiv\sum_{m=0}^{n-1}\psi(S_{K/F}\xi^{4m+n})x^m \pmod{x^n-1}.$$

Then we have $g(x)\equiv\alpha(x)+i^n\beta(x) \pmod{x^n-1}$ and $\alpha(x)$ and $\beta(x)$ have the following properties.

Lemma 3. *For the polynomials $\alpha(x)$ and $\beta(x)$, we have*

(1) $\alpha(x^{-1})\equiv\alpha(x), \beta(x^{-1})\equiv\beta(x) \pmod{x^n-1}$,

(2) $\alpha(x)\alpha(x^{-1})+\beta(x)\beta(x^{-1})\equiv q \pmod{x^n-1}$.

6. **Sketch of proof of Theorem 1.** We define the matrices A and B by using the polynomials $\varphi_0(x)$ and $\varphi_1(x)$ in Lemma 2, and let

$$A=\begin{pmatrix}1 & 1\\ 1 & 1\end{pmatrix}\otimes\varphi_0(T)+\begin{pmatrix}1 & -1\\ -1 & 1\end{pmatrix}\otimes I_{(q-1)/2},\quad B=\begin{pmatrix}1 & 1\\ 1 & 1\end{pmatrix}\otimes\varphi_1(T),$$

where T is the basic circulant matrix of order $(q-1)/2$.

Since there exists an Hadamard matrix H_0 of order $(q-1)/2$ by assumption, we define the matrices C and D by

$$C=\begin{pmatrix}1 & -1\\ -1 & 1\end{pmatrix}\otimes H_0, D=C \text{ or } D=C^*.$$

We can verify that the matrices A, B, C and D satisfy the conditions of Theorem 4. Therefore we can construct an Hadamard matrix of order $4q$.

7. **Sketch of proof of Theorem 2.** We define the matrices A and B by using the polynomials $\alpha(x)$ and $\beta(x)$ in Lemma 3, and let

$$A=\begin{pmatrix}1 & -1\\ -1 & 1\end{pmatrix}\otimes\beta(T)+\begin{pmatrix}1 & 1\\ 1 & 1\end{pmatrix}\otimes I_{(q+1)/2},\quad B=\begin{pmatrix}1 & -1\\ -1 & 1\end{pmatrix}\otimes\alpha(T),$$

where T is the basic circulant matrix of order $(q+1)/2$.

Let Q denote a skew-Hadamard matrix of order $(q+1)/2$, assumed to exist. We transform Q in a normalized form

$$Q=\begin{pmatrix} 1 & \boldsymbol{e}^* \\ -\boldsymbol{e} & S+I_{(q+1)/2} \end{pmatrix},$$

where $\boldsymbol{e}$ is the column vector of length $(q+1)/2$ with every element $+1$.

The matrices C and D are defined by

$$C=\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}\otimes S+\begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix}\otimes I_{(q+1)/2}, D=C \text{ or } D=C^*.$$

The matrices A, B, C and D satisfy all the conditions of Theorem 4. Hence Theorem 2 is proved.

8. Sketch of proof of Theorem 3. Let A, B be the same as in proof of Theorem 2. Let R be a C-matrix of order $(q+3)/2$, assumed to exist. We transform R in the form

$$R=\begin{pmatrix} 0 & \boldsymbol{e}^* \\ \boldsymbol{e} & U \end{pmatrix}.$$

Similarly we define the matrices C and D:

$$C=\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}\otimes U+\begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix}\otimes I_{(q+1)/2}, D=C \text{ or } D=C^*.$$

Now we proceed in the same way as in proof of Theorem 2.

References

[1] A. V. Geramita and J. Seberry: Orthogonal Designs. Lec. Notes in Pure and Applied Math., Marcel Dekker, New York-Basel, vol. 45 (1979).

[2] Z. Kiyasu: An Hadamard Matrix and its Applications. Denshi-Tsushin Gakkai, Tokyo (1980) (in Japanese).

[3] M. Yamada: Hadamard matrices generated by an adaptation of generalized quaternion type array. Graphs and Combinatorics, **2**, 179–187 (1986).

[4] K. Yamamoto and M. Yamada: Williamson Hadamard matrices and Gauss sums. J. Math. Soc. Japan, **37**, 703–717 (1985).

[5] K. Yamamoto: On congruences arising from relative Gauss sums. Number Theory and Combinatorics Japan 1984, World Scientific Publ., Singapore, 423–446 (1985).