

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 $n \leq 10000$, 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 $t \geq 2$

$S_{K/F}$: 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