New Constructions of Quaternary Hadamard Matrices [1]

*Ji-Woong Jang^{O}, *Sang-Hyo Kim, *Jong-Seon No, and +Habong Chung
*Seoul National University, +Hongik University
{stasera,kimsh}@ccl.snu.ac.kr, jsno@snu.ac.kr, habchung@hongik.ac.kr

Abstract

In this paper, we propose two new construction methods for quaternary Hadamard matrices. By the first method, which is applicable for any positive integer n, we are able to construct a quaternary Hadamard matrix of order 2^n from a binary sequence with ideal autocorrelation. The second method also gives us a quaternary Hadamard matrix of order 2^n from a binary extended sequence of period $2^n - 1$, where n is a composite number.

I. Introduction

A generalized Hadamard matrix $\mathcal{H}$ of order N is an $N \times N$ matrix satisfying $\mathcal{H}\mathcal{H}^\dagger = NI_N$, where $\dagger$ denotes the conjugate transpose and I_N is the identity matrix of order N [3]. In other words, any two distinct rows of $\mathcal{H}$ are orthogonal. For this reason, Hadamard matrices have been studied for the applications in many areas such as wireless communication systems, coding theory, and signal design[1]. Hadamard matrices have strong ties to sequences. Matsufuji and Suehiro proposed the complex Hadamard matrices related to bent sequences[7]. Popovic, Suehiro, and Fan[10] proposed orthogonal sets of quaternary sequences by using quadriphase sequence family $\mathcal{A}$ by Boztas, Hammons, and Kumar[2].

In this paper, we propose two new construction methods for quaternary Hadamard matrices. By the first method, which is applicable for any positive integer n, we are able to construct a quaternary Hadamard matrix of order 2^n from a binary sequence with ideal autocorrelation. The second method also gives us a quaternary Hadamard matrix of order 2^n from a binary extended sequence of period $2^n - 1$, where n is a composite number.

Let F_{2^n} be the finite field with 2^n elements. Let $F_{2^n}^* = F_{2^n} \setminus \{0\}$ and $s(x)$ be a mapping from F_{2^n} to F_2 or Z_4. If we restrict the mapping $s(x)$ to $F_{2^n}^*$ and replace x by α^t, where α is a primitive element in F_{2^n}, then we can obtain a sequence $s(\alpha^t)$, $0 \le t \le 2^n - 2$, of period $2^n - 1$. Hence, for convenience, we will use the expression 'a binary or quaternary sequence $s(\alpha^t)$ of period $2^n - 1$' interchangeably with 'a mapping $s(x)$ from F_{2^n} to F_2 or Z_4'.

It is not difficult to see that a variable v over Z_4 can be expressed using two binary variables v_1 and v_2 as $v = v_1 + 2v_2$ where addition is modulo 4. Let us define two maps ϕ and ψ as $\phi(v) = v_1$, $\psi(v) = v_2$.

It can be shown that $\phi(v - w)$ and $\psi(v - w)$ of the difference $v - w$ are expressed as

$$\begin{aligned} \phi(v-w) &= v_1 + w_1 \\ \psi(v-w) &= v_1 w_1 + w_1 + w_2 + v_2. \end{aligned} \qquad (1)$$

II. Preliminaries

Lemma 1 For a positive integer n, let $g(t)$ be a binary sequence of period $2^n - 1$ with ideal autocorrelation. Then for any z, $1 \le z \le 2^n - 2$, the following sequence $q_z(t)$ is balanced over Z_4.

$$q_z(t) = g(t) + 2g(t+z).$$

□

Using the above lemma, we get the quaternary Hadamard matrices as in the following theorem.

Theorem 1 Let n be an integer and $g(t)$, $0 \le t \le 2^n - 2$, be a sequence of period $2^n - 1$ with ideal autocorrelation. Then the following matrix $\mathcal{H}_Q$ is the $2^n \times 2^n$ quaternary Hadamard matrix.

$$\mathcal{H}_Q = (h_{ij}), \quad 0 \le i, j \le 2^n - 1$$

where h_{ij} is given as

$$h_{ij} = \begin{cases} 1, & \text{for } i = 0 \text{ or } j = 0 \\ w_4^{2g(j-1)}, & \text{for } i = 1 \text{ and } 1 \le j \le 2^n - 1 \\ w_4^{q_{i-1}(j-1)}, & \text{otherwise.} \end{cases}$$

□

[1] This work was supported in part by BK21 and ITRC program.