Generalized Complex Hadamard Codes

Xueqin Jiang TaeChol Shin MoonHo Lee Gi Yean Hwang
Chonbuk National University

Jiangxueqin@hotmail.com tcshin@naver.com Moonho@chonbuk.ac.kr Informan@chonbuk.ac.kr

Abstract

In this paper we consider a family $\{H_m\}, m=1,2,\ldots,$ of generalized Hadamard matrices of order p^m, where p is a prime number, and construct the corresponding family $\{C_m^*\}$ of generalize p-ary Hadarmard codes which meet the Plotkin bound.

Index terms: Cyclotomic fields, cocyclic matrices, Butson-Hadamard matrices, generalized Hadamard codes, decoding.

I. Introduction

In this paper we construct two families $\{C_m^*\}$ and $\{\tilde{C}_m^*\}$ of nonlinear p-ary codes derived from Kronecker powers $H_m = H^{\otimes m}$ of the generalized Butson Hadamard matrix [1] $H=\left(\omega^{(i-1)(j-1)}\right)_{(1\le i,j\le p)}$.

In [2], [3] and [4], the authors introduced a very general construction of cocyclic Hadamard codes derived from Hadamard matrices with entries from a finite abelian group G. this construction requires multiplication of matrices, so we have to work in the group ring RG, where R is a unitary commutative ring.

These codes have nice parameters and very easy encoding and decoding procedures. The main result of the paper is formulated as follows.

Theorem 1. The codes C_m^* and $\tilde{C}_m^*$ are nonlinear p-ary codes with parameters $\left(p^m, p^m, (p-1)p^{m-1}\right)$ and $\left(p^m, p^{m+1}, (p-1)p^{m-1}\right)$, respectively, which meet the Plotkin bound and correct any $t \le \left[\frac{(p-1)p^{m-1}-1}{2}\right]$ errors.

II. Generalized Hadamard Matrices

In this paper we work in the ring $Z[\omega]$ of algebraic integers of $Q(\omega)$. The elements of $Z[\omega]$ are algebraic integers of the form $\alpha = a_0 + a_1\omega + \cdots + a_{p-2}\omega^{p-2}$ Where $a_0, a_1, \cdots, a_{p-2} \in Z$. The ring $Z[\omega]$ contains the multiplicative cyclic group $C=\{1, \omega, \omega^2, \cdots, \omega^{p-1}\}$ of order p with the property that $1+\omega+\omega^2+\cdots+\omega^{p-1}=0$ (1)

If $H=\left(\omega^{(i-1)(j-1)}\right)_{1\le i,j\le p}$ is a generalized Butson-Hadamard matrix, we set $r_{i-1,j-1} \equiv (i-1)(j-1)(\mathrm{mod}\, p)$

$0 \le r_{i-1,j-1} \le p-1$

And write H in the form $H=(\alpha_{ij})_{1\le i,j\le p}$

Where $\alpha_{i,j} = \omega^{r_{i-1,j-1}}$ are elements of the group C, Now we define H^* as the Hermitian transpose of H, or the transpose of $\overline{H} = (\overline{a}_{ij})$, where $\overline{\alpha}_{ij}$ is the complex conjugate of α_{ij} .We observe that $\overline{\alpha}_{ij} = \overline{\omega}^{r_{i-1,j-1}} = \omega^{-r_{i-1,j-1}} = \omega^{p-r_{i-1,j-1}}$, so $\overline{\alpha}_{ij}$ again is an element of C. It is clear, that H and H^* are symmetric complex matrices, which implies $H^* = \overline{H}$. We observe also, that the core $(\overline{\alpha}_{ij})_{2\le i,j\le p}$ of H^* is just a permutation of the core $(\alpha_{ij})_{2\le i,j\le p}$ of the matrix H. Taking into account (1) we obtain $H\cdot H^* = H\cdot \overline{H} = pI$ (2)

Where I is the identity $p\times p$ matrix.

For any integer $m\ge 1$, we define the Kronecker m-th power $H_m = H^{\otimes m}$ of the matrix $H=H_1$ recursively by the relation $H_m = H_1 \otimes H_{m-1}$, Where

$$H_1 \otimes H_{m-1} = \begin{pmatrix} \alpha_{1,1}H_{m-1} & \cdots & \alpha_{1,j}H_{m-1} & \cdots & \alpha_{1,p}H_{m-1} \\ \vdots & & \vdots & & \vdots \\ \alpha_{i,1}H_{m-1} & & \alpha_{i,j}H_{m-1} & & \alpha_{i,p}H_{m-1} \\ \vdots & & \vdots & & \vdots \\ \alpha_{p,1}H_{m-1} & \cdots & \alpha_{p,j}H_{m-1} & \cdots & \alpha_{p,p}H_{m-1} \end{pmatrix}$$

Clearly, H_m is a complex symmetric $p^m \times p^m$ matrix with entries from C. Similarly, if $H_m^* = H_1^* \otimes H_{m-1}^*$ is the Kronecker m-th power of $H^* = H_1^*$, then H_m^* again is a symmetric $p^m \times p^m$ matrix over C, it follows from (2) that $H_m \cdot H_m^* = p^* I_m$, (3) where I_m is the identity $p^m \times p^m$ matrix.

III. Generalized Hadamard Codes

Let H_m^* be the Kronecker m-th power of the Butson-Hadamard matrix H^*. A generalized Hadamard code C_m^*

is defined as the set of all columns of H_m^*. Since H_m^* is a symmetric matrix, the code C_m^* can be also be defined as the set of rows of the matrix H_m^*.

Proposition 2. Any two distinct columns of the matrix H_m^* differ from each other exactly in $(p-1)p^{m-1}$ positions.

Corollary 3. The codes C_m^*, for $m=1,2,\cdots,$ are generalized Hadamard p-ary $\left(p^m, p^m, (p-1)p^{m-1}\right)$ codes which meet the Plotkin bound.

Now we construct a generalized Hadamard code $\tilde{C}_m^*$ as follows. Consider the matrix $\tilde{H}_m = \left(H_m \quad \omega H_m \quad \cdots \quad \omega^{p-1} H_m\right)^t$ And its Hermitian conjugate $\tilde{H}_m^* = \left(H_m^*, \overline{\omega} H_m^* \cdots \overline{\omega}^{p-1} H_m^*\right)$. An ω iterated Hadamard code $\tilde{C}_m^*$ is defined as the set of all columns of the matrix H_m^*. Using the same arguments as above, we arrive at the following result.

Proposition 4. The codes $\tilde{C}_m^*$, for $m=1,2,\cdots,$ are nonlinear p-ary $\left(p^m, p^{m+1}, (p-1)p^{m-1}\right)$ codes which meet the Plotkin bound.

IV. Decoding Algorithm

The codes C_m^* and $\tilde{C}_m^*$, introduced above, admit a highly effective decoding procedure, decoding algorithms for C_m^* and $\tilde{C}_m^*$ are very similar and we restrict ourselves by description of a decoding algorithm for the code C_m^*. Let $H_m = \left(\alpha_{ij}\right)_{1\le i,j\le p^m}$ be the generalized $p^m \times p^m$ Hadamard matrix $\overline{\alpha}_i^\tau = \left(\overline{\alpha}_{i,1}, \cdots, \overline{\alpha}_{i,p^m}\right)^\tau \in C_m^*$ a transmitted code-vector, and $\overline{c}^\tau = \left(\overline{c}^\tau{}_{i,1,\cdots,}\overline{c}^\tau{}_{i,p^m}\right)^\tau$ a received vector that differs from $\overline{\alpha}_i^\tau$ in t positions. We assume that the noisy channel transforms each symbol $\overline{\alpha}$ from the alphabet C to some another symbol $\overline{c}^\tau$ form C with the same small probability.To restore the transmitted vector $\overline{\alpha}_i^\tau$ from received vector $\overline{c}^\tau$ we multiply the matrix H_m by $\overline{c}^\tau$ and then consider the resulting vector $s_i^\tau = H_m \cdot \overline{c}_i^\tau$. Since the entries of H_m and the components of $\overline{\alpha}_i^\tau$ are elements of the cyclic group $C = \left\{1, \omega, \omega^2, \cdots, \omega^{p-1}\right\}$, then resulting vector is a vector of size p^m whose components are elements of $Z[\omega]$ which has a unique representation $s_{ij} = s_{ij}^{(0)} + s_{ij}^{(1)}\omega + s_{ij}^{(2)}\omega^2 + \cdots, s_{ij}^{(p-1)}\omega^{p-1}$ Which coefficients $s_{ij} \in Z$. To correct possible errors we examine the components of the syndrome $s_i^\tau = \left(s_{i,1}, \cdots, s_{i,p^m}^\tau\right)$. If the number of distorted symbols in the received vector is $t \le \left[\frac{d-1}{2}\right] = \left[\frac{(p-1)p^{m-1}-1}{2}\right]$

Then among s_{ij}, $1 \le j \le p^m$, we choose a unique component $s_{i,i}$ whose real part $\mathrm{Re}(s_{i,i})$ is strictly greater than the real part $\mathrm{Re}(s_{i,j})$ of any other component s_{ij}. We notice that if there is no error then the number $s_{i,i}$ is real and has the maximal possible value p^m. Thus we decode the received vector as the transmitted vector $\overline{\alpha}_i^\tau = \left(\overline{\alpha}_{i,1}, \cdots, \overline{\alpha}_{i,p^m}\right)^\tau$. In other words, the received vector $\overline{c}_i$ is decoded as the complex conjugate $\overline{\alpha}_i$ of the i-th row of the Hadamard matrix H^*. As a result, we see that the code C^* corrects any $t \le \left[\frac{d-1}{2}\right] = \left[\frac{(p-1)p^{m-1}-1}{2}\right]$ errors.

Similarly, the ω-iterated Hadamard code $\tilde{C}_m^*$ corrects any $t \le \left[\frac{d-1}{2}\right] = \left[\frac{(p-1)p^{m-1}-1}{2}\right]$ errors.

Reference

[1] A.T. Butson, “ Generalized Hadamard matrices”, Proc, Amer. Math. Soc., vol. 13, pp. 894-898, 1963.
[2] K. J. Horadam and A. A. I. Perera , “ Codes from cocycles”, in Proc. AAECC-12, Lecture Notes in Computer Sciences, vol. 1255, pp. 151-163, Springer Verlog, Berlin, 1997.
[3] K. J. Haradam and P. Udaya, “Cocyclic Hadamard codes, IEEE Trans. Inform. Theory, vol. 44, no. 4, pp. 1545-1550.
[4] Wen Ping Ma, Moon Ho Lee, “ Complex hadamard codes”, IEICE Trans. Fundamentals, vol. E88-A, No. 1, pp. 396-398.

Acknowledgement

This work was partial supported by KOTEF (Ministry of Commerce, Industry and Energy)