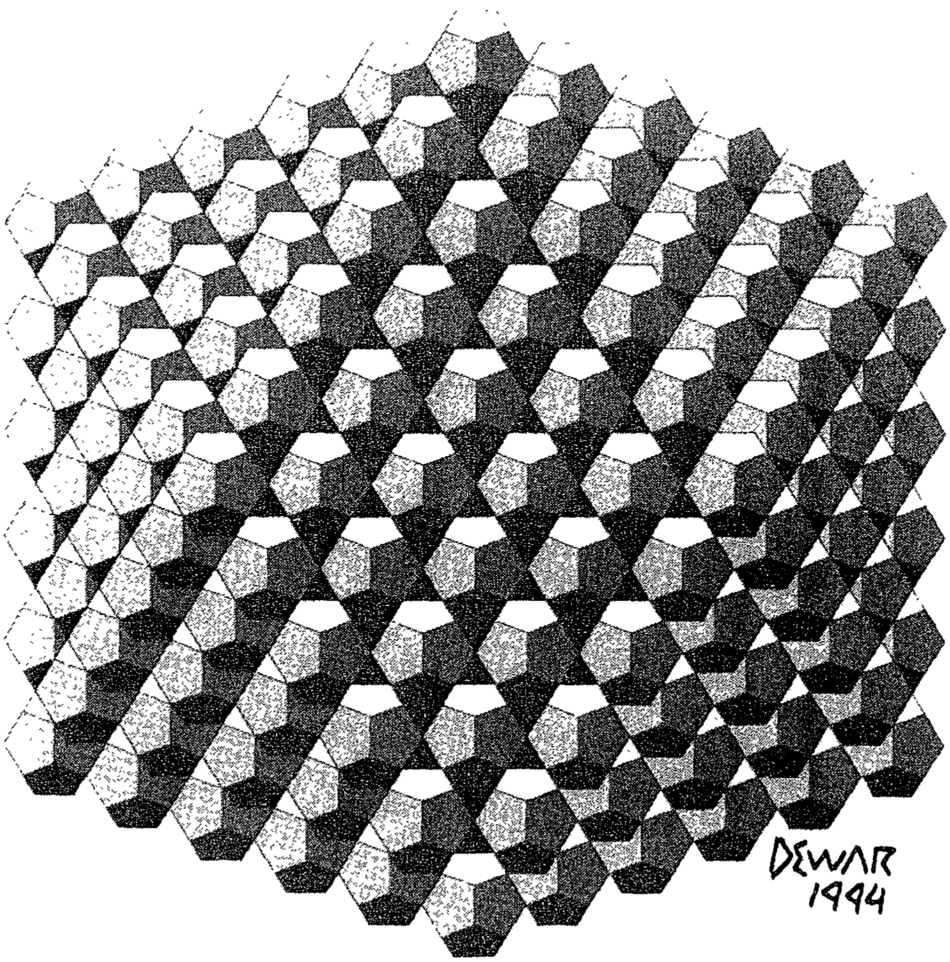
Symmetry: Culture and Science

Symmetry: Natural and Artificial, 3

The Quarterly of the
International Society for the
Interdisciplinary Study of Symmetry
(ISIS-Symmetry)

Editors:
György Darvas and Dénes Nagy

Volume 6, Number 3, 1995



Third Interdisciplinary Symmetry Congress and Exhibition
Washington, D.C., U.S.A. August 14 - 20, 1995

BINARY BLOCK CODE WHICH COMPOSES 16 DIMENSIONAL HYPER REGULAR POLYHEDRON AND A CLASS OF GENERALIZED HADAMARD MATRICES EACH OF WHICH IS A CUBIC ROOT FOR THE UNIT MATRIX

Naoki Suehiro
Institute of Applied Physics, University of Tsukuba
1-1-1 Tennoudai, Tsukuba, Ibaraki 305, Japan
e-mail suehiro@hermes.bk.tsukuba.ac.jp
fax +81-298-53-5205

Abstract. A class of hyper regular polyhedron in 16 dimensional Euclid space is introduced as a class of binary block codes of length 16. Each code has 256 codewords. The minimum Euclid distance in the proposed code is $2\sqrt{6}$. The 256 codewords compose a regular hyperpolyhedron in the 16 dimensional signal space.

A class of generalized Hadamard matrices (polyphase matrices), each of which is a cubic root for the unit matrix, are also reviewed.

1 Introduction

Binary code, which composes hyper regular polyhedron in 16 dimensional Euclid space, had been discovered for the first by Nordostrom and Robinson as Nordostrom-Robinson Code[5]. It had been discovered for the second by Suehiro in 1991[6] as a class of binary codes derived from even-shift orthogonal sequences. It also has been discovered for the third by Hammons, Kumar, Calderbank, Sloane and Sole in 1992[7] as another class of binary codes derived from a class of four phase sequences. All of these codes have different correlation property each other as sequences. This paper discuss on the second class of codes proposed by the author.

Hatori, et.al.[1] defined and searched "even-shift orthogonal sequences." A binary sequence, whose elements are 1 or -1, is called an even-shift orthogonal sequence, when every even-shift term in the autocorrelation function is 0 except the 0-shift term. (The concept of even-shift orthogonal sequences has been generalized by Suehiro, et. al.[3] as N-shift cross-orthogonal sequences.) Hatori, et.al. found 192 even-shift orthogonal sequenced of length 16 by computer search.

Suehiro et.al. discovered that the set of 192 even-shift orthogonal sequence divided into two sets, each of which containes 96 even-shift orthogonal sequences with minimum Hamming distance 6.

Suehiro et.al.[4] also discovered a class of Hadamard matrices, all of whose rows are even-shift orthogonal sequences. Let $N = 4^n$, and H be a Sylvester type $N \times N$ Hadamard matrix, and λ be an $N \times N$ diagonal matrix whose diagonal elements correspond an even-shift orthogonal sequences. Then it can be proved that all rows in a matrix $H\lambda$ are even-shift oethogonal sequences.

2 A Class of Binary Block Codes of Length 16 which Compose 16 Dimensional Hyper Regular Polyhedron

Let 16 × 16 dimensional Sylvester type Hadamard matrix B be defined as

$$B = \frac{1}{\sqrt{2}}\begin{bmatrix} + & + \\ + & - \end{bmatrix} \otimes \frac{1}{\sqrt{2}}\begin{bmatrix} + & + \\ + & - \end{bmatrix} \otimes \frac{1}{\sqrt{2}}\begin{bmatrix} + & + \\ + & - \end{bmatrix} \otimes \frac{1}{\sqrt{2}}\begin{bmatrix} + & + \\ + & - \end{bmatrix},$$

where + denotes 1, − denotes −1, and $\otimes$ denotes Cronecker product.

Let even-shift orthogonal sequences of length 16 $\mathbf{S}_1$, $\mathbf{S}_2$ and $\mathbf{S}_3$ be defined as

$${}^t\mathbf{S}_1 = (+ - - + + - + - + + - - - - - -)$$
$${}^t\mathbf{S}_2 = (+ - + - + + - - - + + - - - - -)$$
$${}^t\mathbf{S}_3 = (+ - + + - + - - + - - - + - - -)$$

where ${}^t\mathbf{S}_1$ denotes transposed $\mathbf{S}_1$, so that each Hamming distance is 6. Let a 16 × 16 dimensional diagonal matrix Λ_{S_1} be also defined that the connected diagonal elements in the diagonal matrix compose the binary vector $\mathbf{S}_1$. 16 × 16 dimensional diagonal matrices Λ_{S_2} and Λ_{S_3} are defined similarly.

Let 16 dimensional vectors $\mathbf{T}_1$, $\mathbf{T}_2$ and $\mathbf{T}_3$ be defined as

$$\mathbf{T}_1 = B\mathbf{S}_1,\ \mathbf{T}_2 = B\mathbf{S}_2,\ \mathbf{T}_3 = B\mathbf{S}_3$$

where B is the 16 dimensional Sylvester type Hadamard matrix. Then

$${}^t\mathbf{T}_1 = (- + + + + - + + + + - + - - - +)$$
$${}^t\mathbf{T}_2 = (- + + - + + - - + + + + - + - +)$$
$${}^t\mathbf{T}_3 = (- + + + + + - + + - - - + + - +).$$

We can say $\mathbf{S}_1$, $\mathbf{S}_2$ and $\mathbf{S}_3$ are "white for B", because all elements in $B\mathbf{S}_1$, $B\mathbf{S}_2$ and $B\mathbf{S}_3$ have the same absolute value. Farthermore, since $B^2 = I$, $\mathbf{S}_1 = B\mathbf{T}_1$, $\mathbf{S}_2 = B\mathbf{T}_2$ and $\mathbf{S}_3 = B\mathbf{T}_3$. So, $\mathbf{T}_1$, $\mathbf{T}_2$ and $\mathbf{T}_3$ are also white for B. Thus, it has been shown that $\mathbf{S}_1, \mathbf{S}_2, \mathbf{S}_3, \mathbf{T}_1, \mathbf{T}_2$ and $\mathbf{T}_3$ are binary vectors which are white for B.

Let $\mathbf{U}_1$ be defined as

$${}^t\mathbf{U}_1 = (- - - + - + + + - + + + + + + -).$$

$\mathbf{U}_1$ is obtained from $\mathbf{S}_1$, $\mathbf{S}_2$, $\mathbf{S}_3$, $\mathbf{T}_1$, $\mathbf{T}_2$ and $\mathbf{T}_3$ by multiplying corresponding elements. For example, the first element in $\mathbf{U}_1$ is obtained by multiplying the first elements in these

6 vectors as

$$-1 = 1 \times 1 \times 1 \times (-1) \times (-1) \times (-1).$$

It can be shown by computing that all rows in $B\Lambda_{S_1}$, $B\Lambda_{S_2}$, $B\Lambda_{S_3}$, $B\Lambda_{T_1}$, $B\Lambda_{T_2}$, $B\Lambda_{T_3}$ and $B\Lambda_{U_1}$ are binary vectors which are white for B, where $\Lambda_{T_1}, \Lambda_{T_2}, \Lambda_{T_3}$ and Λ_{U_1} are defined similarly as Λ_{S_1}.

We can make a new binary block code composed of all rows in $B\Lambda_{S_1}$, $-B\Lambda_{S_1}$, $B\Lambda_{S_2}$, $-B\Lambda_{S_2}$, $B\Lambda_{S_3}$, $-B\Lambda_{S_3}$, $B\Lambda_{T_1}$, $-B\Lambda_{T_1}$, $B\Lambda_{T_2}$, $-B\Lambda_{T_2}$, $B\Lambda_{T_3}$, $-B\Lambda_{T_3}$, $B\Lambda_{U_1}$, $-B\Lambda_{U_1}$, B and $-B$. All words in this binary block code are length 16. The number of this code is 256. Each of 32 words obtained from B and $-B$ is transformed into a pulse by B. The remained 224 words are white for B. The minimum Euclid distance in this code is $2\sqrt{6}$.

We can make another code of the same property from the remained 96 even-shift orthogonal sequences similarly.

3 A Class of Polyphase Matrices, each of which is a Cubic Root for the Unit Matrix

A class of polyphase matrices, each of which is a cubic root for the unit mtrix, has been proposed[2]. In this section, the theory is reviewed.

Let m and n be natural numbers. N is defined as $N = m^n$. Let i, i_0, i_1, j, j_0 and j_1 be integers, where

$$0 \le i \le N^2 - 1,\ 0 \le i_0 \le N - 1,\ 0 \le i_1 \le N - 1$$
$$0 \le j \le N^2 - 1,\ 0 \le j_0 \le N - 1,\ 0 \le j_1 \le N - 1$$
$$i = i_0 N + i_1,\ j = j_0 N + j_1.$$

$\mathbf{i}_0$ is defined as

$$\mathbf{i}_0 = (i_{00}, i_{01}, ..., i_{0(n-1)}),$$

where

$$i_0 = i_{00} m^{n-1} + i_{01} m^{n-2} + ... + i_{0(n-1)} m^0,\quad 0 \le i_{0k} \le m - 1.$$

$\mathbf{i}_1, \mathbf{j}_0$ and $\mathbf{j}_1$ are defined similarly. Let H be an $N^2 \times N^2$ matrix, where

$$\begin{aligned} H &= [h(i,j)]\ , \\ h(i,j) &= \frac{1}{N} \exp\{\frac{2\pi\sqrt{-1}}{m}(\mathbf{i}_1\mathbf{j}_0^* + \mathbf{i}_0\mathbf{j}_1^* + \mathbf{j}_0\mathbf{j}_1^*)\}\ , \end{aligned}$$

[Theorem 1]

$$H^3 = I$$

where I is a unit matrix, and $\mathbf{i}_1\mathbf{j}_0^*$ is the inner product between $\mathbf{i}_1$ and $\mathbf{j}_0$.

4 Acknowledgement

The author wish to thank Prof. Mitsutoshi Hatori and Prof. Noriyoshi Kuroyanagi, who encouraged this work. The author also wish to thank Dr. Tsutomu Kawabata who discussed with me about this work.

The author also wish to thank SCAT (Support Center for Advanced Telecommunications Technology Research) for the research fund.

References

[1] Y.Taki, H.Miyakawa, M.Hatori and S.Namba, "Even-shift orthogonal sequences," IEEE Trans. on Information Theory, vol. IT-15, pp.295-300,(1969).

[2] N.Suehiro, "Complete complementary codes derived from cubic roots of unit matrices," Trans. of IECE (presently IEICE, in Japanese), vol. J66-A, pp.486-491,(1983).

[3] N.Suehiro and M.Hatori, "N-shift cross-orthogonal sequences," IEEE Trans. on Information Theory, vol. IT-34, pp.143-146,(1988).

[4] N.Suehiro and M.Hatori, "Even-shift orthogonal sequences compose Hadamard matrices which are cubic roots for unity," Technical Report of IEICE, vol. SS88-22, pp.32-35,(1988).

[5] A.E.Brouwer, James B.Shearer, N.J.A.Slone, and Warren D.Smith, "A new table of constant weight codes," IEEE Trans. on Information Theory, vol. IT-36, pp.1334-1380,(1990).

[6] N.Suehiro, "Binary block code whose words are white or pure colour for an Hadamard transform," Technical Report of IEICE, vol. IT91-72, pp.21-26,(1991).

[7] A.R.Hammons,Jr., P.V.Kumar, A.R.Calderbank, N.J.A.Sloane and P.Sole, "The Z_4 Linearity of Kerdock, Preparata, Goethals and Related Codes," (1993)