Ternary Codes from Modified Jacket Matrices

Xueqin Jiang, Moon Ho Lee, Ying Guo, Yier Yan and Sarker Md. Abdul Latif

Abstract: **In this paper, we construct two families C_m^* and $\tilde{C}_m^*$ of ternary $(2^m, 3^m, 2^{m-1})$ and $(2^m, 3^{m+1}, 2^{m-1})$ codes, for $m = 1, 2, 3, \cdots$, derived from the corresponding families of modified ternary Jacket matrices. These codes are close to the Plotkin bound and have a very easy decoding procedure.**

Index Terms: **Algebraic integers, cyclotomic fields, Jacket codes, Kronecker products of matrices, modified ternary, modified ternary Jacket matrices.**

I. INTRODUCTION

Many discrete signal transforms are based on the use of transform matrices with entries on the complex circle, such as the family of discrete generalized transforms (DGT) for signals of length $n = 2^m$ [1, 10.2]. This family includes the Walsh-Hadamard transform (WHT) and the 2^m-point discrete Fourier transform (DFT). Interpretation of the Cooley-Turkey fast Fourier transform (FFT) in terms characters of abelian groups [2], [3] means that the DFT is itself a generalized transform which includes the WHT. Both of the WHT and DFT are suboptimal discrete orthogonal transforms, but each has wide application.

The above transform matrices belong to the more general matrices, Jacket matrices, which are motivated by the center weighted Hadamard matrices [4]. In a general definition, any square matrix $[J] = [j_{s,t}]_{n\times n}$ is called a Jacket matrix if its inverse matrix is obtained simply by an element-wise inverse [5]–[7], namely,

$$[J]^{-1} = \frac{1}{c}\left[\frac{1}{j_{s,t}}\right]^T_{n\times n}$$

for $1 \leq s, t \leq n$ where T denotes the transpose of the matrix, c is the normalized constant. The cyclic function on Jacket matrices will be help in signal processing [8], sequence design, cryptography [9], and quantum information [7].

In this paper, we consider two families $\{M_m\}$ and $\{\tilde{M}_m\}$ of modified ternary Jacket matrices and construct the corresponding families $\{C_m^*\}$ and $\{\tilde{C}_m^*\}$ of nonlinear ternary codes C_m^* and $\tilde{C}_m^*$, derived from the matrices M_m and $\tilde{M}_m$, respectively. The parameters of these codes are described as follows.

Theorem 1: The ternary codes C_m^* and $\tilde{C}_m^*$ have parameters

$$(2^m, 3^m, 2^{m-1}) \text{ and } (2^m, 3^{m+1}, 2^{m-1})$$

respectively, and correct $t \leq \left[\frac{2^{m-1}-1}{2}\right]$ errors.

The rest of this paper is organized as follows. In Section II, we will introduce a family of modified Jacket matrix. In Section III, we introduce two families $\{C_m^*\}$ and $\{\tilde{C}_m^*\}$ of nonlinear p-ary codes. Section IV introduces the encoding procedure and Section V introduces the decoding algorithm. In Section VI, we give an example of a ternary Jacket code. Finally, Section V concludes the paper.

II. MODIFIED TERNARY JACKET MATRICES

Let $\omega = e^{2\pi i/3}$ be a primitive cubic root of unity, and $Q(\omega)$ the cyclotomic field obtained from the field of rational numbers Q by enjoining of ω. The field $Q(\omega)$ is a quadratic extension of Q, and the minimal polynomial of ω over Q is

$$f(x) = x^2 + x + 1. \tag{1}$$

The elements $1, \omega$ form a basis of $Q(i)$ over Q, so any $\alpha \in Q(\omega)$ can be uniquely written as a linear combination $\alpha = a + b\omega$ of the basis elements 1 and ω with coefficients $a, b \in Q$.

Let Z be the ring of rational integers. In this paper, we work in the ring $Z[\omega]$ of algebraic integers of $Q(i)$. The elements of $Z[\omega]$ are algebraic integers of the form $\alpha = a + b\omega$, where $a, b \in Z$. The ring $Z[\omega]$ contains the multiplicative cyclic group $G = \{1, \omega, \omega^2\}$ of order 3.

Consider the Jacket matrix

$$J = \begin{pmatrix} 1 & 1 & 1 \\ 1 & \omega & \omega^2 \\ 1 & \omega^2 & \omega \end{pmatrix} \tag{2}$$

and then use the elements of J to compose a new matrix M_1 as follows

$$M_1 = \begin{pmatrix} 1 & 1 \\ 1 & \omega \\ \omega & 1 \end{pmatrix}. \tag{3}$$

The Jacket matrix J in (2) is a square and symmetric matrix and $JJ^* = nI$ where J^* is the Hermite transpose of J. We extend this property to a new nonsquare and nonsymmetric matrix M_1. M_1 is similar to J in many aspects which will be shown by (10) and property 2.1. However, M_1 is not a Jacket matrix. It is a matrix obtained from the Jacket matrix in (2).

We define a modified ternary matrices M_m and $\tilde{M}_m$, for $m = 2, 3, \cdots$, respectively by the relations

$$M_m = M_1 \otimes M_{m-1} = \begin{pmatrix} M_{m-1} & M_{m-1} \\ M_{m-1} & \omega M_{m-1} \\ \omega M_{m-1} & M_{m-1} \end{pmatrix} \tag{4}$$

Manuscript received September 26, 2009; approved for publication by Emanuele Viterbo, Division I Editor, August 10, 2010.

This work was supported by World Class University R32-2008-000-20014-0 NRF, Korea.

X. Jiang is with the School of Information Science and Technology of Donghua University, China, email: xqjiang@dhu.edu.cn.

M. Lee is with the Division of Electronic and Information Engineering of Chonbuk National University, Korea, email: moonho@jbnu.ac.kr.

Y. Guo is with the Central South University, China, email: yingguo@mail.csu.edu.cn.

Y. Yan is with School of Mechanical and Electrical Engineering of Guangzhou University, China, email: year0080@gzhu.edu.cn.

S. M. A. Latif is with the Electronics Engineering from Chonbuk National University, Korea, email: latifsarker@gmail.com.

1229-2370/11/$10.00 © 2011 KICS

and

$$\tilde{M}_m = \begin{pmatrix} M_m \\ \omega M_m \\ \omega^2 M_m \end{pmatrix}. \quad (5)$$

Clearly, M_m and $\tilde{M}_m$ are $3^m \times 2^m$ and $3^{m+1} \times 2^m$ matrices, respectively, with entries from the cyclic group $G = <\omega>$. If

$$M_1^* = \begin{pmatrix} 1 & 1 & \omega^2 \\ 1 & \omega^2 & 1 \end{pmatrix} \quad (6)$$

is the Hermite transpose of M_1, we set

$$D_1 = M_1 M_1^* = \begin{pmatrix} 2 & 1+\omega^2 & 1+\omega^2 \\ 1+\omega & 2 & \omega+\omega^2 \\ 1+\omega & \omega+\omega^2 & 2 \end{pmatrix}. \quad (7)$$

Taking into account that $1+\omega+\omega^2 = 0$, we can rewrite D_1 in the form

$$D_1 = \begin{pmatrix} 2 & -\omega & -\omega \\ \omega^2 & 2 & -1 \\ -\omega^2 & -1 & 2 \end{pmatrix}. \quad (8)$$

It is easy to see that D_1 is a self-conjugate complex matrix, that is $D_1^* = D_1$.

Finally, we defined complex self-conjugate matrices D_m, for $m = 2, 3, \cdots$, recursively by

$$\begin{aligned} D_m &= D_1 \otimes D_{m-1} \\ &= \begin{pmatrix} 2D_{m-1} & -\omega D_{m-1} & -\omega D_{m-1} \\ -\omega^2 D_{m-1} & 2D_{m-1} & -D_{m-1} \\ -\omega^2 D_{m-1} & -D_{m-1} & 2D_{m-1} \end{pmatrix}. \end{aligned} \quad (9)$$

Since $M_1 M_1^* = D_1$, it follows that

$$M_m M_m^* = D_m. \quad (10)$$

The last relation show that the matrices M_m, for $m = 1, 2, \cdots$, do not fall into the class of Jacket matrices. On the other hand, it is easy to see, using induction on m, that the following holds.

Proposition 1: Let $D_m = (\theta_{kl})$. For any $m \geq 1$ we have $D_m^* = D_m$. The entries $\theta_{kl} = a_{kl} + b_{kl}\omega$ of D_m are algebraic integers form the ring $Z[\omega]$. The diagonal elements $\theta_{k,k}$ of D_m all are equal to 2^m, and the first coefficients a_{kl} of the entries θ_{kl} lying outside of the diagonal do not exceed 2^{m-1}.

The above Proposition and relations (10) show that the modified matrices M_m in many aspects are very similar to the corresponding Jacket matrices. This fact provides a very easy and sufficiently fast decoding algorithm for the codes C_m^* and $\tilde{C}_m^*$, described below in Section IV.

III. MODIFIED TERNARY JACKET CODES

Let M_m and $\tilde{M}_m$ be modified ternary Jacket matrices defined as above. A modified ternary Jacket code C_m^* is defined as the set of all columns of the Hermite transpose M_m^* of M_m. The columns of M_m^* can be indexed by the integers from 0 to $3^m - 1$. Similarly, a modified ternary Jacket code $\tilde{C}_m^*$ is the set of all columns of the Hermitian transpose $\tilde{M}_m^*$ of the matrix $\tilde{M}_m$. The columns of $\tilde{M}_m^*$ can be indexed by the integers from 0 to $3^{m+1} - 1$. It is clear that C_m^* and $\tilde{C}_m^*$ are nonlinear $(2^m, 3^m, d)$ and $(2^m, 3^{m+1}, d)$ codes, respectively. Let us find the minimum Hamming distances d of the codes C_m^* and $\tilde{C}_m^*$.

Theorem 2: The minimal Hamming distances d of the codes C_m^* and $\tilde{C}_m^*$ is equal to 2^{m-1}.

Proof: It is clear that the minimal Hamming distance of C_m^* and $\tilde{C}_m^*$ are equal to the minimum distance between distinct rows of the matrices M_m and $\tilde{M}_m$, respectively.

To prove that this minimal distance is 2^{m-1}, we use induction in m. The statement is clearly true for $m = 1$. Let now $m \geq 2$. Suppose that the minimum Hamming distance between distinct rows of M_{m-1} is equal to 2^{m-2} and prove that the minimum Hamming distance between distinct rows of M_m equals 2^{m-1}. Write

$$M_m = \begin{pmatrix} M_{m-1} & M_{m-1} \\ M_{m-1} & \omega M_{m-1} \\ \omega M_{m-1} & M_{m-1} \end{pmatrix}$$

and consider the following submatrices

$$M^{(1,1)} = (M_{m-1}\, M_{m-1}), \; M^{(1,\omega)} = (M_{m-1}\, \omega M_{m-1})$$

and

$$M^{(\omega,1)} = (\omega M_{m-1}, M_{m-1})$$

of the matrix M_m. By the induction hypothesis, the minimum distance between distinct rows of M_{m-1} is equal to 2^{m-2}. Consider the matrix M_{m-1} as an ordered set of its rows. If (a_k, a_k) and (a_l, a_l) are two distinct rows of $M_{m-1}(1,1)$, then the Hamming distance between (a_k, a_k) and (a_l, a_l) equals $d(a_k, a_l) + d(a_k, a_l)$ where $d(a_k, a_l)$ is the Hamming distance between two distinct rows a_k and a_l of the matrix M_{m-1}. This shows that the minimum Hamming distance between distinct rows of $M_{m-1}^{(1,1)}$ is equal to 2^{m-1}. Similarly, the minimum Hamming distance between distinct rows of each matrix $M^{(1,\omega)}$ and $M^{(\omega,1)}$ is equal to 2^{m-1}. Now we proceed as follows.

(i) First we show that the minimum Hamming distance between any two rows of the submatrices $M_{m-1}^{(1,1)}$ and $M_{m-1}^{(1,\omega)}$ is at least 2^{m-1}. Let (a_k, a_k) and $(a_l, \omega a_l)$ be two arbitrary rows of $M_{m-1}^{(1,1)}$ and $M_{m-1}^{(1,\omega)}$, respectively. If $l = k$, then the Hamming distance between (a_k, a_k) and $(a_l, \omega a_l)$ is at least 2^{m-1}. Let now $l \neq k$. The Hamming distance between (a_k, a_k) and $(a_l, \omega a_l)$ equals $d(a_k, a_l) + d(a_k, \omega a_l)$. Using the triangle inequality

$$d(a_l, \omega a_l) \leq d(a_l, a_k) + d(a_k, \omega a_l)$$

we find that the Hamming distance between (a_k, a_k) and $(a_l, \omega a_l)$ is at least $d(a_l, \omega a_l) = 2^{m-1}$. Thus, the minimum Hamming distance between any two rows of $M_{m-1}^{(1,1)}$, respectively, is at least 2^{m-1}. Similarly, the minimum Hamming distance between the rows of $M_{m-1}^{(1,1)}$ and $M_{m-1}^{(\omega,1)}$, respectively, is at least $2^m - 1$.

(ii) Now we prove that the minimum Hamming distance between any two rows of the submatrices $M_{m-1}^{(1,\omega)}$ and $M_{m-1}^{(\omega,1)}$ again is at least 2^{m-1}. Consider two arbitrary elements $(a_k, \omega a_k) \in M_{m-1}^{(1,\omega)}$ and $(\omega a_l, a_l) \in M_{m-1}^{(\omega,1)}$. If $l = k$ then the Hamming distance between $(a_k, \omega a_k)$ and $(\omega a_l, a_l)$ is at least 2^{m-1}. If $l \neq k$, we have

$$d(\omega a_l, a_l) \leq d(\omega a_l, a_k) + d(a_k, \omega a_l)$$

and since $d(\omega a_l, a_k) = d(a_k, \omega a_l)$ and $d(a_k, \omega a_l) = d(\omega a_k, a_l)$ then

$$d(\omega a_l, a_l) \leq d(a_k, \omega a_l) + d(\omega a_k, a_l).$$

Thus, the Hamming distance between $(a_k, \omega a_k)$ and $(\omega a_l, a_l)$ is at least

$$d(\omega a_l, a_l) = 2^{m-1}.$$

This completes the proof. □

Corollary 1: The nonlinear ternary codes C_m^* and $\tilde{C}_m^*$ have parameters $(2^m, 3^m, 2^{m-1})$ and $(2^m, 3^{m+1}, 2^{m-1})$, respectively.

IV. ENCODING ALGORITHM

If we would like to transmit symbols 0, 1, and 2, we can transform these symbols to $1, \omega$, and ω^2 using the following one-to-one map

$$b_k = \omega^{i_k}. \tag{11}$$

In fact, the multiplicative cyclic group $G = \{1, \omega, \omega^2\}$ of order 3 is isomorphic to the set $\{0, 1, 2\}$ with modulo 3. Each modified ternary Jacket code C_m^* carries m symbols of information. Given the input information sequence $(i_0, i_1, \cdots, i_{(m-1)})$ where $i_k \in \{0, 1, 2\}$, for $k = 0, 1, \cdots, m-1$. We obtain $(b_0, b_1, \cdots, b_{(m-1)})$ from the one-to-one map (11). The encoding procedure of C_m^* includes two steps:

Given b_0, calculate a_0^τ with the fomular

$$a_0^\tau = \begin{cases} (1, b_0^2)^\tau, & b_0 \in \{1, \omega\} \\ (\omega^2, 1)^\tau, & b_0 = \omega^2 \end{cases} \tag{12}$$

and calculate $a_{(k)}^\tau$ from $a_{(k-1)}^\tau$ recursively with the formula

$$a_{(k+1)}^\tau = \begin{cases} \left(a_k, b_{(k+1)}^2 a_k\right)^\tau, & b_{(k+1)} \in \{1, \omega\} \\ \left(\omega^2 a_k, a_k\right)^\tau, & b_{(k+1)} = \omega^2 \end{cases} \tag{13}$$

where τ denotes the transpose of a vector. Actually, given the information sequence $(i_0, i_1, \cdots, i_{m-1})$, the result code-vector $a_{(m-1)}^\tau \in C_m^*$ is the ith column of M_m^* where $i = i_0 + i_1 3 + \cdots + i_{(m-1)} 3^{m-1}$.

Let us illustrate the encoding process by using an example. Assume $m = 2$ and the information sequence is $(i_0, i_1) = (0, 2)$. From (3) and (4), we have the following ternary matrix

$$M_2 = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & \omega & 1 & \omega \\ \omega & 1 & \omega & 1 \\ 1 & 1 & \omega & \omega \\ 1 & \omega & \omega & \omega^2 \\ \omega & 1 & \omega^2 & \omega \\ \omega & \omega & 1 & 1 \\ \omega & \omega^2 & 1 & \omega \\ \omega^2 & \omega & \omega & 1 \end{pmatrix}$$

and its Hermitian transpose

$$M_2^* = \begin{pmatrix} 1 & 1 & \omega^2 & 1 & 1 & \omega^2 & \omega^2 & \omega^2 & \omega \\ 1 & \omega^2 & 1 & 1 & \omega^2 & 1 & \omega^2 & \omega & \omega^2 \\ 1 & 1 & \omega^2 & \omega^2 & \omega^2 & \omega & 1 & 1 & \omega^2 \\ 1 & \omega^2 & 1 & \omega^2 & \omega & \omega^2 & 1 & \omega^2 & 1 \end{pmatrix}.$$

From (11), we get $(b_0, b_1) = (1, \omega^2)$. With (12) and $b_0 = 1$, we get $a_0 = (1, 1)$. Then, with (13) and $b_1 = \omega^2$, $a_0 = (1, 1)$, we get the finally code word $a_1 = (\omega^2, \omega^2, 1, 1)$. Actually, from $i = i_0 + i_1 3 = 6$, we can also see that the final code word is the 6th column of M_2^*, which confirms our encoding algorithm.

Each modified ternary Jacket code $\tilde{C}_m^*$ carries $(m+1)$ symbols of information. Given the input information sequence $(b_0, b_1, \cdots, b_{(m-1)}, b_m)$ where $b_i \in \{1, \omega, \omega^2\}$, for $i = 0, 1, \cdots, m$. The encoding procedure of $\tilde{C}_m^*$ includes two steps. First, code-vector $a_{(m-1)}^\tau$ can be obtained recursively based on (12) and (13). Second, the code-vector $a_m^\tau \in \tilde{C}_m^*$ can be obtained by

$$a_m^\tau = \bar{b}_m a_{(m-1)}^\tau \tag{14}$$

where $\bar{b}_m$ is the complex conjugate of b_m. Then, the result code-vector $a_m^\tau \in \tilde{C}_m^*$ is the ith column of $\tilde{M}_m^*$ where $i = i_0 + i_1 3 + \cdots + i_{(m-1)} 3^{m-1} + i_m 3^m$.

V. DECODING ALGORITHM

The codes C_m^* and $\tilde{C}_m^*$ admit an effective decoding procedure. Decoding algorithms for C_m^* and $\tilde{C}_m^*$ are very similar and we restrict ourselves by description of the decoding algorithm for the code C_m^*. Let $M_m = (a_{i,j})$, $1 \leq i \leq 3^m$, $1 \leq j \leq 2^m$ be a modified $3^m \times 2^m$ Jacket matrix, a transmitted code-vector $\bar{a}_i^\tau = (\bar{a}_{i,1}, \cdots, \bar{a}_{i,2^m})^\tau \in C_m^*$, and a received vector $\bar{c}_i^\tau = (\bar{c}_{i,1}, \cdots, \bar{c}_{i,2^m})$ that differs from $\bar{a}_i^\tau$ in t positions. We assume that the noisy channel can transform each symbol $\bar{a}_{i,j}$ from the alphabet $G = \{1, \omega, \omega^2\}$ to some another symbol $\bar{c}_{i,j}$ from G with the same small probability p^* and leaves $\bar{a}_{i,j}$ fixed with probability $1 - p^*$.

To restore the transmitted vector $\bar{a}_i^\tau$ from received vector $\bar{c}_i^\tau$, there are three steps in the decoding process. First, we multiply the matrix M_m by $\bar{c}_i^\tau$ and then resulting vectors $s^\tau = M_m \bar{c}_i^\tau$. Since the entries of M_m and the components of $\bar{a}_i^\tau$ are elements of the cyclic group $G = \{1, \omega, \omega^2\}$, the resulting vector $s^\tau = (s_1, \cdots, s_{3^m})^\tau$ is a vector of size 3^m, whose components s_k, for $1 \leq k \leq 3^m$, are elements of the ring $Z[\omega]$. This means that each component s_k is a linear combination

$$s_k = s_k^{(0)} + s_k^{(1)} \omega$$

of elements 1 and ω with coefficients $s_k^{(0)}, s_k^{(1)} \in Z$.

Secondly, to correct possible errors we example the components of the syndrome $s^\tau = (s_1, \cdots, s_{3^m})^\tau$. If the number of distorted symbols in the received vector is

$$t \leq \left[\frac{d-1}{2}\right] = \left[\frac{2^{m-1}-1}{2}\right]$$

then among the components s_k, $1 \leq k \leq 3^m$, of the vector s, we choose the unique one s_i whose first coefficient $s_i^{(0)}$ is strictly greater than the first coefficient of any other component s_k of s. We notice that if no error occurs then $s_i \in Z$ and s_i has the maximal possible value 3^m.

Thirdly, we decode $\bar{c}_i^\tau$ as the transmitted vector $\bar{a}_i^\tau = (\bar{a}_{i,1}, \cdots, \bar{a}_{i,2^m})^\tau$. In other words, the received vector $\bar{c}_i$ is decoded as the complex conjugate $\bar{a}_i$ of the ith row of the modified ternary Jacket matrix M_m. Then, the input information sequence is $(i_0, i_1, \cdots, i_{(m-1)})$ where $i = i_0 + i_1 3 + \cdots + i_{(m-1)} 3^{m-1}$. The decoding process is finished. It is clear that the code C_m^* corrects $t \leq \left[\frac{d-1}{2}\right] = \left[\frac{2^{m-1}-1}{2}\right]$ errors.

Similarly, the code $\tilde{C}_m$ with parameters $(2^m, 3^{m+1}, 2^{m-1})$ also corrects any $t \leq \left[\frac{2^{m-1}-1}{2}\right]$ errors.

VI. AN EXAMPLE

Again, we consider the matrix M_2 and its Hermitian transpose M_2^*.

In view of (10), we have

$$M_2 M_2^* = D_2$$

where D_2 is shown at the top of next page.

Let now

$$M_3 = \begin{pmatrix} M_2 & M_2 \\ M_2 & \omega M_2 \\ \omega M_2 & M_2 \end{pmatrix}, M_3^* = \begin{pmatrix} M_2^* & M_2^* & \omega^2 M_2^* \\ M_2^* & \omega^2 M_2^* & M_2^* \end{pmatrix}$$

and

$$D_3^* = \begin{pmatrix} 2M_2 & -\omega M_2 & -\omega M_2 \\ -\omega^2 M_2 & 2M_2 & -M_2 \\ -\omega^2 M_2 & -M_2 & 2M_2 \end{pmatrix}$$

so that

$$M_3 M_3^* = D_3$$

and then we have the following 27×8 matrix

$$M_3 = \begin{pmatrix}
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
1 & \omega & 1 & \omega & 1 & \omega & 1 & \omega \\
\omega & 1 & \omega & 1 & \omega & 1 & \omega & 1 \\
1 & 1 & \omega & \omega & 1 & 1 & \omega & \omega \\
1 & \omega & \omega & \omega^2 & 1 & \omega & \omega & \omega^2 \\
\omega & 1 & \omega^2 & \omega & \omega & 1 & \omega^2 & \omega \\
\omega & \omega & 1 & 1 & \omega & \omega & 1 & 1 \\
\omega & \omega^2 & 1 & \omega & \omega & \omega^2 & 1 & \omega \\
\omega^2 & \omega & \omega & 1 & \omega^2 & \omega & \omega & 1 \\
1 & 1 & 1 & 1 & \omega & \omega & \omega & \omega \\
1 & \omega & 1 & \omega & \omega & \omega^2 & \omega & \omega^2 \\
\omega & 1 & \omega & 1 & \omega^2 & \omega & \omega^2 & \omega \\
1 & 1 & \omega & \omega & \omega & \omega & \omega^2 & \omega^2 \\
1 & \omega & \omega & \omega^2 & \omega & \omega^2 & \omega^2 & 1 \\
\omega & 1 & \omega^2 & \omega & \omega^2 & \omega & 1 & \omega^2 \\
\omega & \omega & 1 & 1 & \omega^2 & \omega^2 & \omega & \omega \\
\omega & \omega^2 & 1 & \omega & \omega^2 & 1 & \omega & \omega^2 \\
\omega^2 & \omega & \omega & 1 & 1 & \omega^2 & \omega^2 & \omega \\
\omega & \omega & \omega & \omega & 1 & 1 & 1 & 1 \\
\omega & \omega^2 & \omega & \omega^2 & 1 & \omega & 1 & \omega \\
\omega^2 & \omega & \omega^2 & \omega & \omega & 1 & \omega & 1 \\
\omega & \omega & \omega^2 & \omega^2 & 1 & 1 & \omega & \omega \\
\omega & \omega^2 & \omega^2 & 1 & 1 & \omega & \omega & \omega^2 \\
\omega^2 & \omega & 1 & \omega^2 & \omega & 1 & \omega^2 & \omega \\
\omega^2 & \omega^2 & \omega & \omega & \omega & \omega & 1 & 1 \\
\omega^2 & 1 & \omega & \omega^2 & \omega & \omega^2 & 1 & \omega \\
1 & \omega^2 & \omega^2 & \omega & \omega^2 & \omega & \omega & 1
\end{pmatrix}.$$

The ternary code C_3^* consists of the columns of $3^3 \times 2^3$ matrix M_3^* and has parameters $(2^3, 3^3, 2^2)$. Let us show that the code C_3^* corrects single errors. Consider a code-vector $a^\tau \in C_3^*$, say

$$a^\tau = (\omega^2, 1, \omega^2, 1, \omega^2, 1, \omega^2, 1)^\tau$$

and assume that this vector is sent through a noisy channel. Let

$$c^\tau = (\omega^2, 1, \omega^2, 1, \omega^2, 1, \omega^2, \omega)^\tau$$

be the received vector which differs from a^τ in the last position. To correct the error, we multiply M_3 by c^τ and then take into account the relation

$$1 + \omega + \omega^2 = 0.$$

As a result, we obtain

$$M_3 c^\tau = s^\tau$$

where

$$\begin{aligned} s = (&-1 - 3\omega, -5 - 2\omega, 7 + \omega, 1 - 2\omega, -\omega, 3 + 2\omega, \\ &1 + \omega, -3 - 4\omega, 3 + 5\omega, 1 - 2\omega, -\omega, 3 + 2\omega, 3 + 2\omega, \\ &-1, 2 + 3\omega, -1, 2 + 3\omega, -\omega, 2, -1, 1 + \omega, -3 - 4\omega, \\ &3 + 5\omega, -\omega, 2, -1, 2\omega, -1 - 3\omega, -1 + \omega) \end{aligned}$$

The components of the syndrome s^τ are elements

$$s_i = s_i^{(0)} + s_i^{(1)} \omega$$

of the ring $Z[\omega]$. Since the first coefficient $s_3^{(0)} = 7$ of the element $7 + \omega$ in 3rd position of s^τ is strictly greater than the first coefficient of any other component of s^τ, we decode the received vector c^τ as the vector $a^\tau = (\omega^2, 1, \omega^2, 1, \omega^2, 1, \omega^2, 1)^\tau$ from the 3rd column of the matrix M_3^*

Now we assume that $a^\tau = (\omega, \omega, \omega^2, \omega^2, \omega^2, \omega^2, 1, 1)^\tau$ is a transmitted code-vector, and $c^\tau = (\omega, \omega, \omega, \omega^2, \omega^2, \omega^2, 1, 1)^\tau$ is the received vector. Multiplying the matrix M_3 by c^τ we obtain

$$M_3 c^\tau = s^\tau$$

where

$$\begin{aligned} s = (&-1, 1 + \omega, -2 - 2\omega, -2 + \omega, -3 - \omega, -\omega, 1 - 2\omega, \\ &3 + 2\omega, -\omega, 1 + 4\omega, 2\omega, -3 - \omega, -\omega, -1, 2, -3 + 2\omega, \\ &2\omega, -4 - 3\omega, -2 - 5\omega, -\omega, 3 - \omega, -3 - \omega, -1 - 3\omega, -1, \\ &6 - \omega, 2 + 3\omega, 5 + 3\omega) \end{aligned}$$

Again, the first coefficient $s_{25}^{(0)} = 6$ of the element $6 - \omega$ in 25th position of s^τ is strictly greater than the first coefficient of any other component of s^τ, so we decode the received vector c^τ as the vector $a^\tau = (\omega, \omega, \omega^2, \omega^2, \omega^2, \omega^2, 1, 1)^\tau$ from the 25th column of the matrix M_3^*. In other words, we decode c^τ as the complex conjugate of the 25th column of the matrix M_3^*.

Similarly, it is easy to see that the ternary code $\tilde{c}_3^*$ with parameters $(2^3, 3^4, 2^2)$ also corrects any single errors.

$$D_2 = \begin{pmatrix} 2^2 & -2\omega & -2\omega & -2\omega & \omega^2 & \omega^2 & -2\omega & \omega^2 & \omega^2 \\ -2\omega^2 & 2^2 & -2 & 1 & -2\omega & \omega & 1 & -2\omega & \omega \\ -2\omega^2 & -2 & 2^2 & 1 & \omega & -2\omega & 1 & \omega & -2\omega \\ -2\omega^2 & 1 & 1 & 2^2 & -2\omega & -2\omega & -2 & \omega & \omega \\ \omega & -2\omega^2 & \omega^2 & -2\omega^2 & 2^2 & -2 & \omega^2 & -2 & 1 \\ \omega & \omega^2 & -2\omega^2 & -2\omega^2 & -2 & 2^2 & \omega^2 & 1 & -2 \\ -2\omega^2 & 1 & 1 & -2 & \omega & \omega & 2^2 & -2\omega & -2\omega \\ \omega & -2\omega^2 & \omega^2 & \omega^2 & -2 & 1 & -2\omega^2 & 2^2 & -2 \\ \omega & \omega^2 & -2\omega^2 & \omega^2 & 1 & -2 & -2\omega^2 & -2 & 2^2 \end{pmatrix}$$

VII. CONCLUSION

In this paper, we consider a family $\{M_m\}, m = 1, 2, \cdots,$ of modified ternary Jacket matrix of order 3^m. We construct two families $\{C^*_m\}$ and $\{\tilde{C}^*_m\}$ of nonlinear 3-ary codes derived from Kronecker powers $M_m = M_1^{\otimes m}$ of the modified ternary Jacket Matrix. These codes are close to the Plotkin bound and have nice parameters and very easy encoding and decoding procedures.

REFERENCES

[1] D. F. Elliot and K. R. Rao, "Fast transforms: Algorithms, analyses," *Applications*, Academic Press, New York, 1982.

[2] D. K. Maslen and D. N. Rockmore, "Generalized FFTs-a survey of some recent results," *DIMACS Ser. Discr. Math. Theoret. Comp. Sci.*, vol. 28, pp.183–237, 1997.

[3] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes.* New York: NY, North-Holland, 1977.

[4] M. H. Lee, "The center weighted Hadamard transform," *IEEE Trans. Circuits Syst.*, vol. 36, no. 9, pp.1247–1248, 1989.

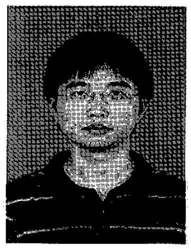
[5] Z. Chen, M. H. Lee, and G. Zeng, "Fast cocyclic Jacket transform," *IEEE Trans. Signal Process.*, vol. 56, no. 5, pp. 2143–2148, May 2008.

[6] G. Zeng and M. H. Lee, "A generalized reverse block Jacket transform," *IEEE Trans. Circuits Syst. I*, vol. 55, no. 6, pp. 1589–1600, July 2008.

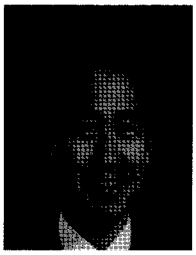
[7] M. H. Lee and G. Zeng, "Fast block Jacket transform based on Pauli matrices," in *Proc. ICC.*, Scotland, U.K., June 24–28, 2007.

[8] G. Feng and M. H. Lee, "An explicit construction of co-cyclic Jacket matrices with any size," in *Proc. Shanghai Conf. Combinatorices*, Shanghai, China, May 14–18, 2005.

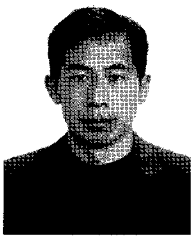
[9] J. Hou and M. H. Lee, "Cocyclic Jacket matrices and its application to cryptography systems," *Lecture Notes in Comput.*, vol. 3391, pp. 662–668, Jan. 2005.



Xueqin Jiang received the B.S. degree Nanjing Institute of Technology, Nanjing, Jiangsu, P. R. China, in computer science. He received the M.S and Ph.D. degree from Chonbuk National university, Jeonju, Korea, in communication engineering. He is currently working at School of Information Science and Technology, Donghua University, China. His research interests include LDPC codes and coding theory.



Moon Ho Lee received his B.S. and M.S. degrees in Electrical Engineering from Chonbuk National University, Korea, in 1967 and 1976, respectively, and Ph.D. (I) degree in Electrical Engineering from Chonnam National University in 1984. Also, he received his Ph.D. (II) degree in Information Engineering from the University of Tokyo in 1990. During August 1985 through August 1986, he studied at the University of Minnesota as a Post Doctor. Also, Professional Engineer Licensed at 1981, Korea. Currently, he is a Professor of Division of Electronic and Information Engineering and a Head of the Institute of Information and Communication in Chonbuk National University. His research interests include image processing, mobile communication, high speed communication networks, and information, and algebra coding theory. He is a Member of Sigma Xi. He is a Korea Engineering Academy Member and Guest Editor of IEEE Communication Magazine at 2007, "Quality of service based routing algorithm for heterogeneous networks."



Ying Guo received the B.S. degree from Qufu Normal University, Qufu, P. R. China, in Mathematics Science in 1999. He received the M.S. degree from Kunming University of Science and Technology, Kunming, P. R. China in Mathematics Science, in 1999. He received the Ph.D. degree Shanghai Jiaotong University, Shanghai, P. R. China, in Communication and Information Science. He is currently working at the Central South University. His research interests include quantum communication and coding theory.

Yier Yan received the B.S. degree from South-Central Nationality University, Wuhan, Hubei, P. R. China, in Applied Electronics. He received the M.S. and Ph.D. degree from Chonbuk National university, Jeonju, Korea, in Communication Engineering. He is currently working at School of Mechanical and Electrical Engineering of Guangzhou University, China. His research interests include information theory, signal processing, and OFDM in MIMO system.

Sarker Md. Abdul Latif received the B.S. (Hons) and M.S. degrees in Applied Physics, Electronics, and Communication Engineering from Islamic University in Bangladesh 2003 and 2004, respectively. He is currently working towards Ph.D. degree on Electronics Engineering from Chonbuk National University, Korea. His research interests include the areas of MIMO, OFDM, wireless communication, Jacket Matrices, UWB, and turbo codes.