2005

A simple element inverse jacket transform coding

Moon Ho Lee
Chonbuk National University

Kenneth Finlayson
University of Wollongong

Publication Details
A simple element inverse jacket transform coding

Abstract
Jacket transforms are a class of transforms which are simple to calculate, easily inverted and are size-flexible. Previously reported jacket transforms were generalizations of the well-known Walsh-Hadamard transform (WHT) and the center-weighted Hadamard transform (CWHT). In this paper we present a new class of jacket transform not derived from either the WHT or the CWHT. This class of transform can be applied to any even length vector, and is applicable to finite fields and is useful for constructing error control codes.

Disciplines
Physical Sciences and Mathematics

Publication Details

This conference paper is available at Research Online: http://ro.uow.edu.au/infopapers/2812
A Simple Element Inverse Jacket Transform Coding

Moon Ho Lee  
Institute of Information and Communication  
Chonbuk National University  
Jeonju, 561-756  
Korea  
E-mail: moonho@moak.chonbuk.ac.kr

Ken Finlayson  
Centre for Computer Security Research  
University of Wollongong  
Wollongong, NSW 2500  
Australia  
E-mail: kaf03@uow.edu.au

Abstract—Jacket transforms are a class of transforms which are simple to calculate, easily inverted and are size-flexible. Previously reported jacket transforms were generalizations of the well-known Walsh-Hadamard transform (WHT) and the center-weighted Hadamard transform (CWHT). In this paper we present a new class of jacket transform not derived from either the WHT or the CWHT. This class of transform can be applied to any even length vector and is applicable to finite fields and is useful for constructing error control codes.

I. INTRODUCTION

The Walsh-Hadamard transform (WHT) and discrete Fourier transform (DFT) are widely used in signal processing [1], [2]. In particular, these transforms are used in image coding and processing [3] and error-control coding [4]–[6]. Variations of these two transforms, called the center weighted Hadamard transform (CWHT) and the complex reverse jacket transform (CRJT) have been reported [7]–[10]. The jacket transform is so named because it brings to mind a reversible jacket. Just as the jacket is easily reversed (turned inside out), so too the jacket matrix is easily inverted. The CWHT and CRJT can be seen as generalizations of the WHT. Recently, the CWHT and CRJT have been generalized to give a transform using the 2nth roots of unity, for any positive integer n [11]. In this paper we present a jacket transform (JT) which does not derive from the WHT or its generalizations.

In this section we briefly discuss the WHT, CWT and CRJT.

A. The WHT

Given a real vector \( (a_0, a_1, \ldots, a_{n-1}) \) of length \( n = 2^m \), the transform vector is an n-length real vector \( (A_0, A_1, \ldots, A_{n-1}) \) given by

\[
A_j = \sum_{i=0}^{n-1} (-1)^{\langle j, i \rangle} a_i \tag{1}
\]

for \( 0 \leq j \leq n-1 \), where \( \langle j, i \rangle \) is the modulo 2 inner product of \( j \) and \( i \):

\[
\langle j, i \rangle = j_{m-1}i_{m-1} \oplus j_{m-2}i_{m-2} \oplus \cdots \oplus j_0i_0.
\]

(Here \( \langle i_{m-1}, i_{m-2}, \ldots, i_0 \rangle \) is the binary representation of \( i \), and \( \oplus \) denotes modulo two addition.)

The inverse transform is given by

\[
a_j = \frac{1}{n} \sum_{i=0}^{n-1} (-1)^{\langle j, i \rangle} A_i.
\]

B. The CWHT

The CWHT is obtained by weighting the center portion of the transform matrix given by (1). Thus the CWHT is given by

\[
A_j = \sum_{i=0}^{n-1} (-1)^{\langle j, i \rangle} (w^{j_{n-1}i_{n-1}} \oplus w^{j_{n-2}i_{n-2}} \oplus \cdots \oplus w^{j_0i_0}) a_i \tag{2}
\]

where the weight \( w \) is any real number. The inverse transform is given by

\[
a_j = \frac{1}{n} \sum_{i=0}^{n-1} (-1)^{\langle j, i \rangle} (w^{-1}w^{-j_{n-1}i_{n-1}} \oplus w^{-j_{n-2}i_{n-2}} \oplus \cdots \oplus w^{-j_0i_0}) A_i
\]

The 4 \( \times \) 4 and the 8 \( \times \) 8 CWHT are then

\[
\begin{bmatrix}
1 & 1 & 1 & 1 \\
1 & w & w^{-1} & -1 \\
1 & -w & w & 1 \\
1 & 1 & 1 & 1
\end{bmatrix}
\tag{3}
\]

and

\[
\begin{bmatrix}
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
1 & -1 & -1 & -1 & 1 & 1 & 1 & 1 \\
1 & 1 & w & -w & w^{-1} & -1 & -1 & -1 \\
1 & -1 & -w & w & w^{-1} & -1 & -1 & -1 \\
1 & 1 & w & -w & w & 1 & 1 & 1 \\
1 & -1 & -w & w & w & -1 & -1 & -1 \\
1 & 1 & -1 & -1 & -1 & -1 & -1 & -1 \\
1 & -1 & -1 & -1 & -1 & -1 & -1 & -1
\end{bmatrix}
\tag{4}
\]

Observe that when we set \( w = 1 \), we get the WHT.

In [8], a class of transform called CRJT is constructed by setting the weight \( w \) equal to the complex number \( j = \sqrt{-1} \). The CRJT is orthogonal and a fast algorithm to compute CRJT is given in [8]. We note for later reference that putting \( w = j \) in (3) and (4) yields the CRJT \( \{C\}_{4 \times 4} \) and \( \{C\}_{8 \times 8} \) respectively.

II. THE PROPOSED JACKET TRANSFORM

In [11], Lee et al. showed that the CRJT could be generalized to give a transform that used the complex 2nth roots of unity, where \( n \) is a positive integer. We look at a different set of jacket matrices due to a construction in [12] and present the corresponding transforms. These jacket transforms use the...
complex $p$th roots, where $p$ is an odd prime. The resulting matrix is $2p \times 2p$. In this section we obtain this matrix, using a mixed-radix representation of integers between 0 and $2p - 1$.

**Definition 1:** Let $n \geq 2$ be an arbitrary positive integer. For any integer $i \in \{0, 1, \ldots, 2n - 1\}$, its mixed-radix representation $(\langle i_1, \ldots, i_n \rangle)$ is given by $i = n_i + i_o$, where $i_1 \in \{0, 1\}$ and $i_o \in \{0, 1, \ldots, n - 1\}$.

**Definition 2:** Let $p$ be an odd prime, and let $\alpha$ denote a primitive $p$th root of unity on the complex circle. For any real or complex $2p$-length vector $(a_0, a_1, \ldots, a_{2p-1})$ the transformed vector $(A_0, A_1, \ldots, A_{2p-1})$ is given by

$$A_j = \sum_{i=0}^{2p-1} (-1)^{i_j} \alpha^{|\phi(p, j)| \phi(p, i)} a_i$$

(5)

where $\phi(p, j) = pj_j + (1 - j)j_0 + j(p - 1 - j_0)$ and $\langle \langle j_1, j_0 \rangle \rangle$ and $\langle \langle i_1, i_0 \rangle \rangle$ are the mixed-radix representation of $j$ and $i$ respectively.

It is easily verified that the inverse transform is given by

$$a_j = \frac{1}{2p} \sum_{i=0}^{2p-1} (-1)^{i_j} \alpha^{-|\phi(p, j)| \phi(p, i)} A_i$$

(6)

Example 1: Let $p = 3$. Then $\alpha = e^{\sqrt{-1} (2\pi/3)}$. The transform matrix and inverse matrix corresponding to Definition 2 are

$$[M]_{6 \times 6} = \begin{bmatrix}
1 & 1 & 1 & 1 & 1 & 1 \\
1 & \alpha & \alpha^2 & \alpha & \alpha & 1 \\
1 & \alpha & \alpha & \alpha & \alpha^2 & 1 \\
1 & \alpha^2 & \alpha & \alpha & -\alpha & -1 \\
1 & \alpha^2 & -\alpha^2 & -\alpha & -1 \\
1 & 1 & 1 & -1 & -1 & -1
\end{bmatrix}$$

and

$$[M]^{-1}_{6 \times 6} = \frac{1}{6} \begin{bmatrix}
1 & 1 & 1 & 1 & 1 & 1 \\
1 & \alpha^2 & \alpha & \alpha & \alpha^2 & 1 \\
1 & \alpha & \alpha^2 & \alpha & \alpha & 1 \\
1 & \alpha & \alpha^2 & -\alpha & -\alpha & -1 \\
1 & \alpha^2 & -\alpha^2 & \alpha & -\alpha & -1 \\
1 & 1 & 1 & -1 & -1 & -1
\end{bmatrix}$$

(7)

Example 2: Let $p = 5$. Then $\alpha = e^{\sqrt{-1} (2\pi/5)}$. The transform matrix corresponding to Definition 1 is

$$[M]_{10 \times 10} = \begin{bmatrix}
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
1 & \alpha & \alpha^2 & \alpha^3 & \alpha^4 & \alpha^3 & \alpha^2 & \alpha & 1 \\
1 & \alpha & \alpha^4 & \alpha & \alpha^3 & \alpha^4 & \alpha & \alpha^2 & 1 \\
1 & \alpha^3 & \alpha & \alpha^4 & \alpha^2 & \alpha & \alpha^3 & 1 \\
1 & \alpha^4 & \alpha^3 & \alpha & \alpha^4 & \alpha & \alpha^3 & 1 \\
1 & \alpha^4 & \alpha^3 & \alpha^2 & \alpha & -\alpha & -\alpha^2 & -\alpha & -1 \\
1 & \alpha^3 & \alpha & \alpha^4 & \alpha^2 & -\alpha^2 & -\alpha^4 & -\alpha^3 & -1 \\
1 & \alpha & \alpha^4 & \alpha & \alpha^2 & -\alpha^4 & -\alpha & -\alpha^3 & -1 \\
1 & \alpha & \alpha^3 & \alpha^2 & \alpha & -\alpha^2 & -\alpha^4 & -\alpha & -1 \\
1 & 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1
\end{bmatrix}$$

and the inverse matrix is also easily calculated.

We can further generalize this jacket transform to size $2^f p$, where $p$ is an odd prime and $\ell$ is a positive integer. To do so, we need the following more general definition of mixed-radix representation of integers.

**Definition 3:** Let $N = 2^t n$, where $t$ and $n$ are positive integers. For any integer $i \in \{0, 1, \ldots, N - 1\}$, its mixed-radix representation $\langle \langle i_1, i_2, \ldots, i_t, i_0 \rangle \rangle$ is given by

$$i = i_t (n^t - 1) + i_{t-1} n^{t-1} + i_{t-2} n^{t-2} + \cdots + i_0 n^0,$$

where $i_k \in \{0, 1\}$ for $0 \leq k \leq t$, $k \neq t - 1$ and $i_{t-1} \in \{0, 1, \ldots, N - 1\}$.

**Definition 4:** Let $N = 2^t p$, where $p$ is an odd prime and $\ell$ is a positive integer, and let $\alpha$ be a primitive $p$th root of unity on the complex circle. For any real or complex valued $N$-length vector $(a_0, a_1, \ldots, a_{2p-1})$, the transformed vector $(A_0, A_1, \ldots, A_{2p-1})$ is given by

$$A_j = \sum_{i=0}^{N-1} (-1)^{\langle \langle j, i \rangle \rangle} \alpha^{-|\phi(p, j)| \phi(p, i)} A_i$$

(9)

where $\phi(p, j) = pj_j + (1 - j)j_0 + j(p - 1 - j_0)$ and $\langle \langle j_1, j_0 \rangle \rangle$ and $\langle \langle i_1, i_0 \rangle \rangle$ the mixed-radix representation of $j$ and $i$ respectively.

It is easy to verify that the inverse transform is given by

$$a_j = \frac{1}{N} \sum_{i=0}^{N-1} (-1)^{\langle \langle j, i \rangle \rangle} \alpha^{-|\phi(p, j)| \phi(p, i)} A_i.$$

We observe that the JT given by Definitions 2 and 4 are orthogonal.

Lastly, we remark that the ratio of the number of weighted elements to the total number of elements is

$$\frac{2t(n - 1)}{2^t n},$$

where $N = 2^t n = 2^\ell p$. Here $t$ and $n$ are the numbers used to form the mixed-radix representation. For a fixed $N$, different choices of $t$ and $n$ give different mixed-radix representations, and so yield different JT. Thus the ratio depends on our choice of $t$ and $n$.

**A. The Jacket Transform Over Finite Fields**

In this section, we discuss the applicability of the new JT over finite fields and its usefulness to construct codes. We show how this new class of JT may be constructed over finite fields. In turn, the JT may be used to construct codes, though we do not give details of code construction here.

**Definition 3:** Let $N = 2^t n$, where $t, n$ are positive integers. Let $T$ be a jacket transform of vectors of length $N$, with $T$ using the $r$th root of unity over the complex circle (denoted $\alpha$). Also let $F_q$ be a finite field with $q$ elements, where $2r$ and $q$ are relatively prime, and $F_q^m$ be an extension field of $F_q$ where $m$ is the least integer such that $r$ divides $q^m - 1$ and $r h = q^m - 1$. Let $\gamma$ be a primitive element of $F_q^m$. Then the element $\gamma^k$, which we denote by $\beta$, has order $r$. We modify the
jacket transform $T$ by putting $\beta$ in place of $\alpha$. The resulting transform $T'$ is a transform of vectors of length $N$ over $\mathbb{F}_q$.

**Example 3:** We begin by considering the CRJT $[C]_{4 \times 4}$. This is a jacket transform using the fourth roots of unity on the complex circle. Thus we have $N = 4$, $n = 2$, $\ell = 1$ and $r = 4$. We choose $q = 5$. Then $m = 2$ and $h = 6$. We construct $F_{3^2}$ with the prime polynomial $x^2 + x + 1$. Thus the elements of the field are the set $\{00, 10, 20, 30, 40, 01, 11, 21, 31, 41, 02, 12, 22, 32, 42, 03, 13, 23, 33, 43, 04, 14, 24, 34, 44\}$, where $ab = a + bx$ and $a, b \in F_{3^2}$. The element $13$ is primitive, so we take $\gamma = 13$. Then $\beta = \gamma^6 = 20$, $\beta^2 = 40$ and $\beta^3 = 30$. The transform matrix of the resulting JT is

$$[F]_{4 \times 4} = \begin{bmatrix} 10 & 10 & 10 & 10 \\ 10 & 30 & 20 & 40 \\ 10 & 20 & 30 & 40 \\ 10 & 40 & 40 & 10 \end{bmatrix}.$$  \hspace{1cm} (10)

Likewise, $[C]_{8 \times 8}$ is a JT using the fourth roots of unity over the complex circle. We have $N = 8$, $n = 2$, $\ell = 2$ and $r = 4$. We can again choose $q = 5$, yielding $m = 2$ and $h = 6$. So the field and the choice of $\gamma$ are as in the previous paragraph. The modified JT will have the following transform matrix:

$$[F]_{8 \times 8} = \begin{bmatrix} 10 & 10 & 10 & 10 & 10 & 10 & 10 & 10 \\ 10 & 40 & 10 & 40 & 10 & 40 & 10 & 40 \\ 10 & 10 & 30 & 30 & 20 & 20 & 40 & 40 \\ 10 & 10 & 30 & 20 & 20 & 30 & 40 & 40 \\ 10 & 40 & 20 & 30 & 30 & 20 & 40 & 40 \\ 10 & 10 & 40 & 40 & 40 & 40 & 40 & 10 \\ 10 & 40 & 40 & 10 & 40 & 10 & 10 & 40 \end{bmatrix}.$$  \hspace{1cm} (11)

**Example 4:** We take the JT with transform matrix (6). It uses the cube roots of unity over the complex circle. We have $N = 6$, $n = 3$, $\ell = 1$ and $r = 3$. We can again choose $q = 5$, with $m = 2$ and $h = 8$. We are still using $F_{3^2}$, as constructed in Example 3, with $\gamma = 13$. But now $\beta = \gamma^6 = 44$ and $\beta^2 = 01$. So the resulting JT has the transform matrix

$$[F]_{6 \times 6} = \begin{bmatrix} 10 & 10 & 10 & 10 & 10 & 10 \\ 10 & 44 & 01 & 01 & 44 & 10 \\ 10 & 01 & 44 & 44 & 01 & 10 \\ 10 & 01 & 44 & 11 & 04 & 40 \\ 10 & 44 & 01 & 04 & 11 & 40 \\ 10 & 10 & 10 & 40 & 40 & 40 \end{bmatrix}.$$  \hspace{1cm} (12)

**Example 5:** We take the JT with transform matrix (8). We have $N = 10$, $\ell = 1$, $n = 5$ and $r = 5$. We choose $q = 3$, giving $m = 4$ and $h = 16$. We construct $F_{3^4}$ with the polynomial $x^4 + x + 2$. (We omit the elements of the field for brevity.) The element $\gamma = 0100$ is primitive, where $\alpha \cdot \beta = a \cdot b + c \cdot d^2 + d \cdot x^3$. Then $\beta = \gamma^6 = 2102$, $\beta^2 = 2021$, $\beta^3 = 2220$ and $\beta^4 = 2002$. The resulting transform matrix is (13).

### III. Conclusion

In this paper, we have presented a new class of jacket transform that uses the complex $p$th root of unity, where $p$ is any odd prime. We have also shown how to construct these transforms over finite fields. The applications of these transforms to image processing, error control coding and sequences have been cited.

### ACKNOWLEDGMENT

This paper was partially supported by the Institute of Information Technology Assessment, Korea.

### REFERENCES


