Real-valued error control coding by using DCT

Ja-Ling Wu
Jiun Shiu

Indexing terms: Algorithms, Codes and decoding, Decoding

Abstract: The discrete cosine theorem (DCT)-based real-valued linear code is derived for the first time in the literature. A BCH-like subclass of DCT linear codes is also developed, for which fast decoding algorithms exist. It is shown that the DCT-based error control codes proposed in the paper can be viewed as a bridge to link the fields of source coding and channel coding.

1 Introduction

Discrete transforms are playing an increasingly important role in many practical applications. The DCT (discrete cosine transform), since its basis set provides a good approximation to the eigenvectors of a class of Toeplitz matrices [1], provides suboptimum methods in the applications of data compression by transform coding approach [2, 3], features extraction, which usually serves as a preprocessing stage in pattern recognition problems [1], etc. There are other branches for investigation of the discrete transform: for example, as indicated by Marshall [40], the use of error control coding for discrete signals.

In this paper, the use of the DCT for defining a class of real-valued linear codes is presented. Additionally, it is worth mentioning that the terminology in this paper comes from communication theory; these codes, however, might have other applications, such as in an algorithm-based fault tolerance problem [5]. Also, we are going to explore the applications of the real number codes in future work.

2 Preliminaries

According to Marshall [4], and as shown in Fig. 1, the transmission of a discrete-time signal, i.e. a sequence of real numbers $\{x_i\}$, by a real-valued (N, K) block coding procedure involves the following steps:

(1) The signal $\{x_i\}$ is divided into blocks of K symbols which are then processed independently. Let the row vector

$$x = [x_0, x_1, \ldots, x_{k-1}]$$

be a typical block and call it the information vector.

(2) The information vector x is encoded into an N-tuple y, called a code vector, as shown by

$$y = x \cdot G \tag{1}$$

where G is a $K \times N$ matrix of rank K, called the generator matrix. The set of all code vectors, say $\mathscr{F}$, is the row space of G, called the code space. Since G is a $K \times N$ matrix of rank K, $\mathscr{F}$ is a K-dimensional subspace of the

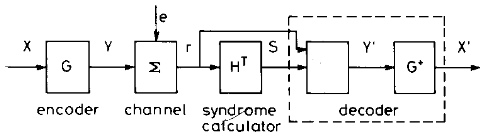

Fig. 1 *Transmission of discrete signal*

vector space that consists of all N-tuples with real components. Thus, by the definition of linear code [7], $\mathscr{F}$ is a real-valued (N, K) linear code generated by G.

(3) Let r be the received vector at the other end of the transmission channel and suppose that an unknown error e is introduced as

$$r = y + e \tag{2}$$

where we assume the channel noise to be random and additive. As is well known, for each $K \times N$ matrix G of rank K, there will be an $(N - K) \times N$ matrix H of rank $N - K$ such that G is in the nullspace of H^T; i.e. matrices G and H are related by

$$G \cdot H^T = 0 \tag{3}$$

H is the so-called parity check matrix of $\mathscr{F}$. The syndrome vector S of a received vector r is defined as

$$\begin{aligned} S &= r \cdot H^T \\ &= (y + e) \cdot H^T \\ &= y \cdot H^T + e \cdot H^T \\ &= e \cdot H^T \end{aligned} \tag{4}$$

If $e = 0$, no error occurs, then

$$S = r \cdot H^T = 0 \tag{5}$$

i.e. the syndrome vector of any code vector is 0.

(4) After identifying the syndromes of the received vector r, the decoder must determine the optimal estimate of e, say e'. According to the maximum-likelihood decoding rule, the optimal estimate e' is the error pattern, generated from the calculated syndromes, which has the fewest nonzero elements. Finally, the estimations y' and x' of the corresponding actual sequences are, respectively, obtained by

$$y' = r - e' \tag{6}$$

$$x' = y' \cdot G^+ \tag{7}$$

Paper 8657I (E5), first received 30th October 1990 and in revised form 12th December 1991

The authors are with the Department of Computer Science and Information Engineering, National Taiwan University, Taipei, 10764, Taiwan, Republic of China

where the matrix G^+ is an $N \times K$ right inverse of G, such that

$$G \cdot G^+ = I_K \tag{8}$$

3 DCT linear codes

As defined in Reference 1, the DCT of a data sequence $x = [x_0, x_1, \ldots, x_{k-1}]$ is

$$X_K = \sum_{n=0}^{N-1} x_n \cdot T_K(n) \quad K = 0, 1, 2, \ldots, N-1 \tag{9}$$

where

$$T_K(n) = \begin{cases} \dfrac{1}{\sqrt{N}} & K = 0 \\ \dfrac{2}{\sqrt{N}} \cos \dfrac{(2n+1)k\pi}{2N} & K = 1, 2, \ldots, N-1 \end{cases} \tag{10}$$

Theorem 1 (*orthogonal property of DCT*):

$$\sum_{n=0}^{N-1} T_p(n) \cdot T_q(n) = \begin{cases} 1 & p = q \\ 0 & p \neq q \end{cases} \tag{11}$$

Writing the N equations of eqn. 9 in matrix form, one gets

$$\begin{bmatrix} X_0 \\ X_1 \\ \vdots \\ X_{N-1} \end{bmatrix} = \begin{bmatrix} T_0(0) & T_0(1) & \cdots & T_0(N-1) \\ T_1(0) & T_1(1) & \cdots & T_1(N-1) \\ \vdots & \vdots & & \vdots \\ T_{N-1}(0) & T_{N-1}(1) & \cdots & T_{N-1}(N-1) \end{bmatrix} \times \begin{bmatrix} x_0 \\ x_1 \\ \vdots \\ x_{N-1} \end{bmatrix} \tag{12}$$

The $N \times N$ matrix in eqn. 12 is the so-called N-point DCT matrix.

Select any K rows of the N-point DCT matrix, say j_0, $j_1, \ldots, j_{K-1}$, as the rows of a $K \times N$ matrix G; i.e.

$$G = \begin{bmatrix} T_{j_0}(0) & T_{j_0}(1) & \cdots & T_{j_0}(N-1) \\ T_{j_0}(0) & T_{j_1}(1) & \cdots & T_{j_1}(N-1) \\ \vdots & \vdots & & \vdots \\ T_{j_{K-1}}(0) & T_{j_{K-1}}(1) & \cdots & T_{j_{K-1}}(N-1) \end{bmatrix} \tag{13}$$

Since G is a $K \times N$ matrix of rank K, G will generate an (N, K) linear code.

Let the $(N-K) \times K$ matrix H consist of the remaining $(N-K)$ rows, say $j_K, j_{K+1}, \ldots, j_{N-1}$, which are called parities, as its $(N-K)$ rows. Then

$$G = \begin{bmatrix} T_{j_K}(0) & T_{j_K}(1) & \cdots & T_{j_K}(N-1) \\ T_{j_{K+1}}(0) & T_{j_{K+1}}(1) & \cdots & T_{j_{K+1}}(N-1) \\ \vdots & \vdots & & \vdots \\ T_{j_{N-1}}(0) & T_{j_{N-1}}(1) & \cdots & T_{j_{N-1}}(N-1) \end{bmatrix} \tag{14}$$

By the orthogonal property of the rows of the DCT matrix (eqn. 11), it is easy to verify that

$$G \cdot H^T = 0 \tag{15}$$

$$G \cdot G^T = I_K \tag{16}$$

Thus, by eqns. 3 and 8, one can see that matrix H is the parity check matrix of the code, and that matrix G^T is the right inverse of generator matrix G.

4 BCH-like subclass of DCT linear codes

Now we define a subclass of the above DCT linear codes and show how to decode it by using existing BCH decoding algorithms. It should be noticed that this BCH-like subclass of codes is defined directly from the class of the DCT linear codes, but not conventionally from a cyclic subclass of them. In fact, it can be shown that a significant cyclic subclass of the DCT linear codes does not exist at all. The arguments of this statement are given in Appendix 7.2.

Suppose that the first d rows, i.e. $0, 1, \ldots, d-1$, are selected as parties; ie.

$$H = \begin{bmatrix} T_0(0) & T_0(1) & \cdots & T_0(N-1) \\ T_1(0) & T_1(1) & \cdots & T_1(N-1) \\ \vdots & \vdots & & \vdots \\ T_{d-1}(0) & T_{d-1}(1) & \cdots & T_{d-1}(N-1) \end{bmatrix}_{d \times N}$$

$$G = \begin{bmatrix} T_d(0) & T_d(1) & \cdots & T_d(N-1) \\ T_{d+1}(0) & T_{d+1}(1) & \cdots & T_{d+1}(N-1) \\ \vdots & \vdots & & \vdots \\ T_{N-1}(0) & T_{N-1}(1) & \cdots & T_{N-1}(N-1) \end{bmatrix}_{(N-d) \times N}$$

Suppose further that the error pattern $e = [e_0, e_1, \ldots, e_{N-1}]$ occurs during a transmission. Then the syndrome vector defined by eqn. 4 will not be zero, and the entries of S will be

$$S_i = \sum_{r=0}^{N-1} e_r \cdot T_i(r)$$

By the definition of $T_i(\cdot)$, and letting

$$f_i = \begin{cases} \dfrac{1}{\sqrt{N}} & K = 0 \\ \dfrac{2}{\sqrt{N}} & K = 1, 2, \ldots, N-1 \end{cases} \tag{17}$$

we will have

$$\frac{1}{f_i} \cdot S_i = \sum_{r=0}^{N-1} e_r \cdot \cos \frac{(2r+1)i\pi}{2N} \qquad \text{for } i = 0, 1, 2, \ldots, d-1 \tag{18}$$

Before going on, a lemma will be described. The proof of this lemma can be found in Reference 6, but the explicit expression to $C_{k,n}$ is not given there. Therefore the derivation of $C_{k,n}$ is also given in Appendix 7.1.

Lemma 1:

$$\cos k\omega = \sum_{n=0}^{k} C_{k,n} \cdot (\cos \omega)^n \tag{19}$$

where

$$C_{k,n} = \begin{cases} 0 & k - n \text{ odd} \\ \displaystyle\sum_{m=0}^{\lfloor n/2 \rfloor} (-1)^{(k-n)/2} \binom{k}{n-2m} \binom{(k-n)/2 + m}{m} & k - n \text{ even} \end{cases}$$

Assume that actually v errors occur, or equivalently there are only v nonzero terms in the error pattern $e = [e_0, e_1, \ldots, e_{N-1}]$. Let $r_1, r_2, \ldots, r_v$ be the locations of these nonzero terms. Then, by introducing Lemma 1, eqn. 18

will be

$$\frac{1}{f_i}\cdot S_i = \sum_{l=1}^{v} e_{r_l}\cdot\cos\frac{(2r_l+1)i\pi}{2N}$$
$$= \sum_{l=1}^{v} e_{r_l}\sum_{n=0}^{i} C_{i,n}\cdot\left[\cos\frac{(2r_l+1)i\pi}{2N}\right]^n \qquad (20)$$

where $C_{i,n}$ is defined in Lemma 1 as eqn. 19. Let Y_l, the error magnitude at location r_l, and X_l, the error location number for r_l, be defined as

$$Y_l = e_{r_l}$$

$$X_l = \cos\frac{(2r_l+1)\pi}{2N} \qquad l = 1, 2, \ldots, v$$

Then eqn. 20 can be written using the above notation, and further in matrix form,

$$\frac{1}{f_i}\cdot S_i = \sum_{l=1}^{v} Y_l \sum_{n=0}^{i} C_{i,n}\cdot X_l^n$$
$$= [Y_1 \quad Y_2 \quad \cdots \quad Y_v] \times \begin{bmatrix} 1 & X_1 & X_1^2 & \cdots & X_1^i \\ 1 & X_2 & X_2^2 & \cdots & X_2^i \\ & \vdots & & & \vdots \\ 1 & X_v & X_v^2 & \cdots & X_v^i \end{bmatrix} \begin{bmatrix} C_{i,0} \\ C_{i,1} \\ \vdots \\ C_{i,i} \end{bmatrix}$$

Thus the modified syndrome vector is

$$\boldsymbol{S} = \left[\sqrt{(N)}S_0 \quad \frac{\sqrt{N}}{2}S_1 \quad \cdots \quad \frac{\sqrt{N}}{2}S_{d-1}\right]$$
$$= \boldsymbol{Y}\begin{bmatrix} 1 & X_1 & X_1^2 & \cdots & X_1^{d-1} \\ 1 & X_2 & X_2^2 & \cdots & X_2^{d-1} \\ & \vdots & & & \vdots \\ 1 & X_v & X_v^2 & \cdots & X_v^{d-1} \end{bmatrix}$$
$$\times \begin{bmatrix} C_{0,0} & 0 & C_{2,0} & 0 & \cdots & \\ 0 & C_{1,1} & 0 & C_{3,1} & \cdots & \cdot \\ 0 & 0 & C_{2,2} & 0 & \cdots & \cdot \\ 0 & 0 & 0 & C_{3,3} & \cdots & \cdot \\ \cdot & & \vdots & & \vdots & \\ 0 & 0 & 0 & 0 & \cdots & C_{d-1,d-1} \end{bmatrix} \qquad (21)$$

Let the $d \times d$ upper triangular matrix in eqn. 21 be $\boldsymbol{C}$, which is always invertible. Then

$$\boldsymbol{S}\boldsymbol{C}^{-1} = \boldsymbol{Y}\begin{bmatrix} 1 & X_1 & X_1^2 & \cdots & X_1^{d-1} \\ 1 & X_2 & X_2^2 & \cdots & X_2^{d-1} \\ & \vdots & & & \vdots \\ 1 & X_v & X_v^2 & \cdots & X_v^{d-1} \end{bmatrix} \qquad (22)$$

By viewing the Peterson–Gorenstein–Zierier algorithm described in Reference 7, we know that X_i, Y_i, $1 \leqslant i \leqslant v$ can be found by the algorith provided that

$$v \leqslant \left\lfloor \frac{d}{2} \right\rfloor = t \qquad (23)$$

or, in other words, the correction capacity of this code is t. By introducing the Berlekamp–Massey algorithm (Fig. 2) and Forney algorithm (Fig. 3), one can have several fast decoding algorithms [7] for this subclass of DCT codes.

Let us now construct a (16, 10) DCT code as an example which can correct all patterns of three or fewer errors. The diagram in a communication context is shown in Fig. 4. The generator matrix $\boldsymbol{G}$ consists of the

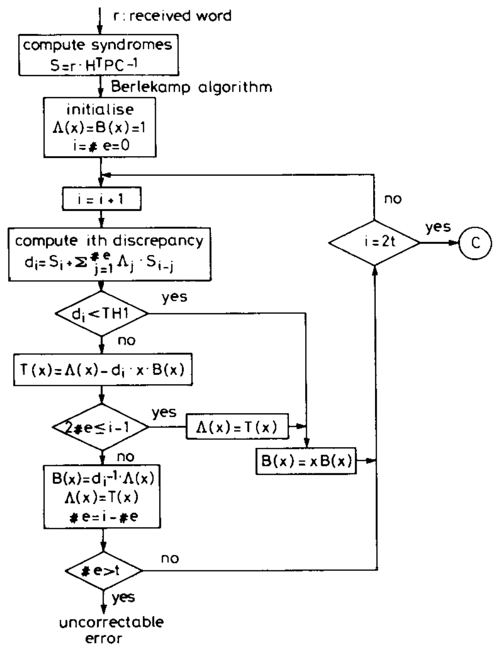

Fig. 2 *Berlekamp–Massey algorithm*

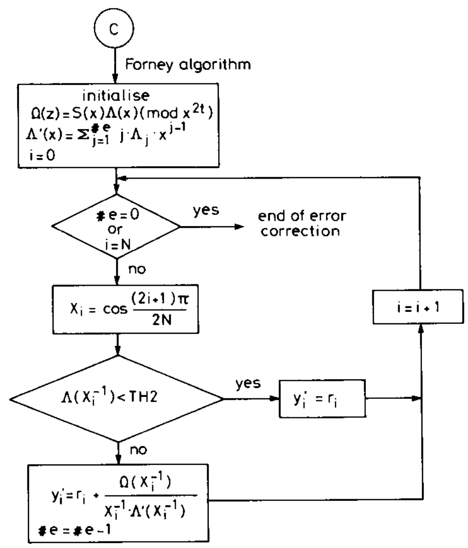

Fig. 3 *Forney algorithm*

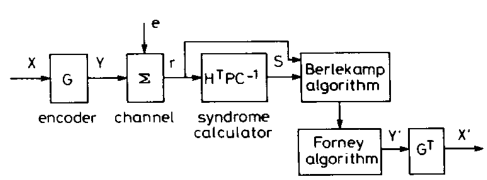

Fig. 4 *(16, 10) DCT code with fast decoding algorithm*

last ten rows of the 16-point DCT matrix, and the parity check matrix $\boldsymbol{H}$ is formed by the other six rows. The matrix $\boldsymbol{P}$ is a diagonal matrix with the normalisation factors f_i, $i = 0, 1, \ldots, 5$ as its nonzero elements. The triangular matrix $\boldsymbol{C}$ is as follows:

$$\boldsymbol{C} = \begin{bmatrix} 1 & 0 & -1 & 0 & 1 & 0 \\ 0 & 1 & 0 & -3 & 0 & 5 \\ 0 & 0 & 2 & 0 & -8 & 0 \\ 0 & 0 & 0 & 4 & 0 & -20 \\ 0 & 0 & 0 & 0 & 8 & 0 \\ 0 & 0 & 0 & 0 & 0 & 16 \end{bmatrix}$$

Thus, matrix $\boldsymbol{H}^T\boldsymbol{P}\boldsymbol{C}^{-1}$ used for calculating syndromes will be

$$\begin{bmatrix}
1.0 & 0.99518460 & 0.99039268 & 0.98562348 & 0.98087764 & 0.97615433 \\
1.0 & 0.95694029 & 0.91573477 & 0.87630355 & 0.83857018 & 0.80246162 \\
1.0 & 0.88192135 & 0.77778506 & 0.68594533 & 0.60494965 & 0.53351808 \\
1.0 & 0.77301055 & 0.59754509 & 0.46190876 & 0.35706016 & 0.27601138 \\
1.0 & 0.63439327 & 0.40245491 & 0.25531465 & 0.16196999 & 0.10275258 \\
1.0 & 0.47139668 & 0.22221494 & 0.10475136 & 0.04937952 & 0.02327732 \\
1.0 & 0.29028457 & 0.08426523 & 0.02446079 & 0.00710065 & 0.00206111 \\
1.0 & 0.09801716 & 0.00960732 & 0.00094173 & 0.00009224 & 0.00000909 \\
1.0 & -0.09801716 & 0.00960732 & -0.00094173 & 0.00009224 & -0.00000909 \\
1.0 & -0.29028457 & 0.08426523 & -0.02446079 & 0.00710065 & -0.00206111 \\
1.0 & -0.47139668 & 0.22221494 & -0.10475136 & 0.04937952 & -0.02327732 \\
1.0 & -0.63439327 & 0.40245476 & -0.25531465 & 0.16196984 & -0.10275258 \\
1.0 & -0.77301055 & 0.59754509 & -0.46190876 & 0.35706016 & -0.27601138 \\
1.0 & -0.88192135 & 0.77778506 & -0.68594533 & 0.60494965 & -0.53351808 \\
1.0 & -0.95694029 & 0.91573477 & -0.87630355 & 0.83857018 & -0.80246162 \\
1.0 & -0.99518460 & 0.99039268 & -0.98562348 & 0.98087764 & -0.97615427
\end{bmatrix}$$

Some simulation results are given in Table 1. As one can see, the arbitrary error patterns with three or fewer nonzero terms can be estimated and thus corrected, though coupled with some small computational error. It should be mentioned that if the error magnitude is not big enough, it will not be detected at all, as in the last case of the simulation.

5 Conclusion

We have defined a new class of real-valued linear codes and have shown that a subclass of them has a similar structure to the BCH code defined over finite field. The BCH bound on code capacity and conventional BCH decoding algorithms can be applied to this new subclass. However, there is no way to describe a nontrivial cyclic subclass of this linear code (a result shown in Appendix 7.2). This result violates the well-known concept that the BCH code should be a subclass of a cyclic code. It is a difference between codes over the two different fields, finite field and real field.

Table 1: Simulation results

info vector:
0.1000000, 0.0000000, 0.0000000, 0.0000000, 0.0000000, 0.0000000, 0.0000000, 0.0000000, 0.0000000, 0.0000000

error vector: (location, magnitude)
(0,0.200000)

estimated error: (location, magnitude)
(0,0.200000)

estimation::
0.1000000, −0.0000000, −0.0000000, −0.0000000, −0.0000000, −0.0000000, −0.0000000, −0.0000000, −0.0000000, −0.0000000

info vector:
0.2000000, 0.0000000, 0.0000000, 0.0000000, 0.0000000, 0.0000000, 0.0000000, 0.0000000, 0.0000000, 0.0000000

error vector: (location, magnitude)
(2,0.800000) (8,0.400000)

estimated error: (location, magnitude)
(2,0.799999) (8,0.400011)

estimation:
0.2000030, −0.0000028, −0.0000030, 0.0000029, 0.0000022, −0.0000032, −0.0000012, 0.0000040, 0.0000010, −0.0000037

info vector:
0.3000000, 0.0000000, 0.0000000, 0.0000000, 0.0000000, 0.0000000, 0.0000000, 0.0000000, 0.0000000, 0.0000000

error vector: (location, magnitude)
(4,0.600000) (6,0.300000) (13,0.170000)

estimated error: (location, magnitude)
4,0.599999) (6,0.300000) (13,0.170000)

estimation:
0.3000000, 0.0000004, 0.0000002, −0.0000001, −0.0000003, −0.0000003, 0.0000001, 0.0000001, 0.0000002, 0.0000000

info vector:
0.4000000, 0.0000000, 0.0000000, 0.0000000, 0.0000000, 0.0000000, 0.0000000, 0.0000000, 0.0000000, 0.0000000

error vector: (location, magnitude)
(2,0.9000000) (4,0.000010)

estimated error: (location, magnitude)
(2,0.899929)

estimation:
0.3999773, −0.0000206, −0.0000153, −0.0000076, 0.0000020, 0.0000126, 0.0000218, 0.0000266, 0.0000244, 0.0000146

info vector:
0.5000000, 0.0000000, 0.0000000, 0.0000000, 0.0000000, 0.0000000, 0.0000000, 0.0000000, 0.0000000, 0.0000000

error vector: (location, magnitude)
(2,0.900000), (4,0.200000) (15,0.600000)

estimated error: (location, magnitude)
(2, 0.899999) (4, 0.200000) (15, 0.600000)

estimation:
0.4999995, −0.0000006, −0.0000004, −0.0000001, 0.0000003, 0.0000004, 0.0000004, 0.0000002, 0.0000001, 0.0000000

6 References

1 AHMED, N., NATARAJAN, T., and RAO, K.R.: 'Discrete cosine transform', *IEEE Trans.*, 1974, **C-23**, (1), pp. 90–93
2 JAYANT, N.S., and NOLL, P.: 'Digital coding of waveforms' (Prentice-Hall, Englewood Cliffs, NJ, 1984)
3 ZELINSKI, R., and NOLL, P.: 'Adaptive transform coding of speech signals', *IEEE Trans.*, 1977, **ASSP-25**, (4), pp. 299–309
4 MARSHALL, T.G., Jr.: 'Coding of real-number sequences for error correction: a digital signal processing problem', *ibid.*, 1984, **SAC-2**, (2), pp. 381–391
5 ANFINSON, C.J., and LUK, F.T.: 'A linear algebraic model of algorithm-based fault tolerance', *ibid.*, 1988, **C-37**, (12), pp. 1599–1604
6 McCLELLAN, J.H., and PARKS, T.W.: 'Eigenvalue and eigenvector decompositon of the discrete Fourier transform', *ibid.*, 1972, **AU-20**, (1), pp. 66–74
7 BLAHUT, R.E.: 'Theory and practice of error control codes' (Addison-Wesley, New York, 1983)

7 Appendix

7.1 Proof of eqn. 19

$$\begin{aligned}
\cos K\omega &= \mathrm{Re}\,[e^{jK\omega}] \\
&= \mathrm{Re}\,[(\cos\omega + j\sin\omega)^K] \\
&= \mathrm{Re}\left[\sum_{i=0}^{K}\binom{K}{i}(\cos\omega)^{K-i}\cdot(j\sin\omega)^i\right] \\
&= \sum_{i=0}^{\lfloor K/2\rfloor}\binom{K}{2i}(\cos\omega)^{K-2i}\cdot(j\sin\omega)^{2i} \\
&= \sum_{i=0}^{\lfloor K/2\rfloor}\binom{K}{2i}(\cos\omega)^{K-2i}\cdot(\cos^2\omega - 1)^i \\
&= \sum_{i=0}^{\lfloor K/2\rfloor}\binom{K}{2i}(\cos\omega)^{K-2i} \\
&\quad\cdot\sum_{j=0}^{i}(-1)^j\binom{i}{j}(\cos^2\omega)^{i-j} \\
&= \sum_{i=0}^{\lfloor K/2\rfloor}\sum_{j=0}^{i}(-1)^j\binom{K}{2i}\binom{i}{j}(\cos\omega)^{K-2j} \\
&= \sum_{j=0}^{\lfloor K/2\rfloor}\sum_{i=j}^{\lfloor K/2\rfloor}(-1)^j\binom{K}{2i}\binom{i}{j}(\cos\omega)^{K-2j}
\end{aligned}$$

For K even, say $K = 2r$, then

$$\begin{aligned}
\cos K\omega &= \sum_{j=0}^{r}\sum_{i=j}^{r}(-1)^j\binom{2r}{2i}\binom{i}{j}(\cos\omega)^{2r-2j} \\
&= \sum_{n=0}^{r}\sum_{i=r-n}^{r}(-1)^{r-n}\binom{2r}{2i}\binom{i}{r-n}(\cos\omega)^{2n} \\
&= \sum_{n=0}^{r}\sum_{m=0}^{n}(-1)^{r-n}\binom{2r}{2(r-n+m)} \\
&\quad\times\binom{r-n+m}{r-n}(\cos\omega)^{2n} \\
&= \sum_{n=0}^{r}\sum_{m=0}^{n}(-1)^{r-n}\binom{2r}{2n-2m} \\
&\quad\times\binom{r-n+m}{m}(\cos\omega)^{2n} \qquad (24)
\end{aligned}$$

For K odd, say $K = 2r + 1$, then

$$\begin{aligned}
\cos K\omega &= \sum_{j=0}^{r}\sum_{i=j}^{r}(-1)^j\binom{2r+1}{2i}\binom{i}{j}(\cos\omega)^{2r+1-2j} \\
&= \sum_{n=0}^{r}\sum_{i=r-n}^{r}(-1)^{r-n}\binom{2r+1}{2i} \\
&\quad\times\binom{i}{r-n}(\cos\omega)^{2n+1} \\
&= \sum_{n=0}^{r}\sum_{m=0}^{n}(-1)^{r-n}\binom{2r+1}{2(r-n+m)} \\
&\quad\times\binom{r-n+m}{r-n}(\cos\omega)^{2n+1} \\
&= \sum_{n=0}^{r}\sum_{m=0}^{n}(-1)^{r-n}\binom{2r+1}{2n+1-2m} \\
&\quad\times\binom{r-n+m}{m}(\cos\omega)^{2n+1} \qquad (25)
\end{aligned}$$

By eqns. 24 and 25, Lemma 1 is proved.

7.2 Trivial DCT linear code

As defined in Reference 7, the cyclic subclass of a class of linear codes is the collection of those linear codes which have the cyclic shift property, and the codes in this subclass are therefore called cyclic codes.

Definition 1 (cyclic shift property): For a linear code $\mathscr{F}$, if

$$y = [y_0, y_1, \ldots, y_{N-1}] \in \mathscr{F}$$

implies that the vector obtained by cyclically shifting y right by one digit is also a code vector;

$$y_{[1]} = [y_{N-1}, y_0, y_1, \ldots, y_{N-2}] \in \mathscr{F}$$

then $\mathscr{F}$ is said to have the cyclic shift property, or, equivalently, C is a cyclic code.

We will show here that there is only a trivial DCT linear code, namely the $(N, N-1)$ code that has row 0 as its parity vector, which possesses the cyclic shift property. This is shown by trying to find all the possible candidates for parity vectors that can be selected as rows of the parity check matrix so that the corresponding generator matrix defines a cyclic code.

Let $\boldsymbol{G}$ and $\boldsymbol{H}$ be defined as in eqns. 13 and 14. By eqns. 1 and 5, one knows that showing $\boldsymbol{y} = [y_0, y_1, \ldots, y_{N-1}]$ is a code vector is equivalent to showing that there is an information vector $\boldsymbol{x} = [x_0, x_1, \ldots, x_{N-1}]$ such that

$$\begin{aligned}
\boldsymbol{y} &= \boldsymbol{x}\cdot\boldsymbol{G} \\
&= \sum_{n=0}^{K-1}x_n\cdot[T_{j_n}(0), T_{j_n}(1), \ldots, T_{j_n}(N-1)] \qquad (26)
\end{aligned}$$

and is also equivalent to showing that the syndrome vector of $\boldsymbol{y}$ is zero; i.e.

$$\boldsymbol{S} = [S_0, S_1, \ldots, S_{N-K-1}] = \boldsymbol{y}\cdot\boldsymbol{H}^T = \boldsymbol{0}$$

or

$$S_i = \sum_{m=0}^{N-1}y_m\cdot T_{j_{K+i}}(m) = 0 \qquad \text{for } i = 0, 1, \ldots, N-K-1$$

Let p_i be the ith parity, i.e. $p_i = j_{K+i}$, then

$$S_i = \sum_{m=0}^{N-1}y_m\cdot T_{p_i}(m) = 0 \qquad (27)$$

Now we try to find a way of selecting parities such that

$$S' = [S'_0, S'_1, \ldots, S_{N-K-1}] = y_{[1]} \cdot H^T = 0 \tag{28}$$

We reach the conclusion, on exploiting eqn. 28, that there is no way to select a significant set of parities such that eqn. 28 is true, and so prove that there is not a nontrivial cyclic subclass of the DCT linear codes. Let us now state some lemmas.

Lemma 2:

$$T_p(m+1) = T_p(m) \cdot \cos\frac{p\pi}{N} - \sqrt{\left(\frac{2}{N}\right)} \cdot \sin\frac{(2m+1)p\pi}{2N} \times \sin\frac{p\pi}{N} \quad m, p \in Z$$

Proof: If $p \neq 0 \Rightarrow$

$$\begin{aligned} T_p(m+1) &= \sqrt{\left(\frac{2}{N}\right)} \cdot \cos\frac{((2m+1)+1)p\pi}{2N} \\ &= \sqrt{\left(\frac{2}{N}\right)} \cdot \cos\left[\frac{(2m+1)p\pi}{2N} + \frac{p\pi}{N}\right] \\ &= \sqrt{\left(\frac{2}{N}\right)} \cdot \cos\frac{(2m+1)p\pi}{2N} \cdot \cos\frac{p\pi}{N} \\ &\quad - \sin\frac{(2m+1)p\pi}{2N} \cdot \sin\frac{p\pi}{N} \\ &= T_p(m) \cdot \cos\frac{p\pi}{N} - \sqrt{\left(\frac{2}{N}\right)} \\ &\quad \times \sin\frac{(2m+1)p\pi}{2N} \cdot \sin\frac{p\pi}{N} \end{aligned} \tag{29}$$

For $p = 0$, both sides of eqn. 29 equal $\sqrt{(1/N)}$. Thus Lemma 2 holds for all $m, p \in Z$.

Lemma 3:

$$T_p(N) = \begin{cases} T_p(0) & p \text{ even} \\ -T_p(0) & p \text{ odd} \end{cases}$$

Proof: For $p \neq 0$,

$$\begin{aligned} T_p(N) &= \sqrt{\left(\frac{2}{N}\right)} \cos\frac{(2N+1)p\pi}{2N} \\ &= \begin{cases} \sqrt{\left(\frac{2}{N}\right)} \cdot \cos\frac{p\pi}{2N} & p \text{ even} \\ -\sqrt{\left(\frac{2}{N}\right)} \cdot \cos\frac{p\pi}{2N} & p \text{ odd} \end{cases} \\ &= \begin{cases} T_p(0) & p \text{ even} \\ -T_p(0) & p \text{ odd} \end{cases} \end{aligned}$$

For $p = 0$, $T_0(N) = T_0(0) = \sqrt{(1/N)}$.

Lemma 4:

$$\sum_{m=0}^{N-1} \cos\frac{(2m+1)p\pi}{2N} = \begin{cases} N & p = 0 \\ 0 & p \neq 0 \end{cases}$$

$$\sum_{m=0}^{N-1} \sin\frac{(2m+1)p\pi}{2N} = \begin{cases} (\sin p\pi/2N)^{-1} & p \text{ odd} \\ 0 & p \text{ even} \end{cases}$$

Proof: For $p = 0$,

$$\sum_{m=0}^{N-1} \cos\frac{(2m+1)0\pi}{2N} = N$$

$$\sum_{m=0}^{N-1} \sin\frac{(2m+1)0\pi}{2N} = 0$$

For $p \neq 0$,

$$\begin{aligned} \sum_{m=0}^{N-1} \cos\frac{(2m+1)p\pi}{2N} + j\sin\frac{(2m+1)p\pi}{2N} &= \sum_{m=0}^{N-1} e^{j(p\pi/2N)(2m+1)} \\ &= \frac{e^{j(p\pi/2N)} \cdot (1 - e^{j(p\pi/N)N})}{1 - e^{j(p\pi/N)}} \\ &= \begin{cases} 0 & p \text{ even} \\ \dfrac{2e^{j(p\pi/2N)}}{1 - e^{j(p\pi/N)}} & p \text{ odd} \end{cases} \end{aligned} \tag{30}$$

Similarly, we have

$$\sum_{m=0}^{N-1} \cos\frac{(2m+1)p\pi}{2N} - j\sin\frac{(2m+1)p\pi}{2N} = \begin{cases} 0 & p \text{ even} \\ \dfrac{2e^{-j(p\pi/2N)}}{1 - e^{-j(p\pi/N)}} & p \text{ odd} \end{cases} \tag{31}$$

1/2 (eqn. 30 + eqn. 31) $\Rightarrow$

$$\sum_{m=0}^{N-1} \cos\frac{(2m+1)p\pi}{2N} = 0 \quad \text{for all } p \neq 0$$

1/2j(eqn. 30 − eqn. 31) $\Rightarrow$

$$\sum_{m=0}^{N-1} \sin\frac{(2m+1)p\pi}{2N} = 0 \qquad \text{for } p \text{ even}$$

$$\sum_{m=0}^{N-1} \sin\frac{(2m+1)p\pi}{2N} = \left(\sin\frac{p\pi}{2N}\right)^{-1} \qquad \text{for } p \text{ odd}$$

Now we return to eqn 28; we have

$$S'_i = y_{N-1} \cdot T_{p_i}(0) + \sum_{m=0}^{N-2} y_m \cdot T_{p_i}(m+1)$$

By Lemma 2, eqn. 26 and eqn. 27, we can derive

$$S'_i = \sum_{n=0}^{K-1} x_n \cdot \left[T_{j_n}(N-1) \cdot (T_{p_i}(0) - T_{p_i}(N)) - \sqrt{\left(\frac{2}{N}\right)} \sin\frac{p_i\pi}{N} \sum_{m=0}^{N-1} T_{j_n}(m) \sin\frac{(2m+1)p_i\pi}{2N} \right]$$

Since $x_0, x_1, \ldots, x_{K-1}$ are K arbitrary real numbers, S'_i will be zero if and only if

$$T_{j_n}(N-1) \cdot (T_{p_i}(0) - T_{p_i}(N)) - \sqrt{\left(\frac{2}{N}\right)} \sin\frac{p_i\pi}{N} \sum_{m=0}^{N-1} T_{j_n}(m) \sin\frac{(2m+1)p_i\pi}{2N} \tag{32}$$

is zero.

(1) For $p_i = 0$, we have $T_{p_i}(0) - T_{p_i}(N) = 0$ (Lemma 3) and $\sin p_i\pi/N = 0$ (eqn. 9). Therefore eqn. 32 is zero, which means that row 0 of the DCT matrix can be a candidate for parity of a cyclic code.

(2) For $p_i \neq 0$, and p_i even, by Lemma 3, we can reduce eqn. 32 to

$$-\sqrt{\left(\frac{2}{N}\right)} \sin \frac{p_i \pi}{N} \sum_{m=0}^{N-1} T_{j_n}(m) \sin \frac{(2m+1)p_i \pi}{2N}$$

(a) If $j_n = 0$, then eqn. 32 can be further reduced to

$$-\frac{\sqrt{2}}{N} \sin \frac{p_i \pi}{N} \sum_{m=0}^{N-1} \sin \frac{(2m+1)p_i \pi}{2N}$$

and is zero by Lemma 4.

(b) If $j_n \neq 0$, and j_n is even, then eqn. 32 will be

$$-\frac{2}{N} \sin \frac{p_i \pi}{N} \sum_{m=0}^{N-1} \cos \frac{(2m+1)j_n \pi}{2N} \cdot \sin \frac{(2m+1)p_i \pi}{2N}$$

The summation of the product of cos and sin in the above equation can be transformed into two summations of sin which are both zero by Lemma 4 since both $j_n + p_i$ and $j_n - p_i$ are even. Therefore, eqn. 32 is zero for this case.

(c) If j_n is odd, then, with similar reasoning, eqn. 32 will not be zero since now $j_n + p_i$ and $j_n - p_i$ are both odd.

(3) For p_i odd, eqn. 32 is, by Lemma 3 again,

$$2T_{j_n}(N-1) \cdot T_{p_i}(0) - \sqrt{\left(\frac{2}{N}\right)} \cdot \sin \frac{p_i \pi}{N} \sum_{m=0}^{N-1} T_{j_n}(m) \sin \frac{(2m+1)p_i \pi}{2N}$$

(a) If $j_n = 0$, then the first term in the above equation is

$$2\sqrt{\left(\frac{1}{N}\right)} \cdot \sqrt{\left(\frac{2}{N}\right)} \cos \frac{p_i \pi}{2N}$$

and the second term can be reduced to, by Lemma 4,

$$\sqrt{\left(\frac{2}{N}\right)} \cdot \sin \frac{p_i \pi}{N} \sum_{m=0}^{N-1} \sqrt{\left(\frac{1}{N}\right)} \cdot \sin \frac{(2m+1)p_i \pi}{2N}$$
$$= \frac{\sqrt{2}}{N} \cdot 2 \sin \frac{p_i \pi}{2N} \cdot \cos \frac{p_i \pi}{2N} \cdot \left(\sin \frac{p_i \pi}{2N}\right)^{-1}$$

which is just equal to the first term. Thus eqn. 32 = 0.

(b) If $j_n \neq 0$, and j_n is even, then, with some effort, we can reduce eqn. 32 to

$$\frac{1}{N}\left(\sin \frac{j_n - p_i}{2N}\right)^{-1} \cdot \left(\sin \frac{j_n + p_i}{2N}\right)^{-1} \times \left(\sin \frac{j_n + p_i}{2N} + \sin \frac{j_n - p_i}{2N}\right) \cdot \left(\sin \frac{p_i}{N}\right)^{-1}$$

which will not be zero for all cases of j_n and p_i.

(c) If j_n is odd, then both $j_n + p_i$ and $j_n - p_i$ are even. Since we have already shown that the second term is zero for this condition (see 2b), we can simply write eqn. 32 as

$$2\sqrt{\left(\frac{2}{N}\right)} \cdot \cos \frac{(2N-1)j_n \pi}{2N} \cdot \sqrt{\left(\frac{2}{N}\right)} \cdot \cos \frac{p_i \pi}{2N}$$

which will not be zero for all cases of j_n and p_i.

From the above verification, we can make the following conclusions:

By (1): the $(N, N-1)$ DCT code containing only row 0 as its parity is a cyclic code.

By (2a) and (3a): the $(N, 1)$ DCT code containing row $1, 2, \ldots, N-1$ as its parities is also a cyclic code.

From (2c): we know that if a cyclic DCT code contains a nonzero even parity, then all odd rows must be included as parities. At the same time, from (3b): if a cyclic DCT code contains an odd parity, then all nonzero even rows must be included as parities. Therefore we cannot define any DCT cyclic codes, with the exception of the two trivial DCT cyclic codes.