NORTH-HOLLAND

On Algebras Related to the Discrete Cosine Transform

Ephraim Feig
IBM Research Division
Thomas J. Watson Research Center
P.O. Box 218
Yorktown Heights, New York 10598

and

Michael Ben-Or
The Institute of Mathematics and Computer Science
The Hebrew University
Jerusalem, Israel

Submitted by Richard A. Brualdi

ABSTRACT

An algebraic theory for the discrete cosine transform (DCT) is developed, which is analogous to the well-known theory of the discrete Fourier transform (DFT). Whereas the latter diagonalizes a convolution algebra, which is a polynomial algebra modulo a product of various cyclotomic polynomials, the former diagonalizes a polynomial algebra modulo a product of various polynomials related to the Chebyshev types. When the dimension of the algebra is a power of 2, the DCT diagonalizes a polynomial algebra modulo a product of Chebyshev polynomials of the first type. In both DFT and DCT cases, the Chinese remainder theorem plays a key role in the design of fast algorithms. © 1997 Elsevier Science Inc.

1. INTRODUCTION

The special properties which make the discrete Cosine transform (DCT) so well suited for image processing were first described in [1]. Essentially, the DCT nearly diagonalizes symmetric Toeplitz matrices whose off-diagonals

LINEAR ALGEBRA AND ITS APPLICATIONS 266:81–106 (1997)

655 Avenue of the Americas, New York, NY 10010
0024-3795/97/$17.00
PII S0024-3795(96)00634-9

decay exponentially. The N-point DCT matrix is defined to be the $N \times N$ matrix

$$(\tilde{C}_N)_{i,j} = \left(c_i \cos \frac{2\pi(2j-1)(i-1)}{4N} \right), \qquad 1 \leqslant i,j \leqslant N, \tag{1}$$

where

$$c_i = \begin{cases} \sqrt{1/N} & \text{for } \quad i = 1, \\ \sqrt{2/N} & \text{otherwise.} \end{cases} \tag{2}$$

If we define the $N \times N$ matrices

$$T_{N,\rho} = \left(\rho^{|i-j|} \right), \qquad 1 \leqslant i,j \leqslant N,$$

then for $0 \leqslant \rho \leqslant 1$, the matrices $\tilde{C}_N T_{N,\rho} \tilde{C}_N^{-1}$ are nearly diagonal. A more exact formulation was given by Jain [11], who showed that the DCT matrix $\tilde{C}_N$ diagonalizes a one-parameter family of $N \times N$ matrices

$$J_{\alpha,N} = \begin{pmatrix} 1-\alpha & -\alpha & 0 & 0 & \cdots & 0 \\ -\alpha & 1 & -\alpha & 0 & \cdots & 0 \\ 0 & -\alpha & 1 & -\alpha & \cdots & 0 \\ \vdots & \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & 0 & \cdots & -\alpha & 1 & -\alpha \\ 0 & 0 & \cdots & 0 & -\alpha & 1-\alpha \end{pmatrix}.$$

Jain's observation serves as a starting point for this paper. First observe that for any diagonal matrix D, the matrix $D\tilde{C}_N$ also diagonalizes $J_{\alpha,N}$. In this paper we will consider the so-called unnormalized DCT matrix C_N which is defined by Equation (1) with the coefficients c_i all equal to 1. The matrices $\tilde{C}_N$ are orthogonal; the matrices C_N are not. However, the various recursive relations that we will exhibit are more simply stated relative to the matrices C_N.

If C_N diagonalizes a matrix, it also diagonalizes the entire algebra generated by that matrix. To be precise, Jain observed that

$$C_N J_{\alpha,N} C_N^{-1} = D_{N,\alpha}, \tag{3}$$

where $D_{N,\alpha}$ is the $N \times N$ diagonal whose (m, m)th entry is $1 - \cos[(m - 1)/4N]$. Therefore for all constants k_j

$$C_N\left(\sum_{j=0}^{N-1} k_j J_\alpha^j\right)C_N^{-1} = \sum_{j=0}^{N-1} k_j D_{N,\alpha}^j \tag{4}$$

is again diagonal. This observation was already made by I. J. Good in [9], who introduced what he called the colleague matrix, a Chebyshev analogue to the companion matrix. It is precisely this analogy which we will further explore here.

The main concern of this paper is to describe the algebra generated by these $J_{\alpha,N}$. Since $J_{\beta,N} = I_N + (\beta/\alpha)(J_{\alpha,N} - I_N)$, where I_N is the $N \times N$ identity matrix, it follows that all the $J_{\alpha,N}$ as α ranges over the field of complex numbers, are in the same algebra.

Our object is to obtain an algebraic theory for the DCT which is analogous to the familiar one for the discrete Fourier transform (DFT). This will yield the analogue to the convolution property so well known with DFTs. It will also lead to a derivation of many of the well-known fast DCT algorithms, just as did the algebraic theory of the DFT provide a uniform approach to the many known FFTs. We do not introduce new algorithms here. Rather we provide a canonical setting for deriving the well-known algorithms of Chen, Smith, and Fralick [5], Wang [20], Lee [12], Suehiro and Hatori [17], Narasinha and Peterson [14], Tseng and Miller [18], Hou [10], Makhoul [13], among others. Each reference derives a fast DCT algorithm via a factorization (either explicit or implicit) of the DCT matrix. Most algebraic approaches to explaining fast transforms via factorizations consider the structure of the transform matrix itself; see Winograd [21] and Van Loan [22]. In [3] the authors take a different approach; they consider the action of the transform on a class of semisimple commutative algebras, and obtain factorizations for the DFT from this functorial approach. A similar approach is taken here for obtaining factorizations of the DCT. Here we will show that these factorizations can be derived as successive steps in either a full or partial diagonalization of an algebra associated with the cosine transform. Not all fast DCT algorithms can be directly derived using our construction. The algorithm of Vetterli and Nussbaumer [19] seems to rely on yet other algebraic properties.

The algebras and matrices discussed here are familiar entities in other fields. They are special sums of Toeplitz and Hankel matrices, which have been studied in connection with solutions of certain systems of equations [7, 16, 4, 6]. The paper by Bini and Bozzo [4] comes close to our approach here. They talk about the DFT diagonalizing the algebra of cyclic convolutions, but do not give an explicit description of the corresponding algebra for the DCT. This we do here, and we relate it to Chebyshev polynomials, cite the factorization result of Rivlin [15]—which he very graciously attributes to Shur (though the latter only hints at it in one brief sentence, whereas Rivlin devotes a whole new chapter in his second edition precisely to this description)—and then give the algorithmic implications.

In the rest of this introduction we review the algebraic theory of the DFT. It is well known that the DFT diagonalizes the convolution algebra, which is generated by the shift operator. This property is more familiar to the engineer as the statement that "convolution in the time domain is multiplication in the frequency domain." The N-dimensional convolution algebra is isomorphic to the ring of polynomials in the variable u with complex coefficients and multiplication modulo $u^N - 1$; this ring is called $\mathbb{C}[u]/\langle u^N - 1\rangle$. The shift operator corresponds to u in the algebra, and the monomials $1, u, u^2, \ldots, u^{N-1}$ form a "natural" basis for this algebra. It is convenient to consider the matrix representation of this algebra given by the correspondence

$$u \to U_N = \begin{pmatrix} 0 & 0 & 0 & \cdots & 0 & 1 \\ 1 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 1 & 0 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & 0 \end{pmatrix}.$$

The matrix U_N is the companion matrix of the polynomial $u^N - 1$, and is often called a circulant or cyclic matrix. The form and sparseness of the matrices U_N^k associated with the monomials u^k reflect the naturalness of this basis.

Let $\mathcal{F}_N$ denote the matrix of the unnormalized N-point DFT. It is defined as

$$(\mathcal{F}_N)_{j,k} = \left(\exp\frac{-2\pi i(j-1)(k-1)}{N}\right), \qquad 1 \leqslant i,j \leqslant N. \tag{5}$$

Then

$$\mathcal{F}_N U_N \mathcal{F}_N^{-1} = \mathcal{D}_N, \tag{6}$$

where $\mathcal{D}_N$ is the $N \times N$ diagonal matrix whose (j,j)th entry is $e^{2\pi i(j-1)/N}$. We say that the DFT diagonalizes the convolution algebra.

The DFT can be viewed as a change of basis given by the Chinese remainder theorem (CRT) isomorphism applied to the factorization

$$u^N - 1 = \prod_{j=0}^{N-1} \left(u - e^{2\pi i j/N}\right). \tag{7}$$

The following rational factorization into irreducible factors is classical:

$$u^N - 1 = \prod_{j|N} \Phi_j(u), \tag{8}$$

where Φ_j are the cyclotomic polynomials

$$\Phi_j(u) = (u - \zeta_1) \cdots \left(u - \zeta_{\phi(j)}\right), \tag{9}$$

$\zeta_1, \ldots, \zeta_{\phi(j)}$ are the primitive jth roots of unity, and $\phi(j)$ is the Euler totient function.

When N is even, the CRT isomorphism can be done in stages, corresponding to factoring $u^N - 1$ in stages. Thus, we can first factor

$$u^N - 1 = \left(u^{N/2} - 1\right)\left(u^{N/2} + 1\right), \tag{10}$$

and then factor each of the two factors above separately:

$$u^{N/2} - 1 = \prod_{j=0}^{(N/2)-1} \left(u - e^{4\pi i j/N}\right) \tag{11}$$

and

$$u^{N/2} + 1 = \prod_{j=0}^{(N/2)-1} \left(u - e^{2\pi i(2j+1)/N}\right). \tag{12}$$

The first factorization corresponds via the regular representation to the block diagonalization

$$R_N U_N R_N^{-1} = \begin{pmatrix} U_{N/2} & \\ & V_{N/2} \end{pmatrix}, \tag{13}$$

where $U_{N/2}$ is the companion matrix of $u^{N/2} - 1$, $V_{N/2}$ is the companion matrix of $u^{N/2} + 1$, and

$$R_N = \begin{pmatrix} I_{N/2} & I_{N/2} \\ I_{N/2} & -I_{N/2} \end{pmatrix}. \tag{14}$$

The CRT isomorphism describing the diagonalization of the algebra modulo $u^{N/2} - 1$ is simply the DFT on $N/2$ point. Letting $\mathscr{F}_{N/2}$ denote the matrix of the $N/2$-point DFT, we have

$$\mathscr{F}_{N/2} U_{N/2} \mathscr{F}_{N/2}^{-1} = \mathscr{D}_{N/2}, \tag{15}$$

where $\mathscr{D}_{N/2}$ is the $(N/2) \times (N/2)$ diagonal matrix whose (j, j)th entry is $e^{\pi(j-1)/N}$. The CRT isomorphism describing the diagonalization of the algebra modulo $u^{N/2} + 1$ (called the algebra of skew-circulant matrices) is described via the regular representation by

$$\mathscr{G}_{N/2} V_{N/2} \mathscr{G}_{N/2}^{-1} = \mathscr{E}_{N/2}, \tag{16}$$

where $\mathscr{E}_{N/2}$ is the $(N/2) \times (N/2)$ diagonal matrix whose (j, j)th entry is $e^{\pi(2j-1)/2N}$, and $\mathscr{G}_{N/2}$ is the Vandermonde matrix generated by the roots of unity $e^{\pi(2j-1)/2N}$. The matrices $\mathscr{F}_{N/2}$ and $\mathscr{G}_{N/2}$ are related as follows:

$$\mathscr{G}_{N/2} = \mathscr{F}_{N/2} \mathscr{E}_{N/2}. \tag{17}$$

The entries in the diagonal matrix $\mathscr{E}_{N/2}$ are the so-called twiddle factors.

The CRT applied via the factorization in Equation (7) can be done in stages: first apply it via Equation (10), and then apply it independently to each of the two direct summands via Equations (11) and (12). This translates to the matrix identity

$$\mathscr{F}_N = \tfrac{1}{2} P \begin{pmatrix} \mathscr{F}_{N/2} & \\ & \mathscr{G}_{N/2} \end{pmatrix} R_N = \tfrac{1}{2} P \begin{pmatrix} \mathscr{F}_{N/2} & \\ & \mathscr{F}_{N/2} \end{pmatrix} \begin{pmatrix} I_{N/2} & \\ & \mathscr{E}_{N/2} \end{pmatrix} R_n, \tag{18}$$

where P is the "even-odd" permutation matrix which rearranges the rows so that the even indexed rows are first, in order, followed by the odd indexed rows. If $N = 2^n$ is an integer power of 2, then this block diagonalization can be done recursively n times, and in this way we can design efficient divide-and-conquer algorithms for the DFT. These are the well-known FFT algorithms, which run in n stages.

Finally notice for $N = 2^n$ the complete rational factorization

$$u^N - 1 = (u - 1)\Phi_1(u)\Phi_2(u)\Phi_4(u)\cdots\Phi_{2^{n-1}}(u), \tag{19}$$

and $\Phi_{2^k}(u) = u^{2^k} + 1$. this implies that the N-point DFT matrix can be factored into a product of two matrices, the first a direct sum of Vandermonde matrices, each generated by roots of unity each of order 2^k, $0 \leqslant k \leqslant n$, and the second a rational matrix. This was used in [2] to determine the complexity of the DFT on input sizes which are powers of 2, and also has algorithmic consequences.

2. THE ALGEBRA OF THE DCT

The DCT matrix C_N diagonalizes $J_{0.5,N}$ and therefore also the matrix $I_N - J_{0.5,N}$. It can be shown, and indeed quite straightforwardly from Jain's results, that the eigenvalues of $I_N - J_{0.5,N}$ are $\cos(\pi j/N)$, $j = 0, 1, \dots, N - 1$. Therefore the minimal polynomial $q_N(u)$ of $I_N - J_{0.5,N}$ is its characteristic polynomial, namely

$$q_N(u) = \prod_{j=0}^{N-1}\left(u - \cos\frac{\pi j}{N}\right). \tag{20}$$

This polynomial is related to the well-known Chebyshev polynomial of the second type, $U_N(u)$, by the relation

$$U_N(u) = \frac{q_N(u)}{u - 1}. \tag{21}$$

Rivlin [15] gives the rational factorization of these polynomials. Consider $N \geqslant 2$ and let h be a divisor of $2N$. Define

$$G_{h,N}(u) = \prod_{\substack{j=1\\(j,2N)=h}}^{N-1}\left(u - \cos\frac{\pi j}{N}\right). \tag{22}$$

Rivlin shows that $G_{h,N}$ is monotonic, has integer coefficients, and is irreducible over the rationals. Then he shows

$$U_N(u) = \prod_{\substack{h|2N\\1\leqslant h\leqslant N-1}} G_{h,N}(u), \tag{23}$$

from which we obtain

$$q_N(u) = (u - 1) \prod_{\substack{h|2N \\ 1 \leqslant h \leqslant N-1}} G_{h,N}(u), \tag{24}$$

A very interesting case is for $N = 2^n$, an integer power of 2. Here the factors $G_{h,N}$ in Equation (23) are all of the form

$$G_{2^k,2^n}(u) = \prod_{j=1}^{2^{n-k}-1} \left(u - \cos \frac{\pi(2j-1)}{2^{n-k+1}} \right) = \psi_{2^{n-k}}(u), \tag{25}$$

where ψ_j denotes the Chebyshev polynomial of first type. Thus

$$q_{2^n}(u) = (u - 1)\psi_1(u)\psi_2(u)\psi_4(u) \cdots \psi_{2^{n-1}}(u). \tag{26}$$

In a sense our problem is solved; we have characterized the algebras of the DCT. The purpose of the paper is to provide insight into these algebras from an engineering point of view. That is, we will mimic the structure theory for the convolution algebra and its relation to the DFT. We will find natural bases for the algebras of the DCT, analogous to bases of the algebras of the DFT which are composed of powers of the companion matrix to the polynomials $u^N - 1$. And we will use our algebraic results to demonstrate a recursive structure for the DCT in the case $N = 2^n$ similar to that of the DFT. As with the DFT, here too the recursive structure will have significant algorithmic implications. Our arguments will provide an independent proof for Equation (26).

3. ON JAIN'S FAMILY OF TRANSFORMS

In his paper, Jain actually considers unitary transforms which diagonalize families matrices of the form

$$\begin{pmatrix} 1 - k_1\alpha & -\alpha & 0 & \cdots & \cdots & k_3\alpha \\ -\alpha & 1 & -\alpha & 0 & \cdots & 0 \\ 0 & -\alpha & 1 & -\alpha & \cdots & 0 \\ \vdots & \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & 0 & \cdots & -\alpha & 1 & -\alpha \\ k_4\alpha & 0 & \cdots & 0 & -\alpha & 1 - k_2\alpha \end{pmatrix},$$

for various choices of k_j. As we have already observed, a transform which diagonalizes a matrix diagonalizes the entire algebra generated by that matrix. In this paper we will focus on these algebras, and for later reference, we change Jain's notation and define the matrices

$$J_{k_1,k_2,k_3,k_4} = \frac{1}{2}\begin{pmatrix} k_1 & 1 & 0 & \cdots & \cdots & k_3 \\ 1 & 0 & 1 & 0 & \cdots & 0 \\ 0 & 1 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 & 0 & 1 \\ k_4 & 0 & \cdots & 0 & 1 & k_2 \end{pmatrix}.$$

We should have had one more subscript in our notation for the J matrix, namely its dimension. But whenever it does not explicitly enter the discussion we will drop it from the notation, anticipating no confusion.

The algebras generated by J_{k_1,k_2,k_3,k_4} are the same as those generated by Jain's matrices. In Table 1 we list five classes from Jain's list, which we will encounter here. The transformations T_{k_1,k_2,k_3,k_4} are the diagonalizers of the algebras; that is,

$$T_{k_1,k_2,k_3,k_4} J_{k_1,k_2,k_3,k_4} T^{-1}_{k_1,k_2,k_3,k_4} = D_{k_1,k_2,k_3,k_4}, \tag{27}$$

and D_{k_1,k_2,k_3,k_4} is diagonal; its entries are the eigenvalues listed in the table. (The last row of the even-sine-2 transform was not printed corrected in Jain's original paper.)

The first algebra (assume for the rest of the section that N is fixed, so that we can speak of algebras rather than classes of algebras) is the one most people are familiar with. Recall the convolution algebra generated by U, the companion matrix to $u^N - 1$, and with the natural basis U^j, which are "shifted" versions of the generator. This algebra is diagonalized by the DFT. Now

$$J_{0,0,1,1} = \frac{U + U^{-1}}{2},$$

so the algebra it generates is a subalgebra of the convolution algebra and is again diagonalizable by the DFT. Let us call this subalgebra $\mathscr{S}$, or $\mathscr{S}_N$ if we want to highlight the dimension.

TABLE 1

FIVE CLASSES FROM JAIN'S FAMILY OF UNITARY TRANSFORMS [5]

No.	J-matrix parameters	Transform name[a]	Transform matrix, $1 \leqslant m, k \leqslant N$	Eigenvalues
1	$k_1 = k_2 = 0,$ $k_3 = k_4 = 1$	DFT	$\frac{1}{\sqrt{N}} \exp \frac{2\pi i(m-1)(k-1)}{N}$	$\cos \frac{2\pi(m-1)}{N}$
2	$k_1 = k_2 = 1,$ $k_3 = k_3 = 0$	DCT	$\frac{1}{\sqrt{N}}, \; m = 1, 1 \leqslant k \leqslant N,$ $\sqrt{\frac{2}{N}} \cos \frac{\pi(2k-1)(m-1)}{2N},$ $m = 2, \ldots, N$	$\cos \frac{\pi(m-1)}{N}$
3	$k_1 = k_2 = -1,$ $k_3 = k_4 = 0$	Even-sine-2 (EDST-2)	$\sqrt{\frac{2}{N}} \sin \frac{\pi(2k-1)m}{2N}, \quad m \neq N,$ $\frac{(-1)^{k-1}}{\sqrt{N}} \quad m = N$	$\cos \frac{\pi m}{N}$
4	$k_1 = 1, k_2 = -1,$ $k_3 = k_4 = 0$	Even-cosine-2 (EDCT-2)	$\sqrt{\frac{2}{N}} \cos \frac{\pi(2k-1)(2m-1)}{2N}$	$\cos \frac{\pi(2m-1)}{2N}$
5	$k_1 = -1, k_2 = 1,$ $k_3 = k_4 = 0$	Even-sine-3 (EDST-3)	$\sqrt{\frac{2}{N}} \sin \frac{\pi(2k-1)(2m-1)}{2N}$	$\cos \frac{\pi(2m-1)}{2N}$

[a] Nowadays transforms 2 and 4 are called DCT-II and DCT-III, respectively.

Recall the Chebyshev polynomial ψ_j defined as $\psi_0(x) = 1$, $\psi_1(x) = x$, and recursively,

$$\psi_m(x) = 2x\psi_{m-1}(x) - \psi_{m-2}(x). \tag{28}$$

One can check by direct computation that

$$\psi_m(J_{0,0,1,1}) = = \frac{U^m + U^{-m}}{2}. \tag{29}$$

It is easy to see that the matrices $\psi_m(J_{0,0,1,1})$, with m ranging from 0 to $(N+1)/2$ if N is odd and to $(N+2)/2$ if N is even, form a basis for this subalgebra. Because of the sparseness and "cyclical" structure of these matrices, we say that they form a natural basis for this subalgebra.

The second algebra is generated by $J_{1,1,0,0}$; this algebra is the focus of this paper, and is diagonalized by the DCT. We will see that Chebyshev iterates $\psi_m(J_{1,1,0,0})$ form a natural basis for this algebra.

The third algebra is generated by $J_{-1,-1,0,0}$ and is diagonalized by what Jain calls the "even-sine-2" transform (the eigenvector corresponding to $m = N$ in our Table 1 was printed incorrectly in Jain's original paper). The fourth and fifth algebras are generated by $J_{-1,1,0,0}$ and $J_{1,-1,0,0}$, respectively, and are diagonalized by what Jain called the even-cosine-2 and the even-sine-3 transforms. Here too we will see that Chebyshev iterates form a natural basis for all these algebras.

For the remainder of the paper we will use a simpler notation for our special algebras and their generators. We will label them by their number as listed in Table 1, and we will highlight their dimensions. Specifically, $\mathscr{A}_{(j,N)}$ and $J_{(j,N)}$ will denote, respectively, the N-dimensional algebra and its generator, listed as the jth class of Table 1.

4. MOTIVATING EXAMPLE

For any field Φ and square matrix M, we define $\mathscr{A}_\Phi[M]$ to be the algebra generated by M with coefficients from Φ. For the remainder of this section, for the sake of exposition, let us take $N = 8$ and $\Phi = \mathbb{C}$, the field of complex numbers. The matrix

$$J_{(2,8)} = \frac{1}{2}\begin{pmatrix} 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \end{pmatrix} \in \mathscr{A}_{\mathbb{C}}[J_\alpha]$$

plays a special role. Recalling from the previous section the Chebyshev polynomials ψ_j, one can check by direct computation that

$$\psi_2(J_{(2,8)}) = \frac{1}{2}\begin{pmatrix} 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 \end{pmatrix},$$

$$\psi_3(J_{(2,8)}) = \frac{1}{2}\begin{pmatrix} 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \end{pmatrix},$$

$$\psi_4(J_{(2,8)}) = \frac{1}{2}\begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 \end{pmatrix},$$

$$\psi_5(J_{(2,8)}) = \frac{1}{2}\begin{pmatrix} 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \end{pmatrix},$$

$$\psi_6(J_{(2,8)}) = \frac{1}{2}\begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \end{pmatrix},$$

$$\psi_7(J_{(2,8)}) = \frac{1}{2}\begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix},$$

$$\psi_8(J_{(2,8)}) = \frac{1}{2}\begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

The Chebyshev iterates unfold in a rather dramatic way. Here is truly an example of a picture worth a thousand words. Clearly $\psi_8^2(J_{(2,8)})$ is the identity I, so that the minimal polynomial $q_8(u)$ of $J_{(2,8)}$ is a divisor of $\psi_8^2(u) - 1$. Because of the special structure of these matrices, we say that $\psi_j(J_{(2,8)})$, $0 \leqslant j \leqslant 7$, are a natural basis for this algebra. We will next determine the characteristic polynomial of $J_{(2,8)}$. We will see that it is in fact the minimal polynomial of $J_{(2,8)}$, and furthermore, our method for this determination will have algorithmic implications.

For any integer N, let I_N denote the $N \times N$ identity matrix and let $\tilde{I}_N$ denote the $N \times N$ matrix obtained from I_N by reversing the order of its columns. We next introduce the 8×8 permutation matrix

$$E_8 \begin{pmatrix} I_4 & \\ & \tilde{I}_4 \end{pmatrix}.$$

Then

$$E_8 J_{(2,8)} E_8^{-1} = \frac{1}{2} \begin{pmatrix} 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \end{pmatrix}.$$

This matrix has the form

$$\begin{pmatrix} A & B \\ B & A \end{pmatrix},$$

where A and B are 4×4 matrices (this partitioning is related to the persymmetry property, which has been observed in many places), and it is easily verified that

$$R_8 \begin{pmatrix} A & B \\ B & A \end{pmatrix} R_8^{-1} = \begin{pmatrix} A + B & \\ & A - B \end{pmatrix}$$

is block diagonal, where R_8 is as defined in Equation (14). This suggests that we define for every integer N the $N \times N$ matrix

$$\tilde{R}_8 = R_8 E_8 = \begin{pmatrix} I_4 & \tilde{I}_4 \\ I_4 & -\tilde{I}_4 \end{pmatrix}.$$

We then obtain

$$\tilde{R}_8 J_{(2,8)} \tilde{R}_8^{-1} = \frac{1}{2}\begin{pmatrix} 1 & 1 & 0 & 0 & & & & \\ 1 & 0 & 1 & 0 & & & & \\ 0 & 1 & 0 & 1 & & & & \\ 0 & 0 & 1 & 1 & & & & \\ & & & & 1 & 1 & 0 & 0 \\ & & & & 1 & 0 & 1 & 0 \\ & & & & 0 & 1 & 0 & 1 \\ & & & & 0 & 0 & 1 & -1 \end{pmatrix} = \begin{pmatrix} J_{(2,4)} & \\ & J_{(4,4)} \end{pmatrix}. \tag{30}$$

The top left 4 × 4 block is a generator for the algebra $\mathscr{A}_{(2,4)}$ of the four-point DCT. Computing its Chebyshev iterates, we have

$$\psi_2(J_{(2,4)}) = \frac{1}{2}\begin{pmatrix} 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{pmatrix},$$

$$\psi_3(J_{(2,4)}) = \frac{1}{2}\begin{pmatrix} 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 \end{pmatrix},$$

$$\psi_4(J_{(2,4)}) = \frac{1}{2}\begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix},$$

which is very reminiscent of the polynomial sequence for $J_{(2,8)}$. In particular, the minimal polynomial $q_4(u)$ of this $J_{(2,4)}$ is a divisor of $\psi_4^2(u) - 1$. Now every nontrivial polynomial $a(u)$ is relatively prime to both $a(u) + 1$ and $a(u) - 1$, and hence also to $a^2(u) - 1$. Therefore $\psi_4(u)$ is relatively prime to $\psi_4^2(u) - 1$. This will be important in later arguments.

The bottom 4 × 4 block, $J_{(4,4)}$, which is the generator for the algebra $\mathscr{A}_{(4,4)}$, behaves differently under Chebyshev iterations. We have

$$\psi_2(J_{(4,4)}) = \frac{1}{2}\begin{pmatrix} 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & -1 \\ 0 & 1 & -1 & 0 \end{pmatrix},$$

$$\psi_3(J_{(4,4)}) = \frac{1}{2}\begin{pmatrix} 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & -1 \\ 1 & 0 & -1 & 0 \\ 1 & -1 & 0 & 0 \end{pmatrix},$$

$$\psi_4(J_{(4,4)}) = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}.$$

Because the degree of ψ_4 is 4, it must be the characteristic polynomial of $J_{(4,4)}$. In fact, it is irreducible over $\mathbb{Q}$, and so it is also the minimal polynomial of $J_{(4,4)}$. Indeed it is well known [8] that for $K = 2^k$ an integer power of 2, the Chebyshev polynomials ψ_K are all irreducible over $\mathbb{Q}$. Recalling from the previous paragraph that ψ_4 and q_4 are relatively prime, this implies that

$$q_8(u) = q_4(u)\psi_4(u). \tag{31}$$

The structure of $J_{(2,4)}$ is obtained via a block diagonalization similar to the one above, yielding the 2 × 2 block $J_{(2,2)}$, which is further diagonalizable and whose minimal polynomial we will call $q_2(u)$, and an irreducible block $J_{(4,2)}$, whose minimal polynomial is ψ_2. One can check that $q_2(u) = (u - 1)u$, and recall that $\psi_1(u) = u$. Therefore we have shown how to block diagonalize $J_{(2,8)}$ to $\mathbb{Q}$-irreducible direct summands whose minimal polynomials over $\mathbb{Q}$ are $u - 1$, $\psi_1(u)$, $\psi_2(u)$, and $\psi_4(u)$. Hence the minimal polynomial of U_8 is

$$q_8(u) = (u - 1)\psi_1(u)\psi_2(u)\psi_4(u). \tag{32}$$

The total block diagonalization may be stated as follows: there exists a rational matrix $\mathscr{R}_8$ such that

$$\mathscr{R}_8 J_{(2,8)} \mathscr{R}_8^{-1} = \begin{pmatrix} 1 & & & \\ & J_{(4,1)} & & \\ & & J_{(4,2)} & \\ & & & J_{(4,4)} \end{pmatrix}. \qquad (33)$$

Returning to Equation (31), the diagonalization of $\mathscr{A}_{(2,8)}$ can be done in stages: first via the factorization given by Equation (31) and then each if the two direct summands can be diagonalized independently. The first direct summand is $\mathscr{A}_{(2,4)}$, which can be diagonalized by the four-point DCT; the second is $\mathscr{A}_{(5,4)}$, which is diagonalized by the four-point even-sine-3 transform.

5. ALGORITHMIC IMPLICATIONS

Equation (3) shows that the eight-point DCT matrix C_8 diagonalizes U_8. As with the DFT, the DCT factorization can be done in stages beginning with the bock diagonalization highlighted by Equation (30), namely that the matrix R_8 block diagonalizes U_8 into two subblocks, one U_4 and the other V_4, whose minimal polynomials is ψ_4. The complete factorization is then accomplished by diagonalizing the subblock U_4 with the four-point DCT matrix C_4, whereas the subblock V_4 is diagonalizable by a matrix we will call L_4. Explicitly,

$$(L_4)_{i,j} = \cos\left(\frac{\pi(2i-1)(2j-1)}{32}\right), \qquad 1 \leqslant i, j \leqslant 4. \qquad (34)$$

This sequence of factorizations implies the matrix identity

$$C_8 = P_8 \begin{pmatrix} C_4 & \\ & L_4 \end{pmatrix} \tilde{R}_8,$$

where P_8 is the permutation matrix mapping

$$(a_0 \quad a_1 \quad a_2 \quad a_3 \quad a_4 \quad a_5 \quad a_6 \quad a_7) P_8$$

$$= \begin{pmatrix} a_0 & a_2 & a_4 & a_6 & a_1 & a_3 & a_5 & a_7 \end{pmatrix}.$$

One checks directly that

$$L_4 = \frac{1}{2}\begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

$$\times C_4 \begin{pmatrix} \sec(\pi/16) & & & \\ & \sec(3\pi/16) & & \\ & & \sec(5\pi/16) & \\ & & & \sec(7\pi/16) \end{pmatrix}. \tag{35}$$

This is the analogue to the twiddle-factor identity (17) for the DCT with $N = 8$, and it suggests a divide-and-conquer approach to computing the product by C_8. We have the block diagonalization

$$\begin{pmatrix} C_2 & \\ & L_2 \end{pmatrix} = \tfrac{1}{2} P_4 C_4 \tilde{R}_4,$$

where

$$P_4 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

and

$$\tilde{R}_4 = \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & -1 \\ 0 & 1 & -1 & 0 \end{pmatrix}.$$

Also

$$L_2 = \frac{1}{2}\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} C_4 \begin{pmatrix} \sec(\pi/8) & \\ & \sec(3\pi/8) \end{pmatrix}. \tag{36}$$

Let us introduce the symbols $T_m(C_N)$ to denote the number of multiplications an algorithm uses to compute the product by C_N, and $T(C_N)$ to denote the total number of arithmetic operations the algorithm uses (the algorithm will be understood in the context of the discussion). Then using our divide-and-conquer approach,

$$T_m(C_8) = 4 + 2T_m(C_4),$$

$$T(C_8) = 15 + 2T(C_4).$$

Similarly

$$T_m(C_4) = 2 + 2T_m(C_2),$$

$$T(C_4) = 7 + 2T(C_2),$$

and

$$T_m(C_2) = 1, \qquad T(C_2) = 3.$$

Therefore,

$$T_m(C_8) = 12, \qquad T(C_8) = 29.$$

A different class of algorithms can be constructed from the factorization in Equation (33). Again from [8], there exist signed-permutation matrices $P_{j,2}$ such that

$$P_{j,2}V_jP_{j,2}^{-1} = \tilde{V}_j, \qquad j = 2, 4,$$

and $\tilde{V}_j$ are signed-cyclic matrices. A signed-permutation matrix is one in which each row and column has only one nonzero entry, which is either 1 or -1. A signed-cyclic matrix is one whose product corresponds to polynomial multiplication modulo $u^j + 1$. Hence; the product with C_8 can be computed by first multiplying by R_8 and the computing various polynomial products modulo $u^4 + 1$ and $u^2 + 1$ and sign changes to account for the products with V_4 and V_2. The product with v_1 involves a single multiplication. Applicability of this observation relies on fast algorithms for polynomial multiplication modulo irreducible polynomials. This approach also yielded the complexity results in [8].

6. THE GENERAL CASE

The goal of this section is to generalize our motivating example of Section 3. We would like to demonstrate the "sparse circular" nature of the iterates of $J_{(2,N)}$ under the action of ψ_k and prove that $\psi_N(J_{(2,N)}) = \tilde{I}_N$ and $\psi_N(J_{(4,N)}) = 0$. We then exhibit a block diagonalization of $J_{(2,N)}$ for N even which generalizes the one given in Equation (30). Finally (and as a consequence), we demonstrate for $N = 2^n$ Equation (26), which gives the factorization into rationally irreducible factors of the minimal polynomial q_{2^n} of $J_{(2,2^n)}$.

We begin again with the convolution algebra $\mathbb{Q}[u]/\langle u^N - 1\rangle$ and its regular representation onto the ring $\mathscr{A}$ of $N \times N$ matrices generated by the companion matrix U_N of $u^N - 1$. While one can actually infer directly the structure of the Chebyshev iterates of $J_{(2,N)}$, we prefer to reduce everything from the power iterates of U_N. As we saw earlier, this algebra contains a subalgebra $\mathscr{S}$ with entries polynomials of the form $\sum_k a_k(u^k + u^{-k})/2$, and these are mapped via the regular representation to

$$\sum_k a_k U_N^{(k)} = \sum_k a_k \left(\frac{U_N^k + U_N^{-k}}{2} \right). \tag{37}$$

These particular summands form a natural basis in that these matrices are simple to describe; they are sums of a shifted version of U and its transpose. And as we saw above,

$$U_N^{(k+1)} = 2U_N^{(1)}U_N^{(k)} - U_N^{(k-1)}, \tag{38}$$

so that

$$\psi_k\left(U_N^{(1)}\right) = U_N^{(k)}. \tag{39}$$

For N even, the matrix R_N [defined by Equation (14)] block-diagonalizes the convolution algebra $\mathscr{A}$, and therefore also the subalgebra $\mathscr{S}$; this block diagonalization corresponds to the Chinese remainder isomorphism defined by the factorization $u^N - 1 = (u^{N/2} + 1)(u^{N/2} - 1)$. But observe (by simple direct computation) that the matrix

$$\tilde{P}_N = \begin{pmatrix} I_{N/2} & \\ & \tilde{I}_{N/2} \end{pmatrix} \tag{40}$$

acting as a change of basis matrix on $\mathcal{S}$ by

$$\tilde{P}_N U_N^{(1)} \tilde{P}_N^{-1} = \begin{pmatrix} M_{N/2} & K_{N/2} \\ K_{N/2} & M_{N/2} \end{pmatrix}, \tag{41}$$

where K_k denotes the $k \times k$ matrix whose entries are all 0 except in the (1, 1) and (k, k) position, where the entry is $\frac{1}{2}$, and $M_k = J_{(2,k)} - N_k$. Setting $\tilde{R}_k = R_k \tilde{P}_k$ (recall the matrix $\tilde{R}_8$ in Section 3), we have

$$\tilde{R}_N U_N^{(1)} \tilde{R}_N^{-1} = \begin{pmatrix} M_{N/2} + K_{N/2} & \\ & K_{N/2} - M_{N/2} \end{pmatrix} = \begin{pmatrix} J_{(2,N/2)} & \\ & J_{(3,N/2)} \end{pmatrix}. \tag{42}$$

It follows that

$$\tilde{R}_N \psi_k\left(U_N^{(1)}\right) \tilde{R}_N^{-1} = \begin{pmatrix} \psi_k\left(J_{(2,N/2)}\right) & \\ & \psi_k\left(J_{(3,N/2)}\right) \end{pmatrix}, \tag{43}$$

from which the sparse circular nature of the matrices $\psi_k(J_{(2,N/2)})$ and $\psi_k(J_{(3,N/2)})$ can readily be discerned.

In particular, for example, taking $k = N/2$, we have

$$\psi_{N/2}\left(U_N^{(1)}\right) = \begin{pmatrix} & I_{N/2} \\ I_{N/2} & \end{pmatrix}, \tag{44}$$

which implies that

$$\tilde{R}_N \psi_{N/2}\left(U_N^{(1)}\right) \tilde{R}_N^{-1} = \begin{pmatrix} \tilde{I}_{N/2} & \\ & -\tilde{I}_{N/2} \end{pmatrix}, \tag{45}$$

from which, by Equation (43),

$$\psi_{N/2}\left(J_{(2,N/2)}\right) = \tilde{I}_{N/2} \tag{46}$$

and

$$\psi_{N/2}\left(J_{(3,N/2)}\right) = -\tilde{I}_{N/2}. \tag{47}$$

This in turn implies that

$$\psi^2_{N/2}\big(J_{(2,\,N/2)}\big) = I_{N/2}, \tag{48}$$

so that the minimal polynomial $q_{N/2}$ of $J_{(2,\,N/2)}$ divides $\psi^2_{N/2} - 1$. Similarly, the minimal polynomial of $J_{(3,\,N/2)}$ also divides $\psi^2_{N/2} - 1$.

For $N = 2^{n+1}$, taking $k = 2^{n-1}$ we have

$$\psi_{2^{n-1}}(U_{2^{n+1}}) = \begin{pmatrix} 0 & I_{2^{n-1}} & 0 & I_{2^{n-1}} \\ I_{2^{n-1}} & 0 & I_{2^{n-1}} & 0 \\ 0 & I_{2^{n-1}} & 0 & I_{2^{n-1}} \\ I_{2^{n-1}} & 0 & I_{2^{n-1}} & 0 \end{pmatrix}, \tag{49}$$

which implies that

$$\tilde{R}_{2^{n+1}}\psi_{2^{n-1}}\big(U^{(1)}_{2^{n+1}}\big)\tilde{R}^{-1}_{2^{n+1}} = \begin{pmatrix} \tilde{I}_{2^{n-1}} & I_{2^{n-1}} & & \\ I_{2^{n-1}} & \tilde{I}_{2^{n-1}} & & \\ & & -\tilde{I}_{2^{n-1}} & I_{2^{n-1}} \\ & & I_{2^{n-1}} & -\tilde{I}_{2^{n-1}} \end{pmatrix}, \tag{50}$$

from which by Equation (43) we get

$$\psi_{2^{n-1}}\big(J_{(2,2^n)}\big) = \begin{pmatrix} \tilde{I}_{2^{n-1}} & I_{2^{n-1}} \\ I_{2^{n-1}} & \tilde{I}_{2^{n-1}} \end{pmatrix}. \tag{51}$$

Direct calculation shows that

$$\tilde{R}_{2^n}J_{(2,2^n)}\tilde{R}^{-1}_{2^n} = \begin{pmatrix} J_{(2,2^{n-1})} & \\ & J_{(4,2^{n-1})} \end{pmatrix} \tag{52}$$

and hence

$$\tilde{R}_{2^n}\psi_{2^{n-1}}\big(J_{(2,2^n)}\big)\tilde{R}^{-1}_{2^n}\begin{pmatrix} \psi_{2^{n-1}}\big(J_{(2,2^{n-1})}\big) & \\ & \psi_{2^{n-1}}\big(J_{(4,2^{n-1})}\big) \end{pmatrix}. \tag{53}$$

Also by direct calculation

$$\tilde{R}_{2^n}\begin{pmatrix} \tilde{I}_{2^{n-1}} & I_{2^{n-1}} \\ I_{2^{n-1}} & \tilde{I}_{2^{n-1}} \end{pmatrix}\tilde{R}_{2^n}^{-1} = \begin{pmatrix} \tilde{I}_{2^{n-1}} & \\ & 0 \end{pmatrix}. \tag{54}$$

Therefore

$$\psi_{2^{n-1}}\left(J_{(4,2^{n-1})}\right) = 0. \tag{55}$$

And since $\psi_{2^{n-1}}$ is irreducible over the rationals, it must be the minimum polynomial of $J_{(4,2^{n-1})}$.

Equation (52) also implies that the minimum polynomial q_{2^n} of $J_{(2,2^n)}$ divides the product of $\psi_{2^{n-1}}$ and $q_{2^{n-1}}$, the minimum polynomial of $J_{(2,2^{n-1})}$. And because all the ψ_{2^k} are irreducible over the rationals, a straightforward induction argument demonstrates Equation (25).

Equation (42) suggests, for N even, a factorization of the unnormalized DCT matrix C_N, with R_N as the leading factor, followed by a matrix which is a direct sum of $C_{N/2}$ and some other matrix which diagonalizes $J_{(3,N/2)}$ (an even-sine 2 matrix, using Jain's terminology). This is equivalent to saying that we apply the Chinese remainder theorem in stages: first decomposing the DCT algebra into two subalgebras, and then diagonalizing each of them independently. We compute explicitly

$$C_N = \begin{pmatrix} C_{N/2} & \\ & L_{N/2} \end{pmatrix}\tilde{R}_N, \tag{56}$$

where $L_{N/2}$ is the $(N/2) \times (N/2)$ matrix whose (j,k)th entry is $\cos[\pi(2j-1)(2k-1)/2N]$. Define the $N \times N$ diagonal matrix D_N whose (k,k)th entry is $\frac{1}{2}\sec[\pi(2k-1)/2N]$ and the $N \times N$ matrix

$$Y_N = \begin{pmatrix} 1 & 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & 1 & \cdots & 0 & 0 \\ 0 & 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & 1 \\ 0 & 0 & 0 & \cdots & 0 & 1 \end{pmatrix}.$$

Recalling the cosine identity

$$2\cos a\cos b = \cos(a+b) + \cos(a-b), \tag{57}$$

we obtain by direct calculation [8]

$$L_N = D_N C_N Y_N. \tag{58}$$

The algorithmic significance of Equations (56) and (58) is apparent. One can compute the product with C_N by first computing a product with $\tilde{R}_N$ and then computing independently products with $C_{N/2}$ and $L_{N/2}$. The latter can be done by computing a product by $Y_{N/2}$ followed by a product by $C_{N/2}$ and then followed by the twiddle-factor product, $D_{N/2}$. For $N = 2^n$ this leads to a divide-and-conquer approach. Letting $T_m(C_N)$ denote the number of multiplications used by the algorithm obtained via this approach, and $T(C_N)$ denote the total number of arithmetic operations, we have for $N = 2^n$ the recurrence relations

$$T_m(N) = \frac{N}{2} + 2T_m\left(\frac{N}{2}\right), \tag{59}$$

$$T(N) = (2N - 1) + 2T\left(\frac{N}{2}\right) \tag{60}$$

with the initial conditions

$$T_m(2) = 1, \qquad T(2) = 3. \tag{61}$$

Then

$$T_m(N) = \frac{N}{2} \log_2 N, \tag{62}$$

$$T(N) = 2N \log_2 N - N + 1. \tag{63}$$

7. CONCLUSIONS

We have presented an algebraic theory for the discrete cosine transform which is analogous to the well-known theory of the discrete Fourier transform. Whereas the latter diagonalizes a convolution algebra, which is a polynomial algebra modulo a product of various cyclotomic polynomials, the former diagonalizes a polynomial algebra modulo a product of various polynomials related to the Chebyshev types. In both DFT and DCT cases, one can use the Chinese remainder theorem to design fast algorithms. As with the DFT, when the dimension of the algebra is a power of 2, these fast algorithms are of a divide-and-conquer nature. These algorithms are, in fact, the most popular fast DCT algorithms, but are not necessarily the most efficient known ones. The algebraic theory also leads to constructions which yield the multiplicative complexity of DCTs.

REFERENCES

1 N. Ahmed, T. Natarajan, and K. R. Rao, Discrete cosine transform, *IEEE Trans. Comput.* 23:90–93 (Jan. 1974).

2 L. Auslander, E. Feig, and S. Winograd, The multiplicative complexity of the discrete Fourier transform, *Adv. in Appl. Math.* 5:87–109 (1984).

3 L. Auslander, E. Feig, and S. Winograd, Abelian semi-simple algebras and algorithms for the discrete Fourier transform, *Adv. Appl. Math.* 5:31–55 (1984).

4 D. Bini and E. Bozzo, Fast discrete transforms by means of eigenpolynomials, *Comput. Math. Appl.* 26(9):35–52 (Nov. 1993).

5 W. H. Chen, C. H. Smith, and S. C. Fralick, A fast computational algorithm for the discrete cosine transform, *IEEE Trans. Commun.* COM-25:1004–009 (Sept. 1977).

6 L. Bergamaschi, R. Bevilacqua, and P. Zellini, Symplectic factorization and parallel iterative algorithms for tridiagonal systems of equations, *Calcolo* 29(3-4):159–191 (July, Dec. 1992).

7 F. Di Benedetto, Iterative solution of Toeplitz systems by preconditioning with discrete sine transform, *Proc. SPIE* 2563:302–312 (1995).

8 E. Feig and S. Winograd, On the Multiplicative Complexity of Discrete Cosine Transforms, IBM RC 15461 (No. 68749), 6 Feb. 1990; *IEEE Trans. Inform. Theory*, submitted for publication.

9 I. J. Good, The colleague matrix, a Chebyshev analogue of the companion matrix, *Quart. J. Math. Oxford* (2) 12:61–68 (1961).

10 H. S. Hou, A fast recursive algorithm for computing the discrete cosine transform, *IEEE Trans. Acoust. Speech Signal Process.* ASSP-35(10):1455–1461.

11 A. K. Jain, A sinusoidal family of unitary transforms, *IEEE Trans. Pattern Anal. Machine Intell.* PAMI-1(4):356–365 (Oct. 1979).

12 B. G. Lee, A new algorithm to compute the discrete cosine transform, *IEEE Trans. Acoust. Speech Signal Process.* ASSP-32(6):1243–1245 (Dec. 1984).

13 J. Makhoul, A fast cosine transform in one and two dimensions, *IEEE Trans. Acoust. Speech Signal Process.* ASSP-28(1):27–34 (Feb. 1980).

14 M. J. Narasinha and A. M. Peterson, On the computation of the discrete cosine transform, *IEEE Trans. Commun.* COM-26(6):934–936 (June 1978).

15 T. J. Rivlin, *Chebyshev Polynomials: From Approximation Theory to Algebra and Number Theory*, 2nd ed. Wiley-Interscience, 1990, pp. 228–230.

16 S. Serra, Multi-iterative methods, *Comput. Math. Appl.* 26(4):65–87 (1993).

17 N. Suehiro and M. Hatori, Fast algorithms for the DFT and other sinusoidal transforms, *IEEE Trans. Acoust. Speech Signal Process.* ASSP-34:642–644 (1986).

18 B. D. Tseng and W. C. Miller, On computing the discrete cosine transform, *IEEE Trans. Comput.* C-27:966–968 (Oct. 1978).

19 M. Vetterli and H. J. Nussbaumer, Simple FFT and DCT algorithms with reduced number of operations, *Signal Process.*, Aug. 1984.

20 Z. Wang, Fast algorithms for the discrete *W* transform and for the discrete Fourier transform, *IEEE Trans. Commun.* COM-25:1004–1008 (Sept. 1977).

21 S. Winograd, On computing the discrete Fourier transform, *Math. Comp.* 32:175–199 (1978).

22 C. Van Loan, *Computational Frameworks for the Fast Fourier Transform*, Frontiers Appl. Math., SIAM, 1992.

Received 2 October 1995; final manuscript accepted 30 October 1996