Algebraic Structure of the Discrete Cosine Transform

Ephraim Feig
IBM

Shmuel Winograd
Michael Ben-Or

Algebraic Theory of DFT

$$\mathcal{F} : L^2(\mathbb{Z}_N) \longrightarrow L^2(\mathbb{Z}_N)$$

$\mathcal{F}$ is the change of basis which diagonalizes the convolution algebra

$$\mathbb{C}[z]/\langle z^N - 1\rangle \xrightarrow{\mathcal{F}} \bigoplus_j \mathbb{C}[z]/\langle z - \omega^j\rangle$$

$$\omega = e^{2\pi i/N}$$

multiplication by z^n

$$p(z) \longrightarrow z^n p(z)$$

$$\Big\downarrow \mathcal{F}$$

phase shift $\quad \hat{p}(z') \longrightarrow \omega^{nz'} \hat{p}(z')$

Shift operator (z) generates the algebra, and

$$1, z, z^2, \dots, z^{N-1}$$

form a "natural basis"

$$\begin{matrix} 0&0&0&0&0&0&0&1\\ 1&0&0&0&0&0&0&0\\ 0&1&0&0&0&0&0&0\\ 0&0&1&0&0&0&0&0\\ 0&0&0&1&0&0&0&0\\ 0&0&0&0&1&0&0&0\\ 0&0&0&0&0&1&0&0\\ 0&0&0&0&0&0&1&0 \end{matrix} \qquad C$$

$$\begin{matrix} 0&0&0&0&0&0&1&0\\ 0&0&0&0&0&0&0&1\\ 1&0&0&0&0&0&0&0\\ 0&1&0&0&0&0&0&0\\ 0&0&1&0&0&0&0&0\\ 0&0&0&1&0&0&0&0\\ 0&0&0&0&1&0&0&0\\ 0&0&0&0&0&1&0&0 \end{matrix} \qquad C^2$$

$$\begin{matrix} 0&0&0&0&0&1&0&0\\ 0&0&0&0&0&0&1&0\\ 0&0&0&0&0&0&0&1\\ 1&0&0&0&0&0&0&0\\ 0&1&0&0&0&0&0&0\\ 0&0&1&0&0&0&0&0\\ 0&0&0&1&0&0&0&0\\ 0&0&0&0&1&0&0&0 \end{matrix} \qquad C^3$$

$$\begin{matrix} 0&0&0&0&1&0&0&0\\ 0&0&0&0&0&1&0&0\\ 0&0&0&0&0&0&1&0\\ 0&0&0&0&0&0&0&1\\ 1&0&0&0&0&0&0&0\\ 0&1&0&0&0&0&0&0\\ 0&0&1&0&0&0&0&0\\ 0&0&0&1&0&0&0&0 \end{matrix} \qquad C^4$$

$$\begin{matrix} 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \end{matrix} \qquad C^5$$

$$\begin{matrix} 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \end{matrix} \qquad C^6$$

$$\begin{matrix} 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{matrix} \qquad C^7$$

$$\begin{matrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{matrix} \qquad C^8 = I$$

$$\langle u^8 - 1 = 0 \rangle$$

Chinese Remainder Theorem

$$\mathbb{C}[z]/\langle z^8-1\rangle \cong \mathbb{C}[z]/\langle z^4-1\rangle \oplus \mathbb{C}[z]/\langle z^4+1\rangle$$

$\exists$ rational matrix R s.t.

$$R\, C_8 R^{-1} = \begin{pmatrix} C_4 & \\ & C_4' \end{pmatrix}$$

$$\mathcal{F}_8 = \begin{pmatrix} \mathcal{F}_4 & \\ & G_4 \end{pmatrix} R$$

$$G_4 = \mathcal{F}_4\, T_4$$

"twiddle factors"

Chinese Remainder Theorem

$$\mathbb{C}[z]/\langle z^8-1\rangle \cong \mathbb{C}[z]/\langle z^4-1\rangle \oplus \mathbb{C}[z]/\langle z^4+1\rangle$$

$\exists$ rational matrix R s.t

$$R\, C_8 R^{-1} = \begin{pmatrix} C_4 & \\ & C_4' \end{pmatrix}$$

$$\mathcal{F}_8 = \begin{pmatrix} \mathcal{F}_4 & \\ & G_4 \end{pmatrix} R$$

$$G_4 = \mathcal{F}_4 T_4$$

"twiddle factors"

$$\begin{matrix} 0 & 0 & 0 & -1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{matrix} \qquad A_{1/2}$$

$$\begin{matrix} 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{matrix} \qquad A_{1/2}^{2}$$

$$\begin{matrix} 0 & -1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -1 \\ 1 & 0 & 0 & 0 \end{matrix} \qquad A_{1/2}^{3}$$

$$\begin{matrix} -1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -1 \end{matrix} \qquad A_{1/2}^{4} = -\underline{I}$$

$$\langle x^4 + 1 = 0 \rangle$$

$$z^8 - 1 = (z^4 - 1)(z^4 + 1)$$

$$(z^2 - 1) \quad (z^2 + 1)$$

$$(z - 1) \quad (z + 1)$$

$$z^8 - 1 = (z-1)(z+1)(z^2+1)(z^4+1)$$

$$= (z-1)\,\varphi_1(z)\,\varphi_2(z)\,\varphi_4(z)$$

Convolution algebra $\Longleftrightarrow$ cyclotomic polynomials

DCT

Ahmed, Natarajan, Rao:

DCT 'nearly' diagonalizes certain Toeplitz matrices

Jain:

DCT diagonalizes all

$$J_\alpha = \begin{pmatrix} 1-\alpha & -\alpha & & & & \\ -\alpha & 1 & -\alpha & & & \\ & -\alpha & 1 & \ddots & & \\ & & \ddots & \ddots & \ddots & \\ & & & \ddots & 1 & -\alpha \\ & & & & -\alpha & 1-\alpha \end{pmatrix}$$

DCT diagonalizes the algebra generated by J_α; in particular

$$\mathcal{U} = -(J_{.5} - I) = \begin{pmatrix} .5 & .5 & & & & \\ .5 & 0 & .5 & & & \\ & .5 & 0 & \ddots & & \\ & & .5 & \ddots & \ddots & \\ & & & \ddots & 0 & .5 \\ & & & & .5 & .5 \end{pmatrix}$$

Describe the algebra generated by $\mathcal{U}$?

Chebychev polynomials

$$\psi_0(x) = 1$$

$$\psi_1(x) = x$$

$$\psi_k(x) = 2x\,\psi_{k-1}(x) - \psi_{k-2}(x)$$

observe:

$$\cos(kx) = 2\cos(x)\cos((k-1)x) - \cos((k-2)x)$$

$$
\begin{matrix}
0.5 & 0.5 & 0 & 0 & 0 & 0 & 0 & 0 \\
0.5 & 0 & 0.5 & 0 & 0 & 0 & 0 & 0 \\
0 & 0.5 & 0 & 0.5 & 0 & 0 & 0 & 0 \\
0 & 0 & 0.5 & 0 & 0.5 & 0 & 0 & 0 \\
0 & 0 & 0 & 0.5 & 0 & 0.5 & 0 & 0 \\
0 & 0 & 0 & 0 & 0.5 & 0 & 0.5 & 0 \\
0 & 0 & 0 & 0 & 0 & 0.5 & 0 & 0.5 \\
0 & 0 & 0 & 0 & 0 & 0 & 0.5 & 0.5
\end{matrix}
\qquad m
$$

$$
\begin{matrix}
0 & 0.5 & 0.5 & 0 & 0 & 0 & 0 & 0 \\
0.5 & 0 & 0 & 0.5 & 0 & 0 & 0 & 0 \\
0.5 & 0 & 0 & 0 & 0.5 & 0 & 0 & 0 \\
0 & 0.5 & 0 & 0 & 0 & 0.5 & 0 & 0 \\
0 & 0 & 0.5 & 0 & 0 & 0 & 0.5 & 0 \\
0 & 0 & 0 & 0.5 & 0 & 0 & 0 & 0.5 \\
0 & 0 & 0 & 0 & 0.5 & 0 & 0 & 0.5 \\
0 & 0 & 0 & 0 & 0 & 0.5 & 0.5 & 0
\end{matrix}
\qquad P_2(m)
$$

$$
\begin{matrix}
0 & 0 & 0.5 & 0.5 & 0 & 0 & 0 & 0 \\
0 & 0.5 & 0 & 0 & 0.5 & 0 & 0 & 0 \\
0.5 & 0 & 0 & 0 & 0 & 0.5 & 0 & 0 \\
0.5 & 0 & 0 & 0 & 0 & 0 & 0.5 & 0 \\
0 & 0.5 & 0 & 0 & 0 & 0 & 0 & 0.5 \\
0 & 0 & 0.5 & 0 & 0 & 0 & 0 & 0.5 \\
0 & 0 & 0 & 0.5 & 0 & 0 & 0.5 & 0 \\
0 & 0 & 0 & 0 & 0.5 & 0.5 & 0 & 0
\end{matrix}
\qquad P_3(m)
$$

$$
\begin{matrix}
0 & 0 & 0 & 0.5 & 0.5 & 0 & 0 & 0 \\
0 & 0 & 0.5 & 0 & 0 & 0.5 & 0 & 0 \\
0 & 0.5 & 0 & 0 & 0 & 0 & 0.5 & 0 \\
0.5 & 0 & 0 & 0 & 0 & 0 & 0 & 0.5 \\
0.5 & 0 & 0 & 0 & 0 & 0 & 0 & 0.5 \\
0 & 0.5 & 0 & 0 & 0 & 0 & 0.5 & 0 \\
0 & 0 & 0.5 & 0 & 0 & 0.5 & 0 & 0 \\
0 & 0 & 0 & 0.5 & 0.5 & 0 & 0 & 0
\end{matrix}
\qquad P_4(m)
$$

$$\begin{matrix} 0 & 0 & 0 & 0 & 0.5 & 0.5 & 0 & 0 \\ 0 & 0 & 0 & 0.5 & 0 & 0 & 0.5 & 0 \\ 0 & 0 & 0.5 & 0 & 0 & 0 & 0 & 0.5 \\ 0 & 0.5 & 0 & 0 & 0 & 0 & 0 & 0.5 \\ 0.5 & 0 & 0 & 0 & 0 & 0 & 0.5 & 0 \\ 0.5 & 0 & 0 & 0 & 0 & 0.5 & 0 & 0 \\ 0 & 0.5 & 0 & 0 & 0.5 & 0 & 0 & 0 \\ 0 & 0 & 0.5 & 0.5 & 0 & 0 & 0 & 0 \end{matrix} \qquad P_5(m)$$

$$\begin{matrix} 0 & 0 & 0 & 0 & 0 & 0.5 & 0.5 & 0 \\ 0 & 0 & 0 & 0 & 0.5 & 0 & 0 & 0.5 \\ 0 & 0 & 0 & 0.5 & 0 & 0 & 0 & 0.5 \\ 0 & 0 & 0.5 & 0 & 0 & 0 & 0.5 & 0 \\ 0 & 0.5 & 0 & 0 & 0 & 0.5 & 0 & 0 \\ 0.5 & 0 & 0 & 0 & 0.5 & 0 & 0 & 0 \\ 0.5 & 0 & 0 & 0.5 & 0 & 0 & 0 & 0 \\ 0 & 0.5 & 0.5 & 0 & 0 & 0 & 0 & 0 \end{matrix} \qquad P_6(m)$$

$$\begin{matrix} 0 & 0 & 0 & 0 & 0 & 0 & 0.5 & 0.5 \\ 0 & 0 & 0 & 0 & 0 & 0.5 & 0 & 0.5 \\ 0 & 0 & 0 & 0 & 0.5 & 0 & 0.5 & 0 \\ 0 & 0 & 0 & 0.5 & 0 & 0.5 & 0 & 0 \\ 0 & 0 & 0.5 & 0 & 0.5 & 0 & 0 & 0 \\ 0 & 0.5 & 0 & 0.5 & 0 & 0 & 0 & 0 \\ 0.5 & 0 & 0.5 & 0 & 0 & 0 & 0 & 0 \\ 0.5 & 0.5 & 0 & 0 & 0 & 0 & 0 & 0 \end{matrix} \qquad P_7(m)$$

$$\begin{matrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{matrix} \qquad P_8(m)$$

$$\left\langle P_8(n)^2 - 1 = 0 \right\rangle$$

Describe this algebra

$$\psi_p(u)^2 - 1 = 0$$

minimal polynomial of u

divides $\psi_p(u)^2 - 1$.

Let's compute it explicitly

in such a way which will

have algorithmic implications

$$
\begin{matrix}
0.5 & 0.5 & 0 & 0 & 0 & 0 & 0 & 0 \\
0.5 & 0 & 0.5 & 0 & 0 & 0 & 0 & 0 \\
0 & 0.5 & 0 & 0.5 & 0 & 0 & 0 & 0 \\
0 & 0 & 0.5 & 0 & 0.5 & 0 & 0 & 0 \\
0 & 0 & 0 & 0.5 & 0 & 0.5 & 0 & 0 \\
0 & 0 & 0 & 0 & 0.5 & 0 & 0.5 & 0 \\
0 & 0 & 0 & 0 & 0 & 0.5 & 0 & 0.5 \\
0 & 0 & 0 & 0 & 0 & 0 & 0.5 & 0.5
\end{matrix}
\qquad m
$$

$$
\begin{matrix}
1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\
0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 \\
0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & -1 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & -1 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 0 & -1 & 0 \\
1 & 0 & 0 & 0 & 0 & 0 & 0 & -1
\end{matrix}
\qquad S
$$

$$
\begin{array}{cccc|cccc}
0.5 & 0.5 & 0 & 0 & 0 & 0 & 0 & 0 \\
0.5 & 0 & 0.5 & 0 & 0 & 0 & 0 & 0 \\
0 & 0.5 & 0 & 0.5 & 0 & 0 & 0 & 0 \\
0 & 0 & 0.5 & 0.5 & 0 & 0 & 0 & 0 \\
\hline
0 & 0 & 0 & 0 & -0.5 & 0.5 & 0 & 0 \\
0 & 0 & 0 & 0 & 0.5 & 0 & 0.5 & 0 \\
0 & 0 & 0 & 0 & 0 & 0.5 & 0 & 0.5 \\
0 & 0 & 0 & 0 & 0 & 0 & 0.5 & 0.5
\end{array}
\qquad SmS^{-1} = \begin{pmatrix} M_{1/2} & \\ & N_{1/2} \end{pmatrix}
$$

$$S\,U_8\,S^{-1} = \begin{pmatrix} U_4 & \\ & V_4 \end{pmatrix}$$

$$\begin{matrix} -0.5 & 0.5 & 0 & 0 \\ 0.5 & 0 & 0.5 & 0 \\ 0 & 0.5 & 0 & 0.5 \\ 0 & 0 & 0.5 & 0.5 \end{matrix} \qquad V_4$$

$$\begin{matrix} 0 & -0.5 & 0.5 & 0 \\ -0.5 & 0 & 0 & 0.5 \\ 0.5 & 0 & 0 & 0.5 \\ 0 & 0.5 & 0.5 & 0 \end{matrix} \qquad \varphi_2(V_4)$$

$$\begin{matrix} 0 & 0 & -0.5 & 0.5 \\ 0 & -0.5 & 0 & 0.5 \\ -0.5 & 0 & 0.5 & 0 \\ 0.5 & 0.5 & 0 & 0 \end{matrix} \qquad \varphi_3(V_4)$$

$$\begin{matrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{matrix} \qquad \varphi_4(V_4)$$

φ_4 is $\mathbb{Q}$-irreducible

is the minimum polynomial of V_4

min. poly of u_8:

$$g_8(u) = g_4(u)\,\varphi_4(u)$$

$\uparrow$ min poly. of u_4

$$g_4(u) = g_2(u)\,\varphi_2(u)$$

$\uparrow$ min poly of u_2

$$g_2(u) = (u-1)\,\varphi_1(u)$$

$$g_8(u) = (u-1)\,\varphi_1(u)\,\varphi_2(u)\,\varphi_4(u)$$

We have used the fact that for $k = 2^n$, φ_k are all $\mathbb{Q}$-irreducible

$$S U_8 S^{-1} = \begin{pmatrix} U_4 & \\ & V_4 \end{pmatrix}$$

$$D_8 = \begin{pmatrix} D_4 & \\ & L_4 \end{pmatrix} S$$

<u>Theorem</u>:

$$L_4 = T_4 \, D_4 \, Y_4$$

$$T_4 = \begin{pmatrix} \cos 4\pi/8 & & & \\ & \cos 6\pi/8 & & \\ & & \cos 10\pi/8 & \\ & & & \cos 14\pi/8 \end{pmatrix}$$

$$Y_4 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \end{pmatrix}$$

Multiplicative (Ring) Theory

DFT : Winograd Construction

$\exists$ rational matrices R_1, R_2

s.t.

$$F = R_1 \begin{pmatrix} 1 & & & \\ & A_1 & & \\ & & A_2 & \\ & & & \ddots \end{pmatrix} R_2$$

A_j are elements in the representations of algebraic extension fields

Theorem: For $\underline{K} = 2^k$, $\exists$ signed permutation matrix $P_{\underline{K}}$ and rational matrix $R_{\underline{K}}$ s.t.

$$D_K = P_{\underline{K}} \mathcal{L}_{\underline{K}} R_{\underline{K}}$$

$$\mathcal{L}_{\underline{K}} = \begin{pmatrix} 1 & & & & \\ & L_1 & & & \\ & & L_2 & & \\ & & & \ddots & \\ & & & & L_{k-1} \end{pmatrix}$$

L_j are elements in the regular representation of

$$\mathbb{C}[u] / \langle u^{2^j} + 1 \rangle$$

Multidimensional DCTs

$$D_K \otimes D_K = (P_K \mathcal{L}_K R_K) \otimes (P_K \mathcal{L}_K R_K)$$

$$= (P_K \otimes P_K)(\mathcal{L}_K \otimes \mathcal{L}_K)(R_K \otimes R_K)$$

$$\mathcal{L}_K \otimes \mathcal{L}_K = \bigoplus_{m,n} L_m \otimes L_n$$

Tensor product of fields is isomorphic to a direct sum of fields.