

Algebraic Structure
of the Discrete
Cosine Transform

Ephraim Feig
IBM

Shmuel Winograd
Michael Ben-Or

Algebraic Theory of DFT

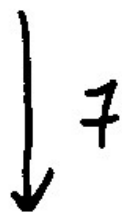
$$F: L^2(\mathbb{Z}_N) \longrightarrow L^2(\mathbb{Z}_N)$$

F is the change of basis which diagonalizes the convolution algebra

$$\mathbb{C}[z]/\langle z^N - 1 \rangle \xrightarrow{F} \bigoplus_j \mathbb{C}[z]/\langle z - \omega^j \rangle$$
$$\omega = e^{2\pi i/N}$$

multiplication by z^n

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



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

Shift operator (z) generates
the algebra, and

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

form a "natural basis"

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

C

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

C²

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

C³

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

C⁴

```

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

```

C^5

```

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

```

C^6

```

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

```

C^7

```

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

```

$C^8 = I$

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

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

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

$$F_8 = \begin{pmatrix} F_4 & \\ & G_4 \end{pmatrix} R$$

$$G_4 = F_4 T_4$$

← "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

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

$$F_8 = \begin{pmatrix} F_4 & \\ & G_4 \end{pmatrix} R$$

$$G_4 = F_4 T_4$$

\nwarrow "twiddle factors"

$$\begin{pmatrix} 0 & 0 & 0 & -1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

$$A_{1/2}$$

$$\begin{pmatrix} 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}$$

$$A_{1/2}^2$$

$$\begin{pmatrix} 0 & -1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -1 \\ 1 & 0 & 0 & 0 \end{pmatrix}$$

$$A_{1/2}^3$$

$$\begin{pmatrix} -1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}$$

$$A_{1/2}^4 = -I$$

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

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

$$\quad \quad \quad / \quad \backslash$$

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

$$\quad \quad \quad / \quad \backslash$$

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

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

$$= (z - 1) \phi_1(z) \phi_2(z) \phi_4(z)$$

Convolution algebra \iff

cyclotomic polynomials

Chebyshev polynomials

$$\psi_0(u) = 1$$

$$\psi_1(u) = u$$

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

observe:

$$\begin{aligned}\cos(ku) &= 2\cos(u)\cos((k-1)u) \\ &\quad - \cos((k-2)u)\end{aligned}$$

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

m

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

$P_2(m)$

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

$P_3(m)$

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

$P_4(m)$

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

$P_5(m)$

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

$P_6(m)$

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

$P_7(m)$

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

$P_8(m)$

$$\langle P_8(h)^2 - 1 = 0 \rangle$$

Describe this algebra

$$\varphi_p(x)^2 - 1 = 0$$

minimal polynomial of α

divides $\varphi_p(x)^2 - 1$.

Let's compute it explicitly

in such a way which will
have algorithmic implications

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

m

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

S

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
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

$S m S^{-1}$

$= \begin{pmatrix} M_{1/2} & \\ & N_{1/2} \end{pmatrix}$

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

$$\begin{pmatrix} -0.5 & 0.5 & 0 & 0 \\ 0.5 & 0 & 0.5 & 0 \\ 0 & 0.5 & 0 & 0.5 \\ 0 & 0 & 0.5 & 0.5 \end{pmatrix}$$

V_4

$$\begin{pmatrix} 0 & -0.5 & 0.5 & 0 \\ -0.5 & 0 & 0 & 0.5 \\ 0.5 & 0 & 0 & 0.5 \\ 0 & 0.5 & 0.5 & 0 \end{pmatrix}$$

$\psi_2(V_4)$

$$\begin{pmatrix} 0 & 0 & -0.5 & 0.5 \\ 0 & -0.5 & 0 & 0.5 \\ -0.5 & 0 & 0.5 & 0 \\ 0.5 & 0.5 & 0 & 0 \end{pmatrix}$$

$\psi_3(V_4)$

$$\begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

$\psi_4(V_4)$

ψ_4 is \mathbb{Q} -irreducible

is the minimum polynomial
of V_4

min. poly of U_8 :

$$f_8(u) = f_4(u) \psi_4(u)$$

↑

min poly. of U_4

$$f_4(u) = f_2(u) \psi_2(u)$$

↑

min poly of U_2

$$f_2(u) = (u-1) \psi_1(u)$$

$$f_8(u) = (u-1) \psi_1(u) \psi_2(u) \psi_4(u)$$

We have used the fact that

for $K = \mathbb{Z}^n$, ψ_n are all

\mathbb{Q} -irreducible

$$S U_8 S^{-1} = \begin{pmatrix} u_4 & \\ & v_4 \end{pmatrix}$$

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

Theorem :

$$L_4 = T_4 D_4 T_4$$

$$T_4 = \begin{pmatrix} \cos^{2\pi/8} & & & \\ & \cos^{6\pi/8} & & \\ & & \cos^{10\pi/8} & \\ & & & \cos^{14\pi/8} \end{pmatrix}$$

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

Multiplicative (Ring) Theory

DFT: Winograd Construction

\exists rational matrices R_1, R_2

s.t.

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

A_j are elements in the representations of algebraic extension fields

Theorem: For $K = \mathbb{Z}^k$, \exists
 signed permutation matrix P_K
 and rational matrix R_K s.t.

$$D_K = P_K Z_K R_K$$

$$Z_K = \begin{pmatrix} 1 & & & & \\ & L_1 & & & \\ & & L_2 & & \\ & & & \ddots & \\ & & & & L_{k-1} \end{pmatrix}$$

L_j are elements in the regular
 representation of

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

Multidimensional DCTs

$$\begin{aligned} D_k \otimes D_k &= (P_k Z_k R_k) \otimes (P_k Z_k R_k) \\ &= (P_k \otimes P_k) (Z_k \otimes Z_k) (R_k \otimes R_k) \end{aligned}$$

$$Z_k \otimes Z_k = \bigoplus_{m,n} L_m \otimes L_n$$

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