Lecture 26: The Fast Fourier Transform

David Woodruff

Thanks to Ryan O' Donnell for many slides

Polynomial multiplication

Let P(x) and Q(x) be polynomials of degree < N.

Assumed in "Coefficients Representation",

$$P(x) = a_0 + a_1 x + a_2 x^2 + \dots + a_{N-1} x^{N-1}$$

$$Q(x) = b_0 + b_1 x + b_2 x^2 + \dots + b_{N-1} x^{N-1}$$

Let $R(x) = P(x) \cdot Q(x)$, of degree < 2N.

Task is to get R(x) in Coefficients Representation.

Naively: takes $O(N^2)$ time to compute R(x)

Polynomial multiplication

Let P(x) and Q(x) be polynomials of degree < N.

Assumed in "Coefficients Representation",

Let $R(x) = P(x) \cdot Q(x)$, of degree < 2N. Task is to get R(x) in Coefficients Representation.



If only everything were in "Values Representation" instead...

Polynomial multiplication

Let P(x) and Q(x) be polynomials of degree < N.

Assumed in "Coefficients Representation",

Let $R(x) = P(x) \cdot Q(x)$, of degree < 2N.

Task is to get R(x) in Coefficients Representation.

If only we knew

P(1), P(2), ..., P(2N),

Q(1), Q(2), ..., Q(2N),

R(1), R(2), ..., R(2N)

uniquely determines R(x) by interpolation

A Divide and Conquer Approach

Want to evaluate P(x) at $x_1, x_2, ..., x_{2N}$ in $O(N \log N)$ time

Write
$$P(x) = P^{0}(x^{2}) + x P^{1}(x^{2})$$
, where

 $P^{0}(x)$ contains the even terms and $x \cdot P^{1}(x)$ contains the odd terms

Example:
$$P(x) = a_0 + a_1x + a_2x^2 + a_3x^3 + a_4x^4 + a_5x^5$$

$$P^0(x) = a_0 + a_2 x + a_4 x^2$$

$$P^{1}(x) = a_1 + a_3 x + a_5 x^2$$

Why is this useful?

A Divide and Conquer Approach

Want to evaluate P(x) at $x_1, x_2, ..., x_{2N}$ in $O(N \log N)$ time

Write $P(x) = P^{0}(x^{2}) + x P^{1}(x^{2})$, where

 $P^{0}(x)$ contains the even terms and $x \cdot P^{1}(x)$ contains the odd terms.

If my points are $x_1, x_2, ..., x_N, -x_1, -x_2, ..., -x_N$,

I just need the evaluations of $P^0(x)$ and $P^1(x)$ at $x_1^2, ..., x_N^2$

T(2N) = 2T(N) + O(N) with solution $T(2N) = O(N \log N)$, are we done?

We need points that can be recursively partitioned into +/-

Use the Complex Roots of Unity

Write $P(x) = P^{0}(x^{2}) + x P^{1}(x^{2})$, where

 $P^{0}(x)$ contains the even terms and $x \cdot P^{1}(x)$ contains the odd terms.

Choose 2N points to be the complex 2N-th roots of unity

Key fact: the 2N squares of the 2N-th roots of unity are: first the N N-th roots of unity, then again the N N-th roots of unity

T(2N) = 2T(N) + O(N) with solution $T(2N) = O(N \log N)$!!

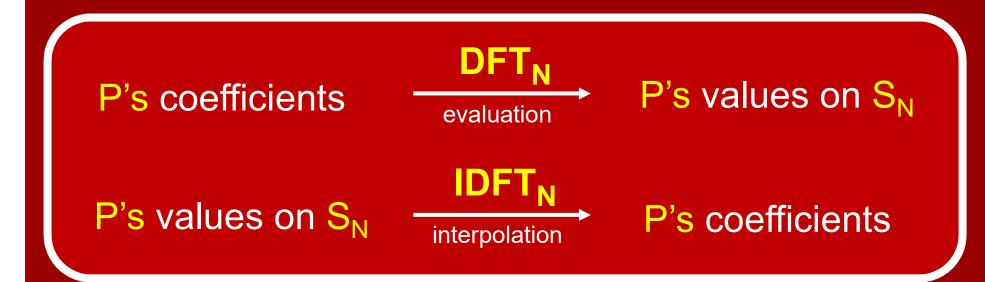
What are the complex N-th roots of unity?

Discrete Fourier Transform (& Inverse)

Let N be a power of 2.

$$S_N = \{1, \omega_N^1, \omega_N^2, \omega_N^3, \dots, \omega_N^{N-1}\}$$
 is the set of N "complex roots of unity" that I'll describe shortly.

Let P(x) be a polynomial of degree N−1.



Fast Fourier Transform

A recursive algorithm for DFT_N and IDFT_N that uses only O(N log N) arithmetic operations.



P's coefficients

evaluation

P's values on S_N

P's values on S_N

IDFT_N interpolation

P's coefficients

Multiplying polynomials with the FFT

Let P(x), Q(x) be polynomials of degree < N. Want $R(x) = P(x) \cdot Q(x)$, which has degree < 2N.

- Use DFT_{2N} to get P(w), Q(w) for all w∈S_{2N}
- 2. Multiply pairs, getting R(w) for all w∈S_{2N}
- 3. Use IDFT_{2N} to get R's coefficients

P's coefficients $\xrightarrow[evaluation]{\text{DFT}_N}$ P's values on S_N P's values on S_N $\xrightarrow[interpolation]{\text{DFT}_N}$ P's coefficients

Multiplying polynomials with the FFT

Let P(x), Q(x) be polynomials of degree < N. Want $R(x) = P(x) \cdot Q(x)$, which has degree < 2N.

- 1. Use DFT_{2N} to get P(w), Q(w) for all w∈S_{2N}
- 2. Multiply pairs, getting R(w) for all w∈S_{2N}
- 3. Use IDFT_{2N} to get R's coefficients

Time: 1. O(N log N) arithmetic ops

2. O(N) arithmetic ops

3. O(N log N) arithmetic ops

O(N log N) arithmetic ops

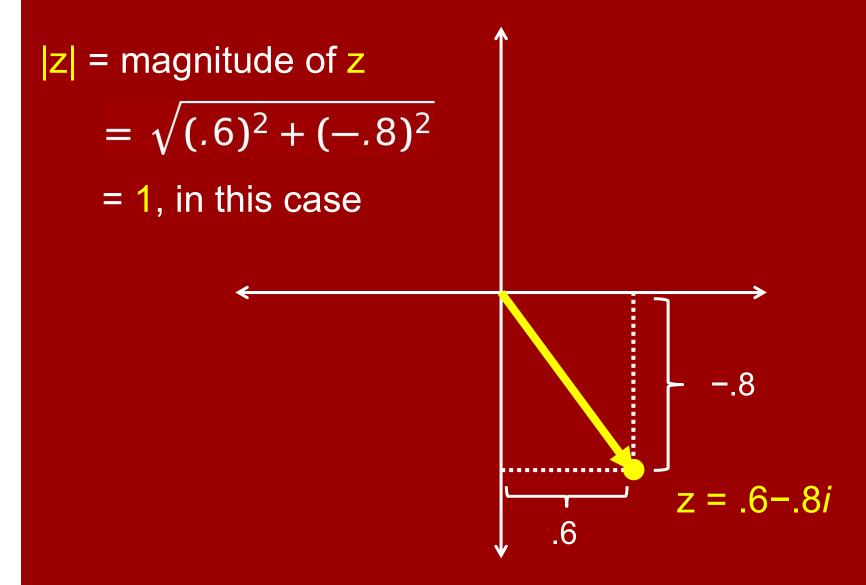
Multiplying polynomials with the FFT

Can multiply two degree-N polynomials using O(N log N) arithmetic operations.

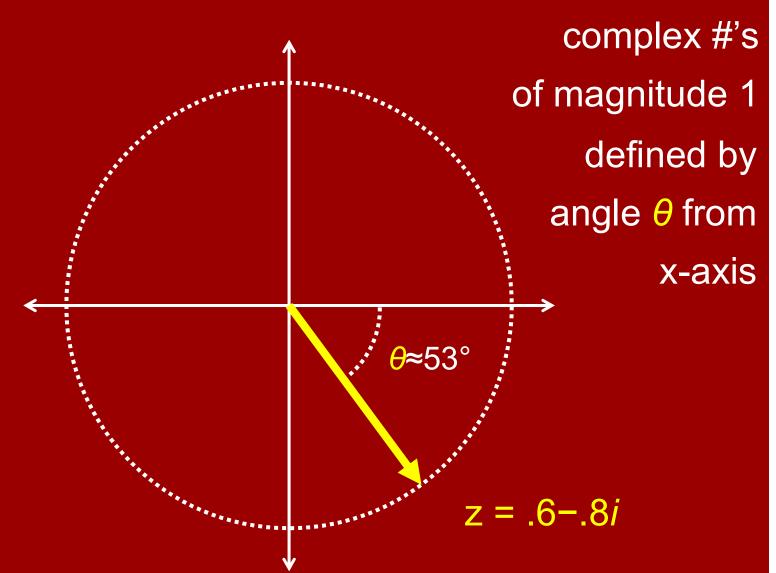
If each coefficient is a word of O(log N) bits, can multiply the polynomials in O(N log N) time.

* Requires proving that you can compute the Nth roots of unity to O(log N) bits of precision in O(N log N) time, and that this precision is sufficient. This is fairly easy to prove, but also boring to prove.

The complex numbers C



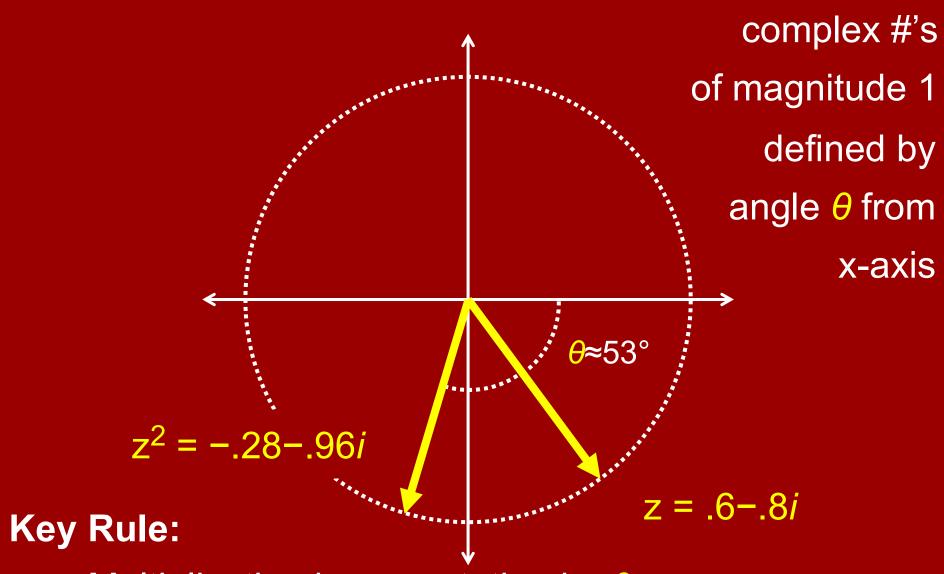
The complex numbers C



Key Rule:

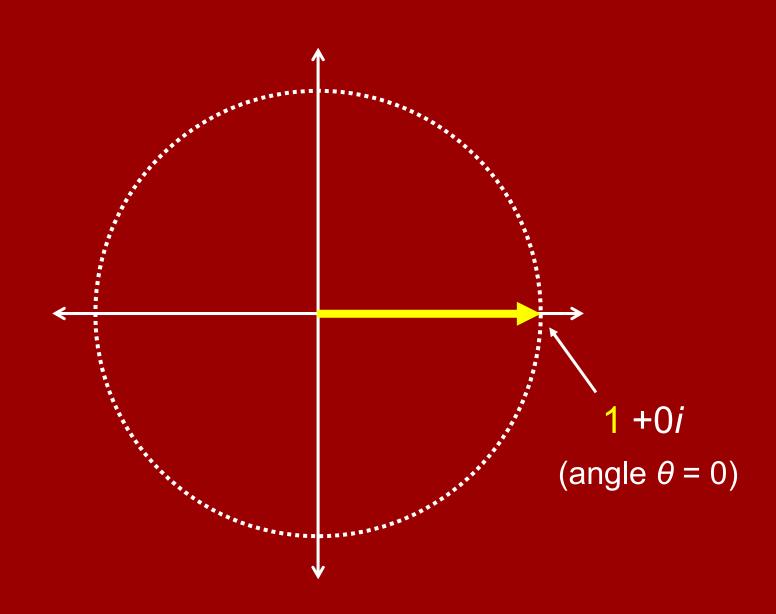
Multiplication by z = rotation by θ .

The complex numbers C

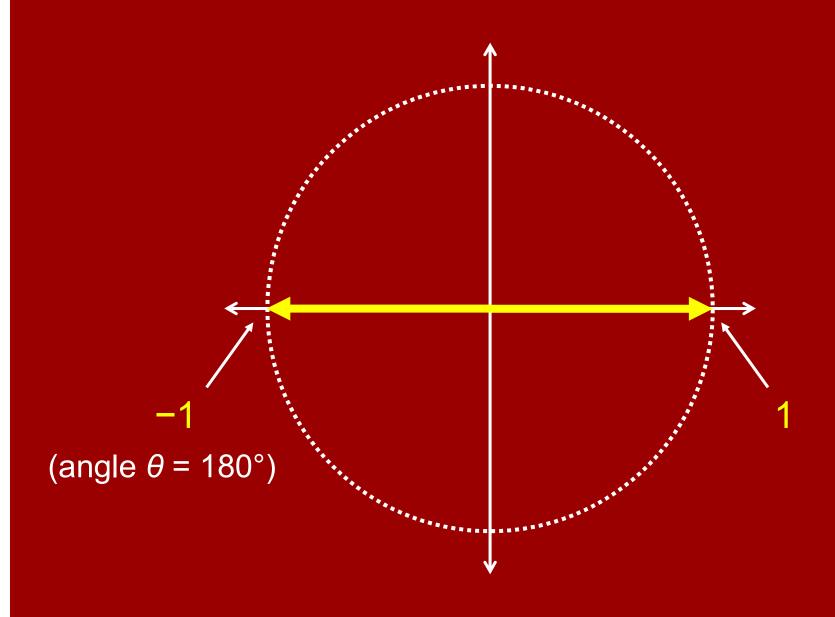


Multiplication by z = rotation by θ .

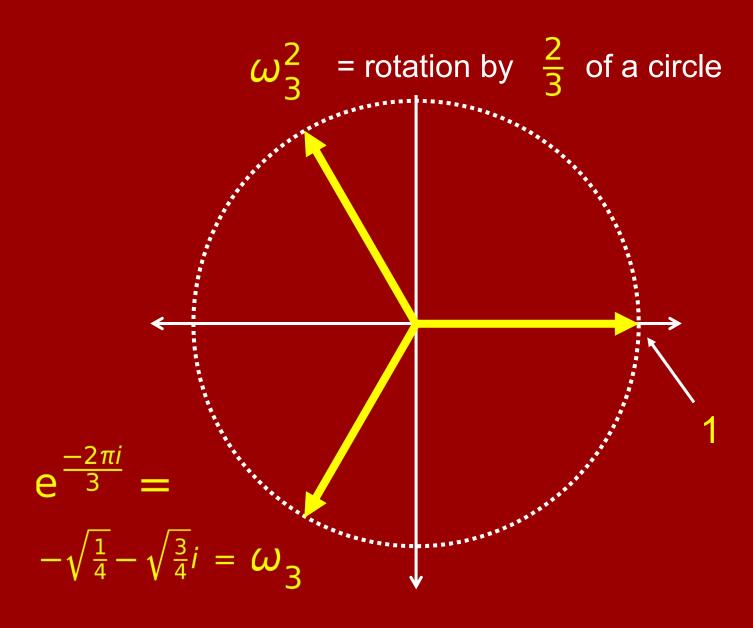
Unity



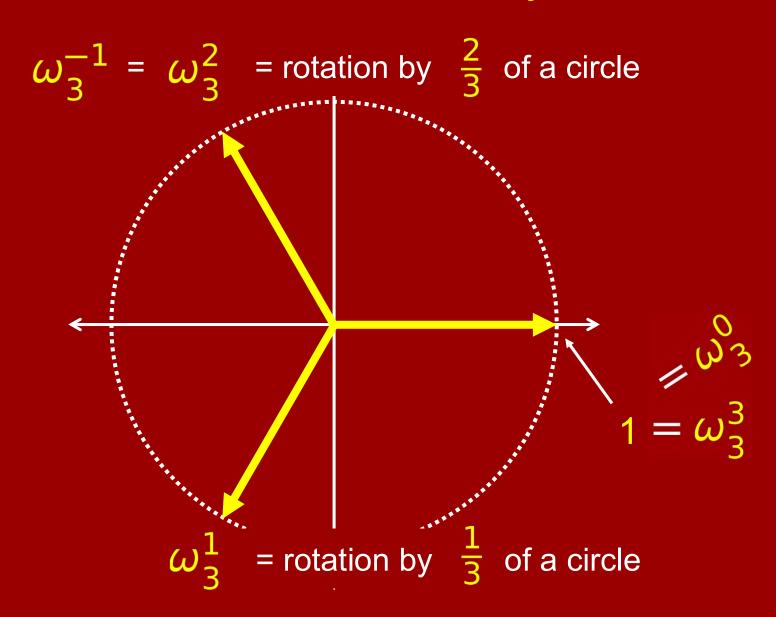
Square Roots of Unity



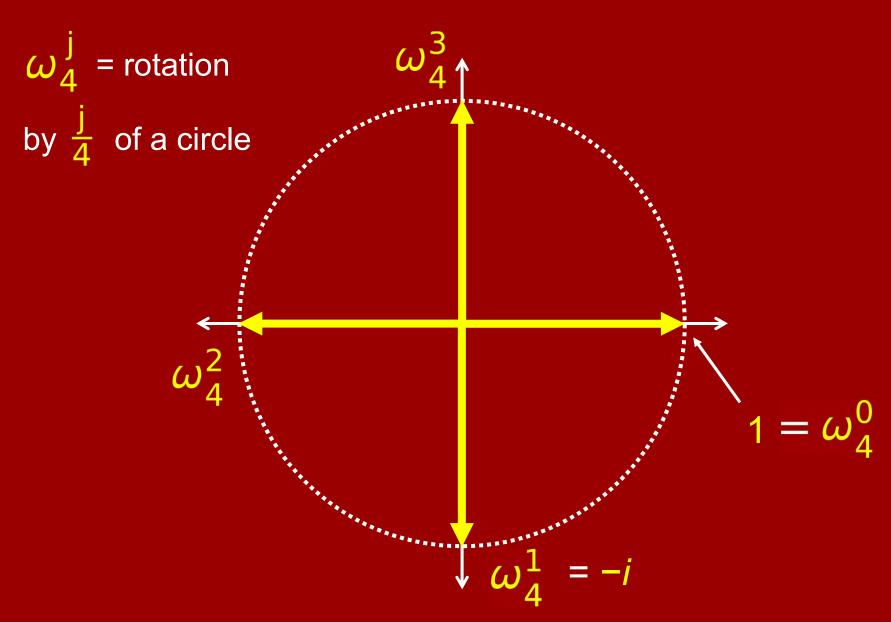
Cube Roots of Unity



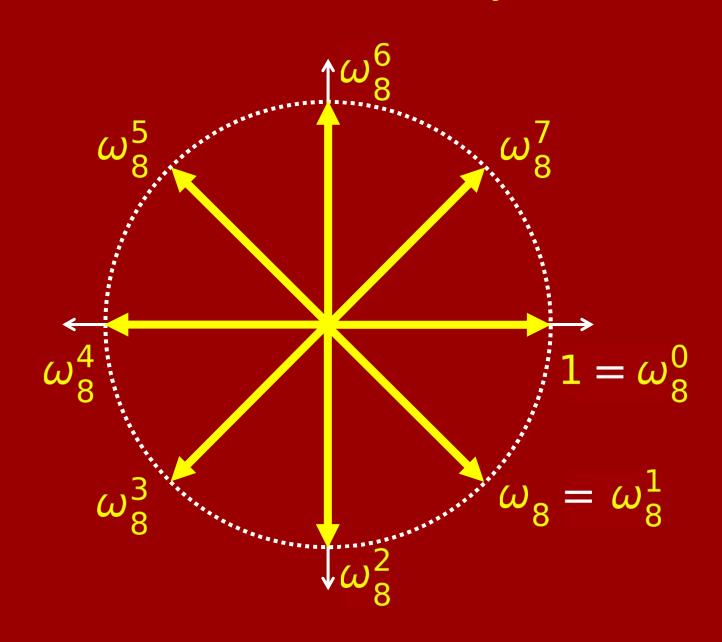
Cube Roots of Unity



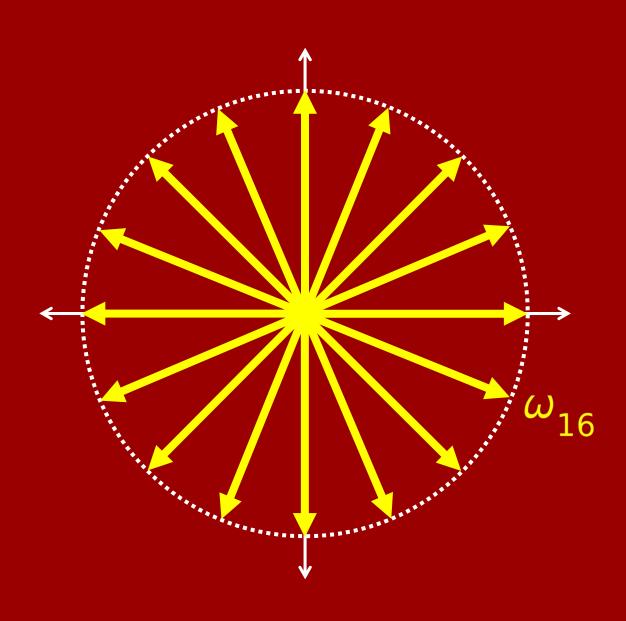
4th Roots of Unity



8th Roots of Unity



16th Roots of Unity

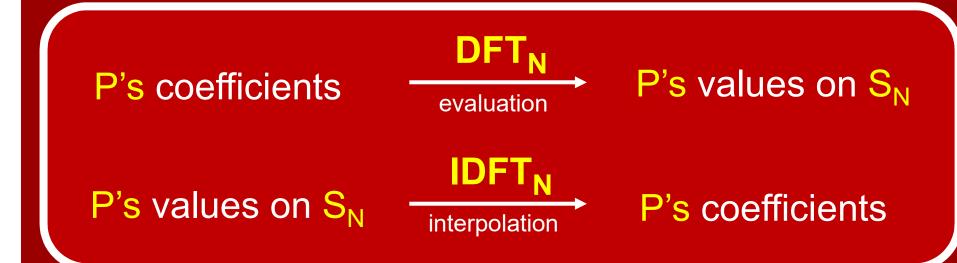


Discrete Fourier Transform (& Inverse)

Let N be a power of 2.

Let
$$S_N = \{1, \omega_N^1, \omega_N^2, \omega_N^3, \dots, \omega_N^{N-1}\}$$

Let P(x) be a polynomial of degree N-1.

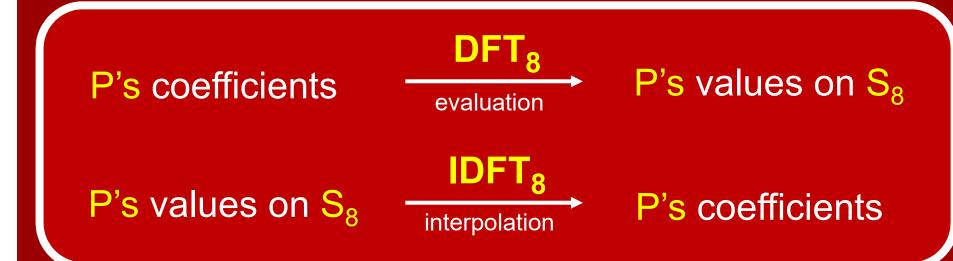


Discrete Fourier Transform (& Inverse)

Let N be 8, and let $\omega = \omega_8$

Let
$$S_8 = \{1, \omega, \omega^2, \omega^3, \omega^4, \omega^5, \omega^6, \omega^7\}$$

Let P(x) be a polynomial of degree 7.



Evaluation at $\{1, \omega, \omega^2, \omega^3, \omega^4, \omega^5, \omega^6, \omega^7\}$

Say P(x) =
$$a_0 + a_1 x + a_2 x^2 + a_3 x^3 + a_4 x^4 + a_5 x^5 + a_6 x^6 + a_7 x^7$$

$$\begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & \omega & \omega^{2} & \omega^{3} & \omega^{4} & \omega^{5} & \omega^{6} & \omega^{7} \\ 1 & \omega^{2} & \omega^{4} & \omega^{6} & \omega^{8} & \omega^{10} & \omega^{12} & \omega^{14} \\ 1 & \omega^{3} & \omega^{6} & \omega^{9} & \omega^{12} & \omega^{15} & \omega^{18} & \omega^{21} \\ 1 & \omega^{4} & \omega^{8} & \omega^{12} & \omega^{16} & \omega^{20} & \omega^{24} & \omega^{28} \\ 1 & \omega^{5} & \omega^{10} & \omega^{15} & \omega^{20} & \omega^{25} & \omega^{30} & \omega^{35} \\ 1 & \omega^{6} & \omega^{12} & \omega^{18} & \omega^{24} & \omega^{30} & \omega^{36} & \omega^{42} \\ 1 & \omega^{7} & \omega^{14} & \omega^{21} & \omega^{28} & \omega^{35} & \omega^{42} & \omega^{49} \end{bmatrix} \cdot \begin{bmatrix} a_{0} \\ a_{1} \\ a_{2} \\ a_{3} \\ a_{4} \\ a_{5} \\ a_{6} \\ a_{7} \end{bmatrix} = \begin{bmatrix} P(1) \\ P(\omega) \\ P(\omega) \\ P(\omega^{2}) \\ P(\omega^{3}) \\ P(\omega^{4}) \\ P(\omega^{5}) \\ P(\omega^{6}) \\ P(\omega^{7}) \end{bmatrix}$$

Since $\omega^8 = 1$, we can reduce all exponents mod 8.

Evaluation at $\{1, \omega, \omega^2, \omega^3, \omega^4, \omega^5, \omega^6, \omega^7\}$

Say P(x) =
$$a_0 + a_1 x + a_2 x^2 + a_3 x^3 + a_4 x^4 + a_5 x^5 + a_6 x^6 + a_7 x^7$$

$$\begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & \omega & \omega^2 & \omega^3 & \omega^4 & \omega^5 & \omega^6 & \omega^7 \\ 1 & \omega^2 & \omega^4 & \omega^6 & 1 & \omega^2 & \omega^4 & \omega^6 \\ 1 & \omega^3 & \omega^6 & \omega & \omega^4 & \omega^7 & \omega^2 & \omega^5 \\ 1 & \omega^4 & 1 & \omega^4 & 1 & \omega^4 & 1 & \omega^4 \\ 1 & \omega^5 & \omega^2 & \omega^7 & \omega^4 & \omega & \omega^6 & \omega^3 \\ 1 & \omega^6 & \omega^4 & \omega^2 & 1 & \omega^6 & \omega^4 & \omega^2 \\ 1 & \omega^7 & \omega^6 & \omega^5 & \omega^4 & \omega^3 & \omega^2 & \omega \end{bmatrix}$$

$$\begin{bmatrix} a_0 \\ a_1 \\ a_2 \\ a_3 \\ a_4 \\ a_5 \\ a_6 \\ a_7 \end{bmatrix} = \begin{bmatrix} P(1) \\ P(\omega) \\ P(\omega^2) \\ P(\omega^3) \\ P(\omega^4) \\ P(\omega^5) \\ P(\omega^6) \\ P(\omega^7) \end{bmatrix}$$

DFT₈

$$DFT_8[j,k] = \omega^{jk \mod 8}$$

 $(0 \le j, k \le 7)$

Multiplication module 9 toble

Multiplication modulo 8 table

| • | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|---|---|---|---|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 1 | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| 2 | 0 | 2 | 4 | 6 | 0 | 2 | 4 | 6 |
| 3 | 0 | 3 | 6 | 1 | 4 | 7 | 2 | 5 |
| 4 | 0 | 4 | 0 | 4 | 0 | 4 | 0 | 4 |
| 5 | 0 | 5 | 2 | 7 | 4 | 1 | 6 | 3 |
| 6 | 0 | 6 | 4 | 2 | 0 | 6 | 4 | 2 |
| 7 | 0 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |

 $^{4}, \omega^{5}, \omega^{6}, \omega^{7}\}$

$$\begin{bmatrix} a_0 \\ a_1 \\ a_2 \\ a_3 \\ a_4 \\ a_5 \\ a_6 \\ a_7 \end{bmatrix} = \begin{bmatrix} P(1) \\ P(\omega) \\ P(\omega^2) \\ P(\omega^3) \\ P(\omega^4) \\ P(\omega^5) \\ P(\omega^6) \\ P(\omega^7) \end{bmatrix}$$

 $DFT_8[j,k] = \omega^{jk \mod 8}$

 $(0 \le j, \, k \le 7)$

Evaluation at $\{1, \omega, \omega^2, \omega^3, \omega^4, \omega^5, \omega^6, \omega^7\}$

Say P(x) =
$$a_0 + a_1 x + a_2 x^2 + a_3 x^3 + a_4 x^4 + a_5 x^5 + a_6 x^6 + a_7 x^7$$

$$\begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & \omega & \omega^{2} & \omega^{3} & \omega^{4} & \omega^{5} & \omega^{6} & \omega^{7} \\ 1 & \omega^{2} & \omega^{4} & \omega^{6} & 1 & \omega^{2} & \omega^{4} & \omega^{6} \\ 1 & \omega^{3} & \omega^{6} & \omega & \omega^{4} & \omega^{7} & \omega^{2} & \omega^{5} \\ 1 & \omega^{4} & 1 & \omega^{4} & 1 & \omega^{4} & 1 & \omega^{4} \\ 1 & \omega^{5} & \omega^{2} & \omega^{7} & \omega^{4} & \omega & \omega^{6} & \omega^{3} \\ 1 & \omega^{6} & \omega^{4} & \omega^{2} & 1 & \omega^{6} & \omega^{4} & \omega^{2} \\ 1 & \omega^{7} & \omega^{6} & \omega^{5} & \omega^{4} & \omega^{3} & \omega^{2} & \omega \end{bmatrix} \cdot \begin{bmatrix} a_{0} \\ a_{1} \\ a_{2} \\ a_{3} \\ a_{4} \\ a_{5} \\ a_{6} \\ a_{7} \end{bmatrix} = \begin{bmatrix} P(1) \\ P(\omega) \\ P(\omega^{2}) \\ P(\omega^{2}) \\ P(\omega^{3}) \\ P(\omega^{4}) \\ P(\omega^{5}) \\ P(\omega^{6}) \\ P(\omega^{7}) \end{bmatrix}$$

$$DFT_{8}[j,k] = \omega^{jk \bmod 8} \quad (0 \le j, k \le 7)$$

Evaluation at $\{1, \omega, \omega^2, \omega^3, \omega^4, \omega^5, \omega^6, \omega^7\}$

Say P(x) =
$$a_0 + a_1 x + a_2 x^2 + a_3 x^3 + a_4 x^4 + a_5 x^5 + a_6 x^6 + a_7 x^7$$

DFT₈ •
$$\begin{vmatrix} a_1 \\ a_2 \\ a_3 \\ a_4 \\ a_5 \\ a_6 \\ a_7 \end{vmatrix} = \begin{vmatrix} P(\omega) \\ P(\omega^2) \\ P(\omega^3) \\ P(\omega^4) \\ P(\omega^5) \\ P(\omega^6) \\ P(\omega^7) \end{vmatrix}$$

Interpolation?

Say P(x) =
$$a_0 + a_1 x + a_2 x^2 + a_3 x^3 + a_4 x^4 + a_5 x^5 + a_6 x^6 + a_7 x^7$$
.

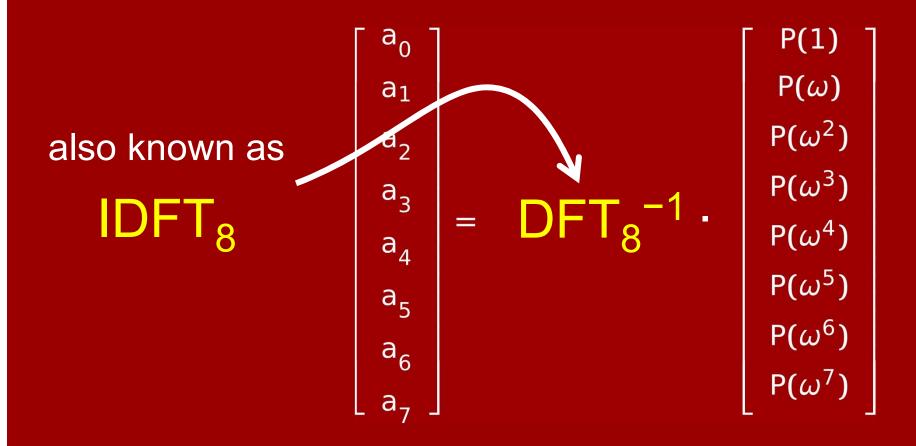
Given P(1), P(ω), ..., P(ω ⁷), how to get a_0 , a_1 , ..., a_7 ?

DFT₈ •
$$\begin{bmatrix} a_0 \\ a_1 \\ a_2 \\ a_3 \\ a_4 \\ a_5 \\ a_6 \\ a_7 \end{bmatrix} = \begin{bmatrix} \Gamma(1) \\ P(\omega) \\ P(\omega^2) \\ P(\omega^3) \\ P(\omega^4) \\ P(\omega^5) \\ P(\omega^6) \\ P(\omega^7) \end{bmatrix}$$

Interpolation?

Say P(x) =
$$a_0 + a_1 x + a_2 x^2 + a_3 x^3 + a_4 x^4 + a_5 x^5 + a_6 x^6 + a_7 x^7$$
.

Given P(1), P(ω), ..., P(ω ⁷), how to get a_0 , a_1 , ..., a_7 ?



P's coefficients

DFT_N evaluation

P's values on S_N

P's values on S_N

IDFT_N interpolation

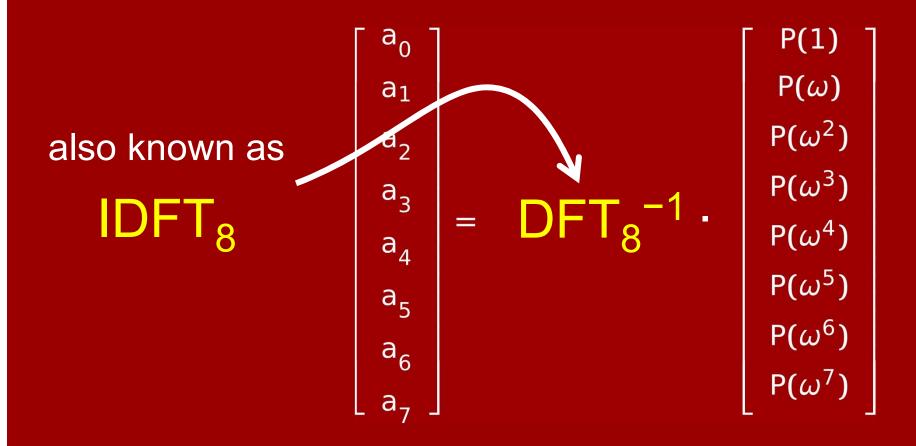
P's coefficients

 a_0 P(1) $P(\omega)$ a_1 $P(\omega^2)$ also known as $P(\omega^3)$ a_3 $P(\omega^4)$ a_4 $P(\omega^5)$ a₅ $P(\omega^6)$ a_6 $P(\omega^7)$ a₇

Interpolation?

Say P(x) =
$$a_0 + a_1 x + a_2 x^2 + a_3 x^3 + a_4 x^4 + a_5 x^5 + a_6 x^6 + a_7 x^7$$
.

Given P(1), P(ω), ..., P(ω ⁷), how to get a_0 , a_1 , ..., a_7 ?



DFT versus IDFT

Question:

We know what matrix DFT₈ is.

What is its inverse matrix, IDFT₈?

Answer:

It's extremely similar to DFT₈.

IDFT₈ ω^{-1} ω^{-2} ω^{-3} ω^{-4} ω^{-5} ω^{-6} ω^{-7} ω^{-2} ω^{-4} ω^{-6} 1 ω^{-2} ω^{-4} ω^{-6} ω^{-3} ω^{-6} ω^{-1} ω^{-4} ω^{-7} ω^{-2} ω^{-5} ω^{-4} 1 ω^{-4} 1 ω^{-4} 1 ω^{-4} ω^{-5} ω^{-2} ω^{-7} ω^{-4} ω^{-1} ω^{-6} ω^{-3} | 1 ω^{5} ω^{2} ω^{7} ω^{4} ω^{1} ω^{6} ω^{3} ω^{-6} ω^{-4} ω^{-2} 1 ω^{-6} ω^{-4} ω^{-2} $\begin{bmatrix} 1 & \omega^{-7} & \omega^{-6} & \omega^{-5} & \omega^{-4} & \omega^{-3} & \omega^{-2} & \omega \end{bmatrix}$

$$\begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & \omega^1 & \omega^2 & \omega^3 & \omega^4 & \omega^5 & \omega^6 & \omega^7 \\ 1 & \omega^2 & \omega^4 & \omega^6 & 1 & \omega^2 & \omega^4 & \omega^6 \\ 1 & \omega^3 & \omega^6 & \omega^1 & \omega^4 & \omega^7 & \omega^2 & \omega^5 \\ 1 & \omega^4 & 1 & \omega^4 & 1 & \omega^4 & 1 & \omega^4 \\ 1 & \omega^5 & \omega^2 & \omega^7 & \omega^4 & \omega^1 & \omega^6 & \omega^3 \\ 1 & \omega^6 & \omega^4 & \omega^2 & 1 & \omega^6 & \omega^4 & \omega^2 \\ 1 & \omega^7 & \omega^6 & \omega^5 & \omega^4 & \omega^3 & \omega^2 & \omega \end{bmatrix}$$

 $(0 \le j, k < N, \omega = \omega_N \text{ is } N^{\text{th}} \text{ root of unity})$

DFT8

$$IDFT_{N}[j,k] = \frac{1}{N}\omega^{-jk \mod N}$$

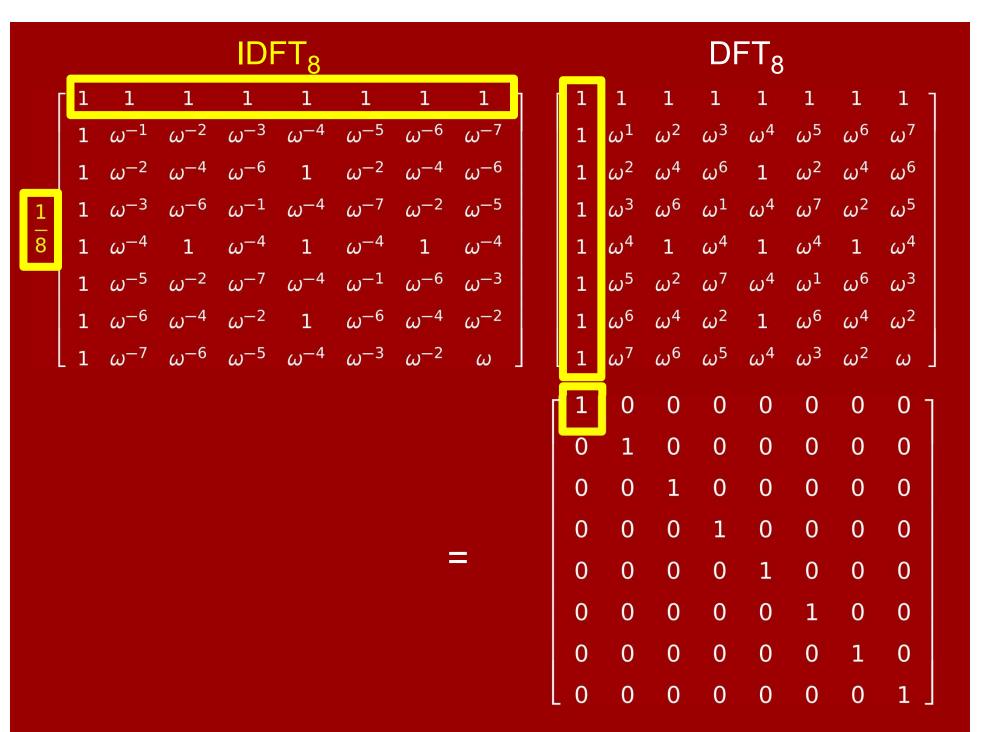
 $DFT_{N}[j,k] = \omega^{jk \mod N}$

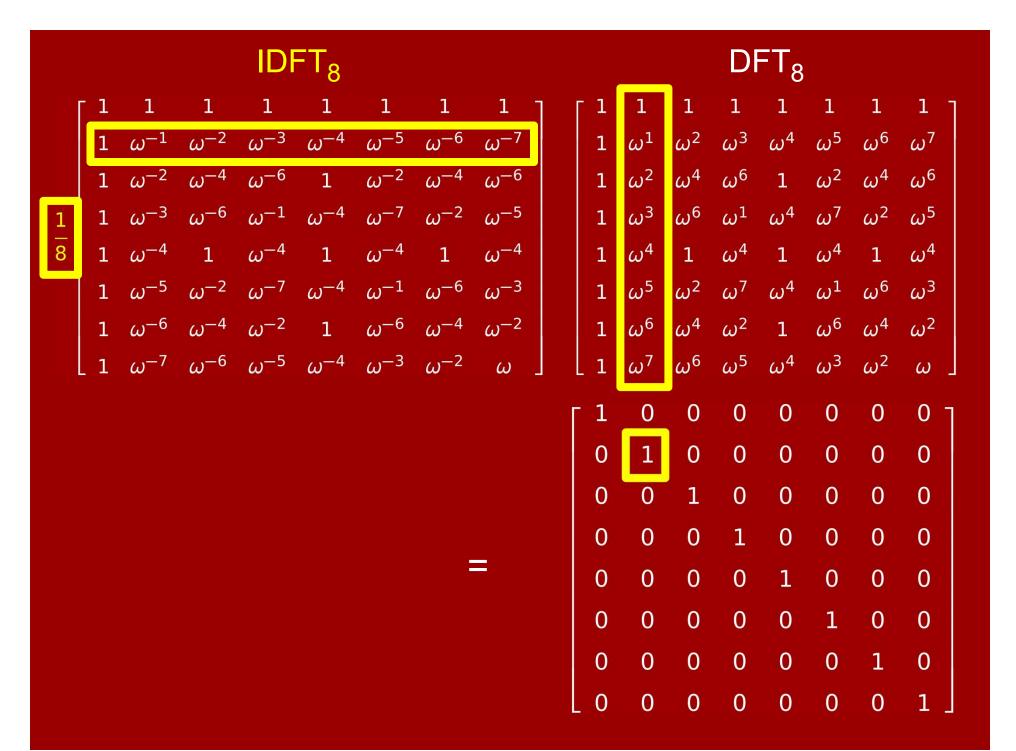
 $\begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & \omega^{1} & \omega^{2} & \omega^{3} & \omega^{4} & \omega^{5} & \omega^{6} & \omega^{7} \\ 1 & \omega^{2} & \omega^{4} & \omega^{6} & 1 & \omega^{2} & \omega^{4} & \omega^{6} \\ 1 & \omega^{3} & \omega^{6} & \omega^{1} & \omega^{4} & \omega^{7} & \omega^{2} & \omega^{5} \\ 1 & \omega^{4} & 1 & \omega^{4} & 1 & \omega^{4} & 1 & \omega^{4} \\ 1 & \omega^{5} & \omega^{2} & \omega^{7} & \omega^{4} & \omega^{1} & \omega^{6} & \omega^{3} \\ 1 & \omega^{6} & \omega^{4} & \omega^{2} & 1 & \omega^{6} & \omega^{4} & \omega^{2} \\ 1 & \omega^{7} & \omega^{6} & \omega^{5} & \omega^{4} & \omega^{3} & \omega^{2} & \omega \end{bmatrix}$

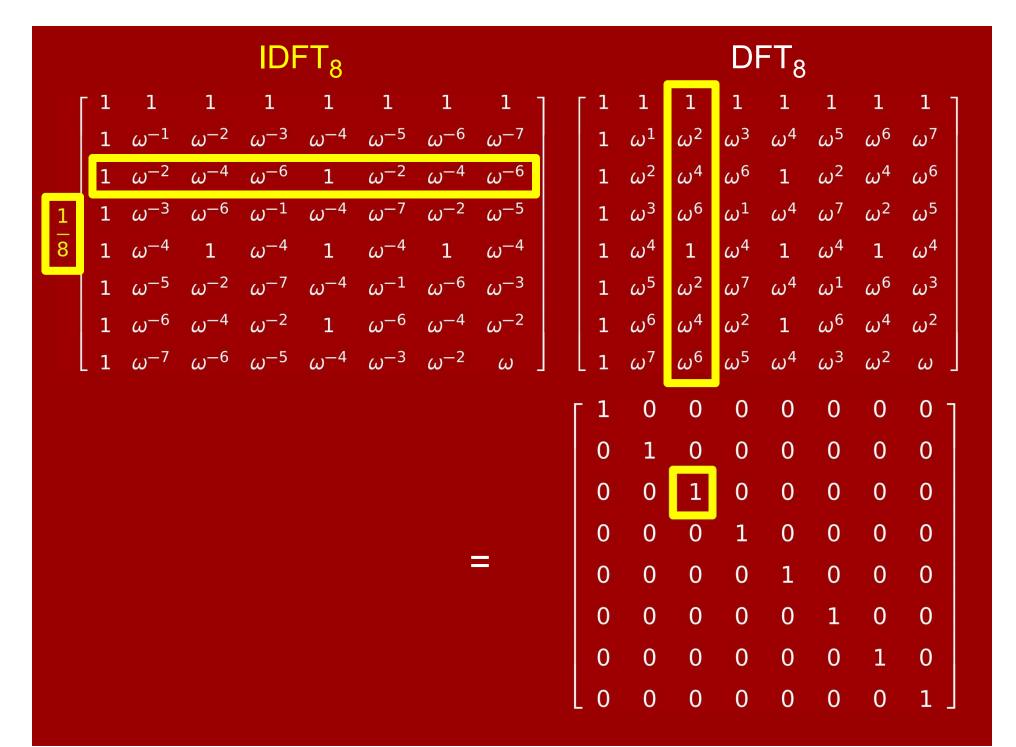
DFT8

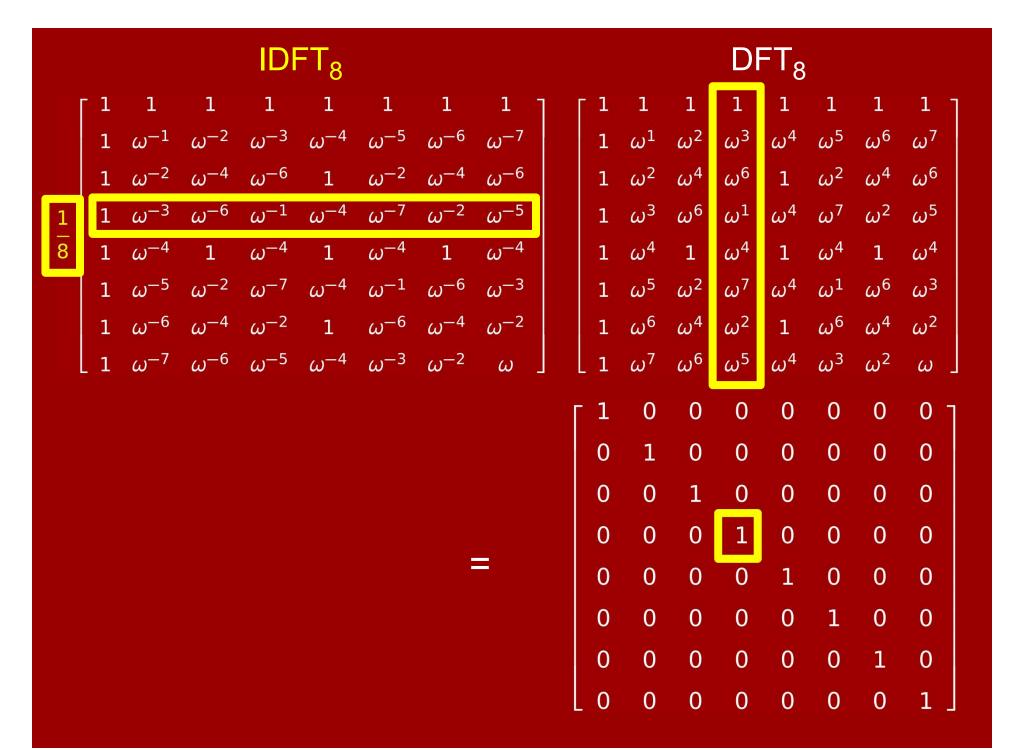
Proof illustration.

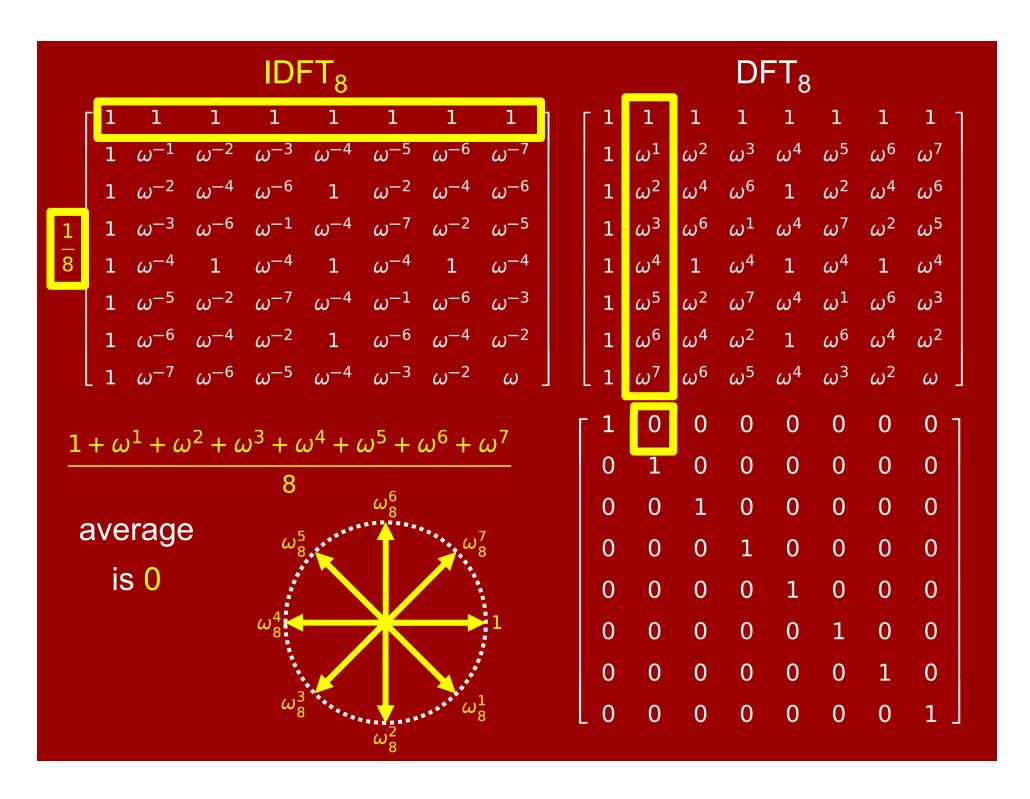
We'll show the product =

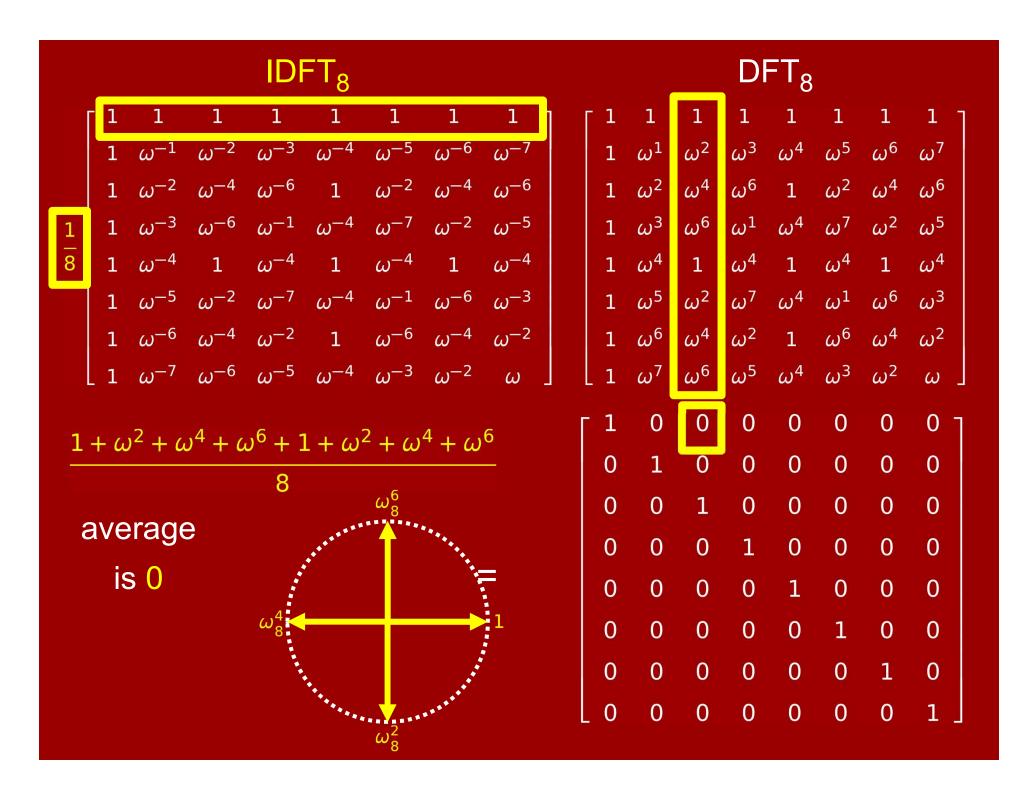


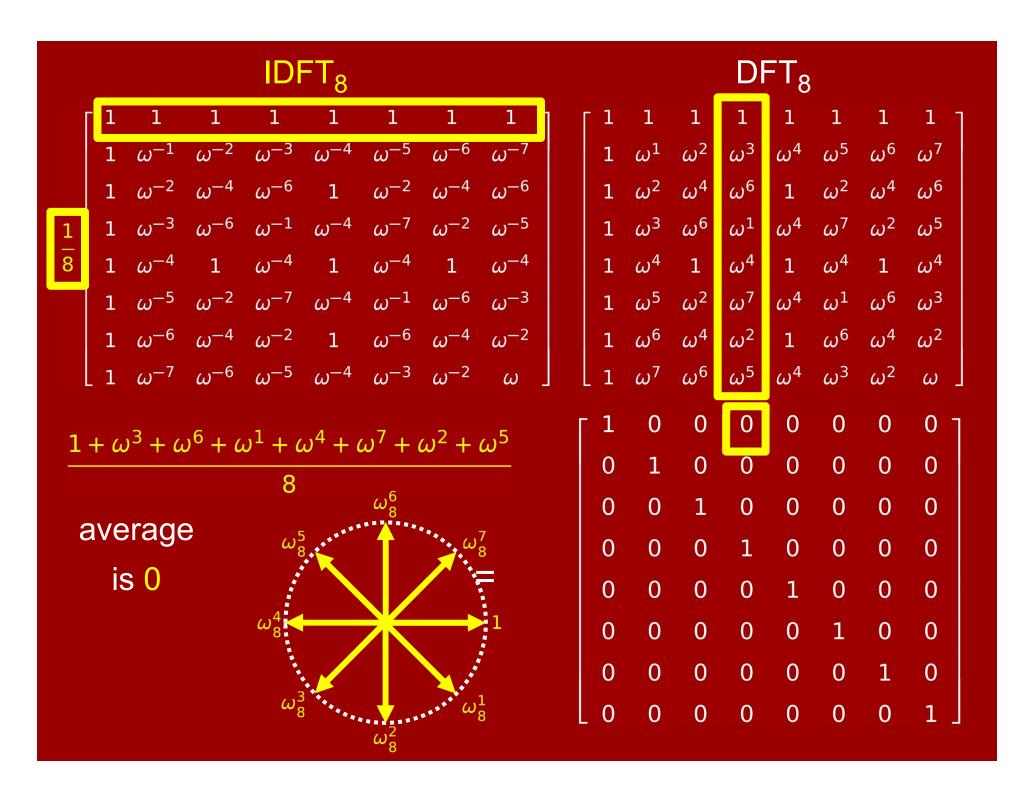


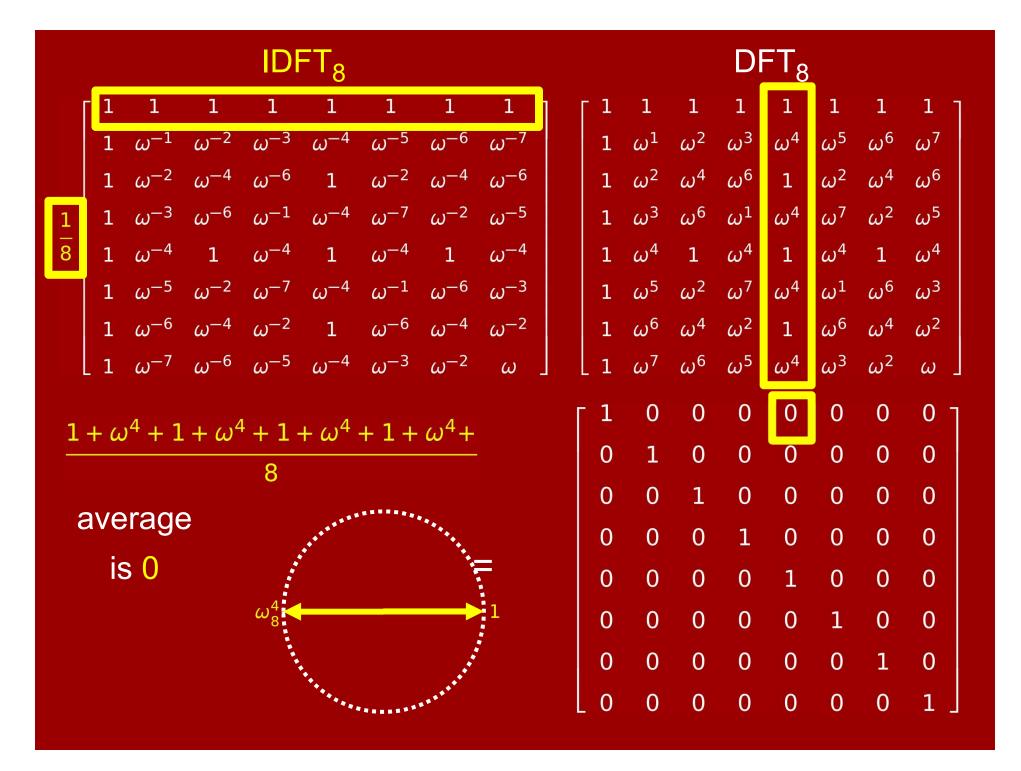


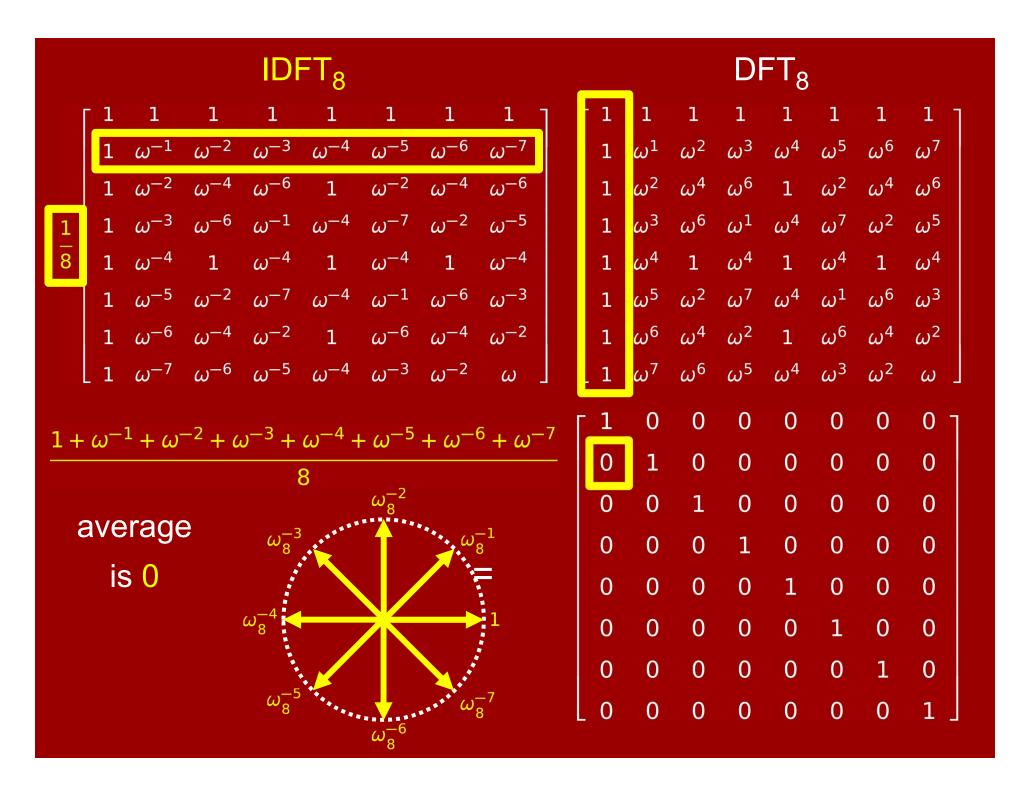


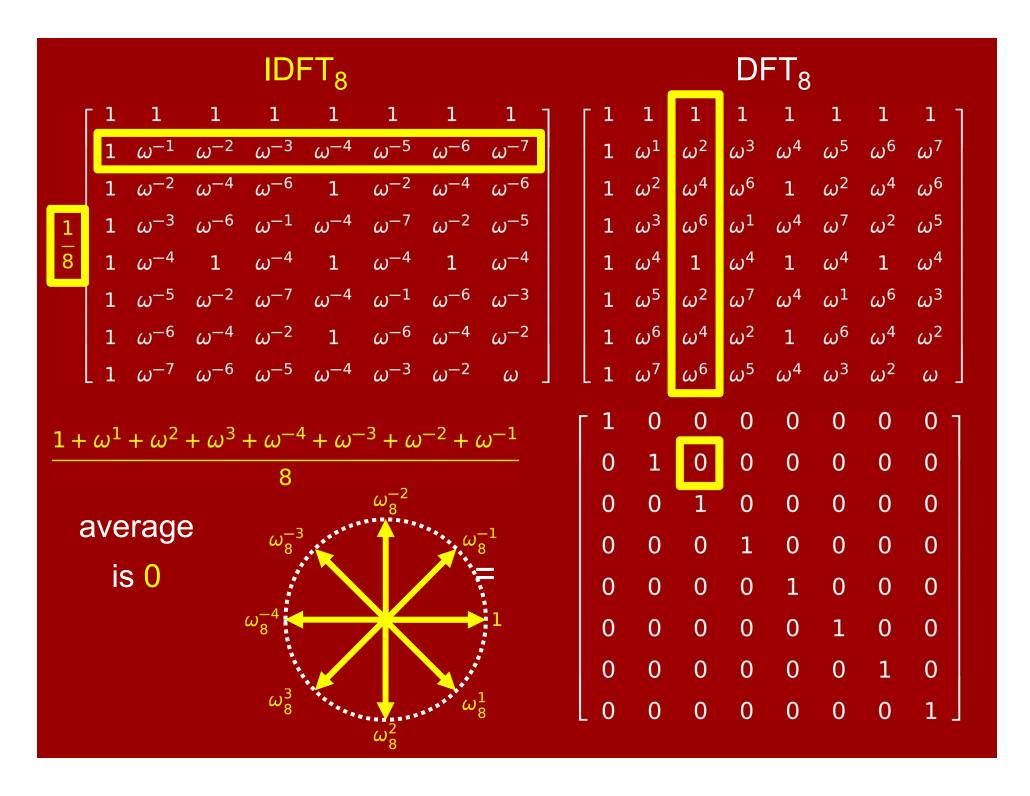


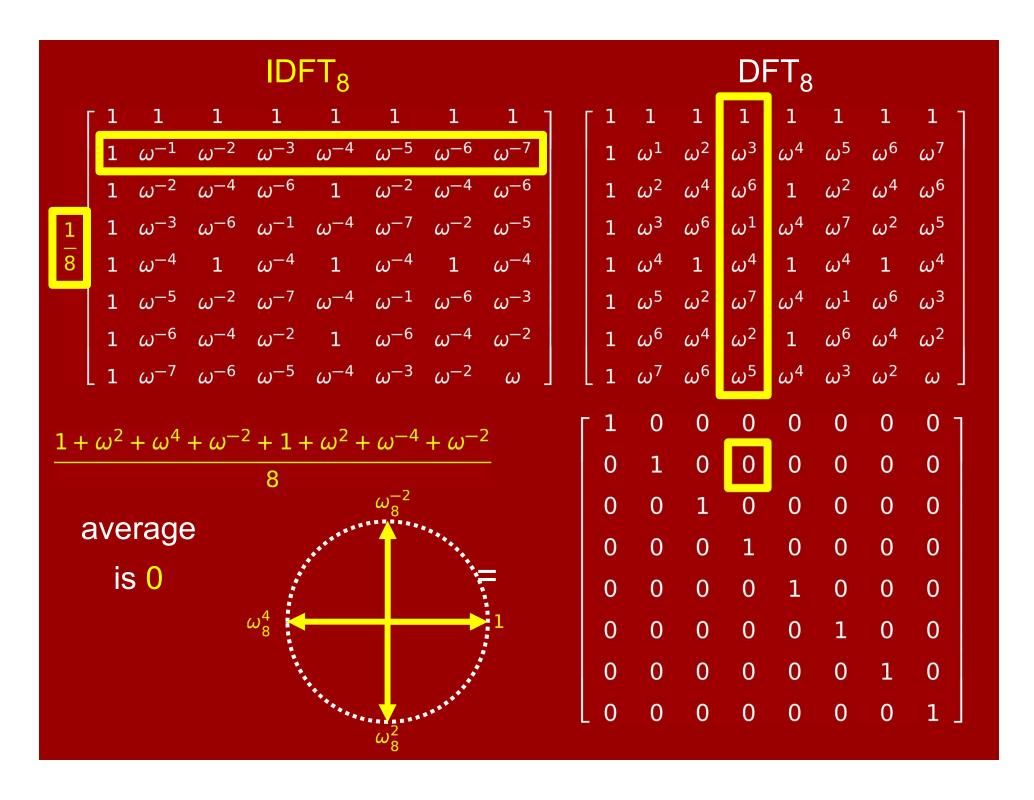












DFI8 ω^1 ω^2 ω^3 ω^4 ω^5 ω^6 ω^{-1} ω^{-2} ω^{-3} ω^{-4} ω^{-5} ω^{-6} ω^{-7} ω^6 1 ω^2 ω^6 ω^{-6} ω^{-1} ω^{-4} ω^{-7} ω^{-2} ω^{-5} ω^1 ω^4 ω^7 ω^4 1 ω^4 ω^{-5} ω^{-2} ω^{-7} ω^{-4} ω^{-1} ω^{-6} ω^{-3} ω^2 ω^7 ω^4 ω^1 $\omega^{-4} \ \omega^{-2} \ 1 \ \omega^{-6} \ \omega^{-4}$ ω^2 1 ω^6 ω^{-7} ω^{-6} ω^{-5} ω^{-4} ω^{-3} ω^{-2} ω^7 ω^6 ω^5 ω^4 ω^3 Well, looks pretty true. See the notes for a

Formal proof.

Last piece of the puzzle: FFT

Computing this in O(N log N) ops

Claim: DFT_N reduces to 2 applications of $DFT_{N/2}$, plus O(N) additional operations.

$$\Rightarrow$$
 T(N) = 2T(N/2) + O(N) \Rightarrow T(N) = O(N log N)

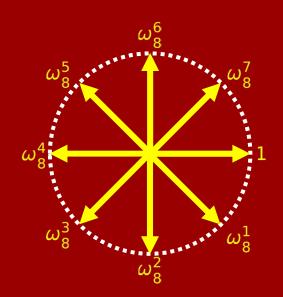
$$= a_{0} \cdot \begin{bmatrix} 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \end{bmatrix} + a_{1} \cdot \begin{bmatrix} 1 \\ \omega^{2} \\ \omega^{4} \\ \omega^{5} \\ \omega^{6} \\ \omega^{7} \end{bmatrix} + a_{2} \cdot \begin{bmatrix} 1 \\ \omega^{2} \\ \omega^{4} \\ \omega^{2} \\ \omega^{4} \\ \omega^{6} \end{bmatrix} + a_{3} \cdot \begin{bmatrix} 1 \\ \omega^{3} \\ \omega^{4} \\ \omega^{4} \\ \omega^{7} \end{bmatrix} + a_{4} \cdot \begin{bmatrix} 1 \\ \omega^{4} \\ \omega^{4} \\ \omega^{6} \\ \omega^{7} \end{bmatrix} + a_{5} \cdot \begin{bmatrix} 1 \\ \omega^{5} \\ \omega^{4} \\ \omega^{6} \\ \omega^{6} \\ \omega^{6} \end{bmatrix} + a_{7} \cdot \begin{bmatrix} 1 \\ \omega^{6} \\ \omega^{4} \\ \omega^{6} \\ \omega^{3} \end{bmatrix} + a_{7} \cdot \begin{bmatrix} 1 \\ \omega^{6} \\ \omega^{4} \\ \omega^{6} \\ \omega^{4} \end{bmatrix} + a_{7} \cdot \begin{bmatrix} 1 \\ \omega^{6} \\ \omega^{4} \\ \omega^{6} \end{bmatrix} + a_{7} \cdot \begin{bmatrix} 1 \\ \omega^{6} \\ \omega^{4} \\ \omega^{6} \end{bmatrix} + a_{7} \cdot \begin{bmatrix} 1 \\ \omega^{6} \\ \omega^{4} \\ \omega^{6} \end{bmatrix} + a_{7} \cdot \begin{bmatrix} 1 \\ \omega^{6} \\ \omega^{4} \\ \omega^{6} \end{bmatrix} + a_{7} \cdot \begin{bmatrix} 1 \\ \omega^{6} \\ \omega^{4} \\ \omega^{6} \end{bmatrix} + a_{7} \cdot \begin{bmatrix} 1 \\ \omega^{6} \\ \omega^{4} \\ \omega^{6} \end{bmatrix} + a_{7} \cdot \begin{bmatrix} 1 \\ \omega^{6} \\ \omega^{4} \\ \omega^{6} \end{bmatrix} + a_{7} \cdot \begin{bmatrix} 1 \\ \omega^{6} \\ \omega^{4} \\ \omega^{6} \end{bmatrix} + a_{7} \cdot \begin{bmatrix} 1 \\ \omega^{6} \\ \omega^{4} \\ \omega^{6} \end{bmatrix} + a_{7} \cdot \begin{bmatrix} 1 \\ \omega^{6} \\ \omega^{4} \\ \omega^{6} \end{bmatrix} + a_{7} \cdot \begin{bmatrix} 1 \\ \omega^{6} \\ \omega^{6} \\ \omega^{6} \end{bmatrix} + a_{7} \cdot \begin{bmatrix} 1 \\ \omega^{6} \\ \omega^{6} \\ \omega^{6} \end{bmatrix} + a_{7} \cdot \begin{bmatrix} 1 \\ \omega^{6} \\ \omega^{6} \\ \omega^{6} \end{bmatrix} + a_{7} \cdot \begin{bmatrix} 1 \\ \omega^{6} \\ \omega^{6} \\ \omega^{6} \end{bmatrix} + a_{7} \cdot \begin{bmatrix} 1 \\ \omega^{6} \\ \omega^{6} \\ \omega^{6} \end{bmatrix} + a_{7} \cdot \begin{bmatrix} 1 \\ \omega^{6} \\ \omega^{6} \\ \omega^{6} \end{bmatrix} + a_{7} \cdot \begin{bmatrix} 1 \\ \omega^{6} \\ \omega^{6} \\ \omega^{6} \end{bmatrix} + a_{7} \cdot \begin{bmatrix} 1 \\ \omega^{6} \\ \omega^{6} \\ \omega^{6} \end{bmatrix} + a_{7} \cdot \begin{bmatrix} 1 \\ \omega^{6} \\ \omega^{6} \\ \omega^{6} \end{bmatrix} + a_{7} \cdot \begin{bmatrix} 1 \\ \omega^{6} \\ \omega^{6} \end{bmatrix} + a_{7} \cdot \begin{bmatrix} 1 \\ \omega^{6} \\ \omega^{6} \end{bmatrix} + a_{7} \cdot \begin{bmatrix} 1 \\ \omega^{6} \\ \omega^{6} \end{bmatrix} + a_{7} \cdot \begin{bmatrix} 1 \\ \omega^{6} \\ \omega^{6} \end{bmatrix} + a_{7} \cdot \begin{bmatrix} 1 \\ \omega^{6} \\ \omega^{6} \end{bmatrix} + a_{7} \cdot \begin{bmatrix} 1 \\ \omega^{6} \\ \omega^{6} \end{bmatrix} + a_{7} \cdot \begin{bmatrix} 1 \\ \omega^{6} \\ \omega^{6} \end{bmatrix} + a_{7} \cdot \begin{bmatrix} 1 \\ \omega^{6} \\ \omega^{6} \end{bmatrix} + a_{7} \cdot \begin{bmatrix} 1 \\ \omega^{6} \\ \omega^{6} \end{bmatrix} + a_{7} \cdot \begin{bmatrix} 1 \\ \omega^{6} \\ \omega^{6} \end{bmatrix} + a_{7} \cdot \begin{bmatrix} 1 \\ \omega^{6} \\ \omega^{6} \end{bmatrix} + a_{7} \cdot \begin{bmatrix} 1 \\ \omega^{6} \\ \omega^{6} \end{bmatrix} + a_{7} \cdot \begin{bmatrix} 1 \\ \omega^{6} \\ \omega^{6} \end{bmatrix} + a_{7} \cdot \begin{bmatrix} 1 \\ \omega^{6} \\ \omega^{6} \end{bmatrix} + a_{7} \cdot \begin{bmatrix} 1 \\ \omega^{6} \\ \omega^{6} \end{bmatrix} + a_{7} \cdot \begin{bmatrix} 1 \\ \omega^{6} \\ \omega^{6} \end{bmatrix} + a_{7} \cdot \begin{bmatrix} 1 \\ \omega^{6} \\ \omega^{6} \end{bmatrix} + a_{7} \cdot \begin{bmatrix} 1 \\ \omega^{6} \\ \omega^{6} \end{bmatrix} + a_{7} \cdot \begin{bmatrix} 1 \\ \omega^{6} \\ \omega^{6} \end{bmatrix} + a_{7} \cdot \begin{bmatrix} 1 \\ \omega^{6} \\ \omega^{6} \end{bmatrix} + a_{7} \cdot \begin{bmatrix} 1 \\ \omega^{6} \\ \omega^{6} \end{bmatrix} + a_{7} \cdot \begin{bmatrix} 1 \\ \omega^{6} \\ \omega^{6} \end{bmatrix} + a_{7} \cdot \begin{bmatrix} 1 \\ \omega^{6} \\ \omega^{6} \end{bmatrix} + a_{7} \cdot \begin{bmatrix} 1 \\ \omega^{6} \\ \omega^{6} \end{bmatrix} + a_{7} \cdot \begin{bmatrix} 1 \\ \omega^{6} \\ \omega^{6} \end{bmatrix} + a_{7} \cdot \begin{bmatrix} 1 \\ \omega^{6} \\ \omega^{6} \end{bmatrix} + a_{7} \cdot \begin{bmatrix} 1 \\ \omega^{6} \\ \omega^{6} \end{bmatrix} + a_{7} \cdot \begin{bmatrix} 1 \\ \omega^{6} \\$$

$$= a_{0} \cdot \begin{bmatrix} 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \end{bmatrix} + a_{1} \cdot \begin{bmatrix} 1 \\ \omega^{2} \\ \omega^{4} \\ \omega^{5} \\ \omega^{6} \\ \omega^{6} \end{bmatrix} + a_{2} \cdot \begin{bmatrix} 1 \\ \omega^{2} \\ \omega^{6} \\ \omega^{2} \\ \omega^{6} \\ \omega^{6} \end{bmatrix} + a_{3} \cdot \begin{bmatrix} 1 \\ \omega^{3} \\ \omega^{6} \\ \omega^{4} \\ \omega^{7} \\ \omega^{7} \end{bmatrix} + a_{4} \cdot \begin{bmatrix} 1 \\ \omega^{4} \\ \omega^{7} \\ \omega^{4} \\ \omega^{7} \end{bmatrix} + a_{5} \cdot \begin{bmatrix} 1 \\ \omega^{5} \\ \omega^{4} \\ \omega^{6} \\ \omega^{6} \\ \omega^{6} \end{bmatrix} + a_{7} \cdot \begin{bmatrix} 1 \\ \omega^{6} \\ \omega^{4} \\ \omega^{6} \\ \omega^{3} \end{bmatrix} + a_{7} \cdot \begin{bmatrix} 1 \\ \omega^{6} \\ \omega^{4} \\ \omega^{6} \\ \omega^{6} \end{bmatrix} + a_{7} \cdot \begin{bmatrix} 1 \\ \omega^{6} \\ \omega^{6} \\ \omega^{6} \end{bmatrix} + a_{7} \cdot \begin{bmatrix} 1 \\ \omega^{6} \\ \omega^{6} \\ \omega^{6} \end{bmatrix} + a_{7} \cdot \begin{bmatrix} 1 \\ \omega^{6} \\ \omega^{6} \\ \omega^{6} \end{bmatrix} + a_{7} \cdot \begin{bmatrix} 1 \\ \omega^{6} \\ \omega^{6} \\ \omega^{6} \end{bmatrix} + a_{7} \cdot \begin{bmatrix} 1 \\ \omega^{6} \\ \omega^{6} \\ \omega^{6} \end{bmatrix} + a_{7} \cdot \begin{bmatrix} 1 \\ \omega^{6} \\ \omega^{6} \\ \omega^{6} \end{bmatrix} + a_{7} \cdot \begin{bmatrix} 1 \\ \omega^{6} \\ \omega^{6} \\ \omega^{6} \end{bmatrix} + a_{7} \cdot \begin{bmatrix} 1 \\ \omega^{6} \\ \omega^{6} \\ \omega^{6} \end{bmatrix} + a_{7} \cdot \begin{bmatrix} 1 \\ \omega^{6} \\ \omega^{6} \\ \omega^{6} \end{bmatrix} + a_{7} \cdot \begin{bmatrix} 1 \\ \omega^{6} \\ \omega^{6} \\ \omega^{6} \end{bmatrix} + a_{7} \cdot \begin{bmatrix} 1 \\ \omega^{6} \\ \omega^{6} \\ \omega^{6} \end{bmatrix} + a_{7} \cdot \begin{bmatrix} 1 \\ \omega^{6} \\ \omega^{6} \\ \omega^{6} \end{bmatrix} + a_{7} \cdot \begin{bmatrix} 1 \\ \omega^{6} \\ \omega^{6} \\ \omega^{6} \end{bmatrix} + a_{7} \cdot \begin{bmatrix} 1 \\ \omega^{6} \\ \omega^{6} \\ \omega^{6} \end{bmatrix} + a_{7} \cdot \begin{bmatrix} 1 \\ \omega^{6} \\ \omega^{6} \\ \omega^{6} \end{bmatrix} + a_{7} \cdot \begin{bmatrix} 1 \\ \omega^{6} \\ \omega^{6} \\ \omega^{6} \end{bmatrix} + a_{7} \cdot \begin{bmatrix} 1 \\ \omega^{6} \\ \omega^{6} \\ \omega^{6} \end{bmatrix} + a_{7} \cdot \begin{bmatrix} 1 \\ \omega^{6} \\ \omega^{6} \\ \omega^{6} \end{bmatrix} + a_{7} \cdot \begin{bmatrix} 1 \\ \omega^{6} \\ \omega^{6} \\ \omega^{6} \end{bmatrix} + a_{7} \cdot \begin{bmatrix} 1 \\ \omega^{6} \\ \omega^{6} \\ \omega^{6} \end{bmatrix} + a_{7} \cdot \begin{bmatrix} 1 \\ \omega^{6} \\ \omega^{6} \end{bmatrix} + a_{7} \cdot \begin{bmatrix} 1 \\ \omega^{6} \\ \omega^{6} \end{bmatrix} + a_{7} \cdot \begin{bmatrix} 1 \\ \omega^{6} \\ \omega^{6} \end{bmatrix} + a_{7} \cdot \begin{bmatrix} 1 \\ \omega^{6} \\ \omega^{6} \end{bmatrix} + a_{7} \cdot \begin{bmatrix} 1 \\ \omega^{6} \\ \omega^{6} \end{bmatrix} + a_{7} \cdot \begin{bmatrix} 1 \\ \omega^{6} \\ \omega^{6} \end{bmatrix} + a_{7} \cdot \begin{bmatrix} 1 \\ \omega^{6} \\ \omega^{6} \end{bmatrix} + a_{7} \cdot \begin{bmatrix} 1 \\ \omega^{6} \\ \omega^{6} \end{bmatrix} + a_{7} \cdot \begin{bmatrix} 1 \\ \omega^{6} \\ \omega^{6} \end{bmatrix} + a_{7} \cdot \begin{bmatrix} 1 \\ \omega^{6} \\ \omega^{6} \end{bmatrix} + a_{7} \cdot \begin{bmatrix} 1 \\ \omega^{6} \\ \omega^{6} \end{bmatrix} + a_{7} \cdot \begin{bmatrix} 1 \\ \omega^{6} \\ \omega^{6} \end{bmatrix} + a_{7} \cdot \begin{bmatrix} 1 \\ \omega^{6} \\ \omega^{6} \end{bmatrix} + a_{7} \cdot \begin{bmatrix} 1 \\ \omega^{6} \\ \omega^{6} \end{bmatrix} + a_{7} \cdot \begin{bmatrix} 1 \\ \omega^{6} \\ \omega^{6} \end{bmatrix} + a_{7} \cdot \begin{bmatrix} 1 \\ \omega^{6} \\ \omega^{6} \end{bmatrix} + a_{7} \cdot \begin{bmatrix} 1 \\ \omega^{6} \\ \omega^{6} \end{bmatrix} + a_{7} \cdot \begin{bmatrix} 1 \\ \omega^{6} \\ \omega^{6} \end{bmatrix} + a_{7} \cdot \begin{bmatrix} 1 \\ \omega^{6} \\ \omega^{6} \end{bmatrix} + a_{7} \cdot \begin{bmatrix} 1 \\ \omega^{6} \\ \omega^{6} \end{bmatrix} + a_{7} \cdot \begin{bmatrix} 1 \\ \omega^{6} \\ \omega^{6} \end{bmatrix} + a_{7} \cdot \begin{bmatrix} 1 \\ \omega^{6} \\ \omega^{6} \end{bmatrix} + a_{7} \cdot \begin{bmatrix} 1 \\ \omega^{6} \\ \omega^{6} \end{bmatrix} + a_{7} \cdot \begin{bmatrix} 1 \\ \omega^{6} \\ \omega^{6} \end{bmatrix} + a_{7} \cdot \begin{bmatrix} 1 \\ \omega^{6} \\ \omega^{6} \end{bmatrix} + a_{7} \cdot \begin{bmatrix} 1 \\ \omega^{6} \\ \omega^{6} \end{bmatrix} + a_{7}$$

$$= a_{0} \cdot \begin{bmatrix} 1 \\ 1 \\ 1 \\ 1 \\ 1 \end{bmatrix} + a_{1} \cdot \begin{bmatrix} \omega \\ \omega^{2} \\ \omega^{3} \\ \omega^{4} \\ \omega^{5} \\ \omega^{6} \end{bmatrix} + a_{2} \cdot \begin{bmatrix} \omega^{2} \\ \omega^{4} \\ \omega^{6} \\ \omega^{2} \\ \omega^{6} \end{bmatrix} + a_{3} \cdot \begin{bmatrix} \omega^{3} \\ \omega^{6} \\ \omega^{4} \\ \omega^{7} \\ \omega^{4} \end{bmatrix} + a_{4} \cdot \begin{bmatrix} \omega^{3} \\ \omega^{4} \\ \omega^{6} \\ \omega^{7} \\ \omega^{4} \end{bmatrix} + a_{5} \cdot \begin{bmatrix} \omega^{5} \\ \omega^{5} \\ \omega^{4} \\ \omega^{6} \\ \omega^{6} \\ \omega^{6} \end{bmatrix} + a_{7} \cdot \begin{bmatrix} \omega^{6} \\ \omega^{4} \\ \omega^{6} \\ \omega^{3} \\ \omega^{6} \end{bmatrix} + a_{7} \cdot \begin{bmatrix} \omega^{6} \\ \omega^{6} \\ \omega^{6} \\ \omega^{6} \end{bmatrix} + a_{7} \cdot \begin{bmatrix} \omega^{6} \\ \omega^{6} \\ \omega^{6} \\ \omega^{6} \end{bmatrix} + a_{7} \cdot \begin{bmatrix} \omega^{6} \\ \omega^{6} \\ \omega^{6} \\ \omega^{6} \end{bmatrix} + a_{7} \cdot \begin{bmatrix} \omega^{6} \\ \omega^{6} \\ \omega^{6} \\ \omega^{6} \end{bmatrix} + a_{7} \cdot \begin{bmatrix} \omega^{6} \\ \omega^{6} \\ \omega^{6} \\ \omega^{6} \end{bmatrix} + a_{7} \cdot \begin{bmatrix} \omega^{6} \\ \omega^{6} \\ \omega^{6} \\ \omega^{6} \end{bmatrix} + a_{7} \cdot \begin{bmatrix} \omega^{6} \\ \omega^{6} \\ \omega^{6} \\ \omega^{6} \end{bmatrix} + a_{7} \cdot \begin{bmatrix} \omega^{6} \\ \omega^{6} \\ \omega^{6} \\ \omega^{6} \end{bmatrix} + a_{7} \cdot \begin{bmatrix} \omega^{6} \\ \omega^{6} \\ \omega^{6} \end{bmatrix} + a_{7} \cdot \begin{bmatrix} \omega^{6} \\ \omega^{6} \\ \omega^{6} \end{bmatrix} + a_{7} \cdot \begin{bmatrix} \omega^{6} \\ \omega^{6} \\ \omega^{6} \end{bmatrix} + a_{7} \cdot \begin{bmatrix} \omega^{6} \\ \omega^{6} \\ \omega^{6} \end{bmatrix} + a_{7} \cdot \begin{bmatrix} \omega^{6} \\ \omega^{6} \\ \omega^{6} \end{bmatrix} + a_{7} \cdot \begin{bmatrix} \omega^{6} \\ \omega^{6} \\ \omega^{6} \end{bmatrix} + a_{7} \cdot \begin{bmatrix} \omega^{6} \\ \omega^{6} \\ \omega^{6} \end{bmatrix} + a_{7} \cdot \begin{bmatrix} \omega^{6} \\ \omega^{6} \\ \omega^{6} \end{bmatrix} + a_{7} \cdot \begin{bmatrix} \omega^{6} \\ \omega^{6} \\ \omega^{6} \end{bmatrix} + a_{7} \cdot \begin{bmatrix} \omega^{6} \\ \omega^{6} \\ \omega^{6} \end{bmatrix} + a_{7} \cdot \begin{bmatrix} \omega^{6} \\ \omega^{6} \\ \omega^{6} \end{bmatrix} + a_{7} \cdot \begin{bmatrix} \omega^{6} \\ \omega^{6} \\ \omega^{6} \end{bmatrix} + a_{7} \cdot \begin{bmatrix} \omega^{6} \\ \omega^{6} \\ \omega^{6} \end{bmatrix} + a_{7} \cdot \begin{bmatrix} \omega^{6} \\ \omega^{6} \\ \omega^{6} \end{bmatrix} + a_{7} \cdot \begin{bmatrix} \omega^{6} \\ \omega^{6} \\ \omega^{6} \end{bmatrix} + a_{7} \cdot \begin{bmatrix} \omega^{6} \\ \omega^{6} \\ \omega^{6} \end{bmatrix} + a_{7} \cdot \begin{bmatrix} \omega^{6} \\ \omega^{6} \\ \omega^{6} \end{bmatrix} + a_{7} \cdot \begin{bmatrix} \omega^{6} \\ \omega^{6} \\ \omega^{6} \end{bmatrix} + a_{7} \cdot \begin{bmatrix} \omega^{6} \\ \omega^{6} \\ \omega^{6} \end{bmatrix} + a_{7} \cdot \begin{bmatrix} \omega^{6} \\ \omega^{6} \\ \omega^{6} \end{bmatrix} + a_{7} \cdot \begin{bmatrix} \omega^{6} \\ \omega^{6} \\ \omega^{6} \end{bmatrix} + a_{7} \cdot \begin{bmatrix} \omega^{6} \\ \omega^{6} \\ \omega^{6} \end{bmatrix} + a_{7} \cdot \begin{bmatrix} \omega^{6} \\ \omega^{6} \\ \omega^{6} \end{bmatrix} + a_{7} \cdot \begin{bmatrix} \omega^{6} \\ \omega^{6} \\ \omega^{6} \end{bmatrix} + a_{7} \cdot \begin{bmatrix} \omega^{6} \\ \omega^{6} \\ \omega^{6} \end{bmatrix} + a_{7} \cdot \begin{bmatrix} \omega^{6} \\ \omega^{6} \\ \omega^{6} \end{bmatrix} + a_{7} \cdot \begin{bmatrix} \omega^{6} \\ \omega^{6} \\ \omega^{6} \end{bmatrix} + a_{7} \cdot \begin{bmatrix} \omega^{6} \\ \omega^{6} \\ \omega^{6} \end{bmatrix} + a_{7} \cdot \begin{bmatrix} \omega^{6} \\ \omega^{6} \\ \omega^{6} \end{bmatrix} + a_{7} \cdot \begin{bmatrix} \omega^{6} \\ \omega^{6} \\ \omega^{6} \end{bmatrix} + a_{7} \cdot \begin{bmatrix} \omega^{6} \\ \omega^{6} \\ \omega^{6} \end{bmatrix} + a_{7} \cdot \begin{bmatrix} \omega^{6} \\ \omega^{6} \\ \omega^{6} \end{bmatrix} + a_{7} \cdot \begin{bmatrix} \omega^{6} \\ \omega^{6} \\ \omega^{6} \end{bmatrix} + a_{7} \cdot \begin{bmatrix} \omega^{6} \\ \omega^{6} \\ \omega^{6} \end{bmatrix} + a_{7} \cdot \begin{bmatrix} \omega^{6} \\ \omega^{6} \\ \omega^{6} \end{bmatrix} + a_{7} \cdot \begin{bmatrix} \omega^{6} \\ \omega^{6} \\ \omega^{6} \end{bmatrix} + a_{7} \cdot \begin{bmatrix} \omega^{6} \\ \omega^{6} \\ \omega^{6} \end{bmatrix} + a_$$

$$= \mathbf{a}_{0} \cdot \begin{bmatrix} 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \end{bmatrix} + \mathbf{a}_{2} \cdot \begin{bmatrix} 1 \\ \omega^{2} \\ \omega^{4} \\ \omega^{6} \\ 1 \end{bmatrix} + \mathbf{a}_{4} \cdot \begin{bmatrix} 1 \\ \omega^{4} \\ 1 \\ \omega^{4} \\ 1 \end{bmatrix} + \mathbf{a}_{6} \cdot \begin{bmatrix} 1 \\ \omega^{6} \\ \omega^{4} \\ \omega^{2} \\ 1 \\ \omega^{4} \end{bmatrix} = \mathbf{a}_{0} \cdot \begin{bmatrix} 1 \\ 1 \\ 1 \\ 1 \end{bmatrix} + \mathbf{a}_{2} \cdot \begin{bmatrix} 1 \\ \omega^{2} \\ \omega^{4} \\ \omega^{6} \end{bmatrix} + \mathbf{a}_{4} \cdot \begin{bmatrix} 1 \\ \omega^{6} \\ \omega^{4} \\ \omega^{2} \end{bmatrix} = \mathbf{ditto}$$

$$+a_{1} \cdot \begin{bmatrix} 1 \\ \omega \\ \omega^{2} \\ \omega^{3} \\ \omega^{4} \\ \omega^{5} \\ \omega^{6} \\ \omega^{7} \end{bmatrix} +a_{3} \cdot \begin{bmatrix} 1 \\ \omega^{3} \\ \omega^{6} \\ \omega^{4} \\ \omega^{7} \\ \omega^{2} \\ \omega^{5} \end{bmatrix} +a_{5} \cdot \begin{bmatrix} 1 \\ \omega^{5} \\ \omega^{2} \\ \omega^{4} \\ \omega^{6} \\ \omega^{3} \\ \omega^{6} \\ \omega^{3} \end{bmatrix} +a_{7} \cdot \begin{bmatrix} 1 \\ \omega^{7} \\ \omega^{6} \\ \omega^{5} \\ \omega^{4} \\ \omega^{3} \\ \omega^{2} \\ \omega^{3} \end{bmatrix}$$



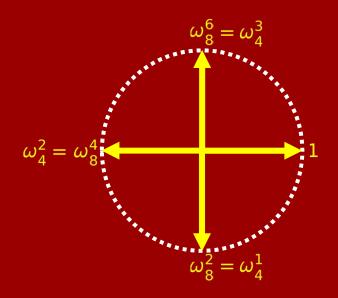
$$= \mathbf{a}_{0} \cdot \begin{bmatrix} 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \end{bmatrix} + \mathbf{a}_{2} \cdot \begin{bmatrix} 1 \\ \omega^{2} \\ \omega^{4} \\ \omega^{6} \\ 1 \\ \omega^{2} \\ \omega^{4} \\ \omega^{6} \end{bmatrix} + \mathbf{a}_{4} \cdot \begin{bmatrix} 1 \\ \omega^{4} \\ 1 \\ \omega^{4} \\ 1 \\ \omega^{4} \\ 1 \end{bmatrix} + \mathbf{a}_{6} \cdot \begin{bmatrix} 1 \\ \omega^{6} \\ \omega^{4} \\ \omega^{2} \\ 1 \\ \omega^{6} \\ \omega^{4} \\ \omega^{2} \end{bmatrix} = \mathbf{a}_{0} \cdot \begin{bmatrix} 1 \\ 1 \\ 1 \\ 1 \end{bmatrix} + \mathbf{a}_{2} \cdot \begin{bmatrix} 1 \\ \omega^{2} \\ \omega^{4} \\ \omega^{6} \end{bmatrix} + \mathbf{a}_{4} \cdot \begin{bmatrix} 1 \\ \omega^{6} \\ \omega^{4} \\ \omega^{2} \end{bmatrix}$$

$$= \mathbf{a}_{0} \cdot \begin{bmatrix} 1 \\ 1 \\ 1 \\ 1 \end{bmatrix} + \mathbf{a}_{2} \cdot \begin{bmatrix} 1 \\ \omega^{2} \\ \omega^{4} \\ \omega^{6} \end{bmatrix} + \mathbf{a}_{4} \cdot \begin{bmatrix} 1 \\ \omega^{6} \\ \omega^{4} \\ \omega^{2} \end{bmatrix}$$

$$= \mathbf{ditto}$$

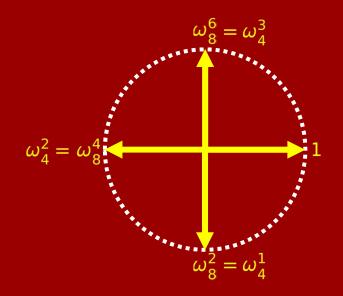
$$\mathbf{ditto}$$

$$+a_{1} \cdot \begin{bmatrix} 1 \\ \omega \\ \omega^{2} \\ \omega^{3} \\ \omega^{4} \\ \omega^{5} \\ \omega^{6} \\ \omega^{7} \end{bmatrix} +a_{3} \cdot \begin{bmatrix} 1 \\ \omega^{3} \\ \omega^{6} \\ \omega^{4} \\ \omega^{7} \\ \omega^{2} \\ \omega^{5} \end{bmatrix} +a_{5} \cdot \begin{bmatrix} 1 \\ \omega^{5} \\ \omega^{2} \\ \omega^{7} \\ \omega^{4} \\ \omega^{6} \\ \omega^{3} \\ \omega^{6} \\ \omega^{3} \end{bmatrix} +a_{7} \cdot \begin{bmatrix} 1 \\ \omega^{7} \\ \omega^{6} \\ \omega^{5} \\ \omega^{4} \\ \omega^{3} \\ \omega^{2} \\ \omega^{2} \\ \omega^{3} \end{bmatrix}$$



$$= \mathbf{a}_{0} \cdot \begin{bmatrix} 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \end{bmatrix} + \mathbf{a}_{2} \cdot \begin{bmatrix} 1 \\ \omega^{2} \\ \omega^{4} \\ \omega^{6} \\ 1 \end{bmatrix} + \mathbf{a}_{4} \cdot \begin{bmatrix} 1 \\ \omega^{4} \\ 1 \\ \omega^{4} \\ 1 \end{bmatrix} + \mathbf{a}_{6} \cdot \begin{bmatrix} 1 \\ \omega^{6} \\ \omega^{4} \\ \omega^{2} \\ 1 \\ \omega^{4} \end{bmatrix} = \mathbf{a}_{0} \cdot \begin{bmatrix} 1 \\ 1 \\ 1 \\ 1 \end{bmatrix} + \mathbf{a}_{2} \cdot \begin{bmatrix} 1 \\ \omega^{1}_{4} \\ \omega^{2}_{4} \\ \omega^{3}_{4} \end{bmatrix} + \mathbf{a}_{4} \cdot \begin{bmatrix} 1 \\ \omega^{3}_{4} \\ \omega^{2}_{4} \\ \omega^{4}_{4} \end{bmatrix} + \mathbf{a}_{6} \cdot \begin{bmatrix} 1 \\ \omega^{4} \\ \omega^{2} \\ \omega^{4} \end{bmatrix} = \mathbf{ditto}$$

$$+a_{1} \cdot \begin{bmatrix} 1 \\ \omega \\ \omega^{2} \\ \omega^{3} \\ \omega^{4} \\ \omega^{5} \\ \omega^{6} \\ \omega^{7} \end{bmatrix} +a_{3} \cdot \begin{bmatrix} 1 \\ \omega^{3} \\ \omega^{6} \\ \omega^{4} \\ \omega^{7} \\ \omega^{6} \\ \omega^{7} \end{bmatrix} +a_{5} \cdot \begin{bmatrix} 1 \\ \omega^{5} \\ \omega^{2} \\ \omega^{7} \\ \omega^{4} \\ \omega^{6} \\ \omega^{3} \\ \omega^{6} \\ \omega^{3} \end{bmatrix} +a_{7} \cdot \begin{bmatrix} 1 \\ \omega^{7} \\ \omega^{6} \\ \omega^{5} \\ \omega^{4} \\ \omega^{3} \\ \omega^{2} \\ \omega^{2} \\ \omega^{3} \end{bmatrix}$$



$$= a_{0} \cdot \begin{bmatrix} 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \end{bmatrix} + a_{2} \cdot \begin{bmatrix} 1 \\ \omega^{2} \\ \omega^{4} \\ 1 \\ \omega^{6} \\ \omega^{4} \end{bmatrix} + a_{4} \cdot \begin{bmatrix} 1 \\ \omega^{4} \\ 1 \\ \omega^{4} \\ 1 \\ \omega^{4} \\ 1 \end{bmatrix} + a_{6} \cdot \begin{bmatrix} 1 \\ \omega^{6} \\ \omega^{4} \\ \omega^{2} \\ 1 \\ \omega^{6} \\ \omega^{4} \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & \omega_{4}^{1} & \omega_{4}^{2} & \omega_{4}^{3} \\ 1 & \omega_{4}^{2} & 1 & \omega_{4}^{2} \\ 1 & \omega_{4}^{3} & \omega_{4}^{2} & \omega_{4}^{1} \end{bmatrix} \cdot \begin{bmatrix} a_{0} \\ a_{2} \\ a_{4} \\ a_{6} \end{bmatrix}$$

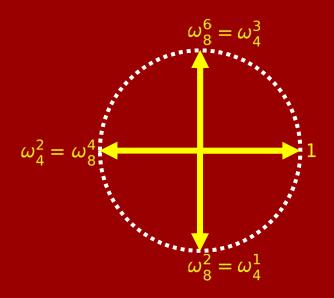
$$= \begin{bmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & \omega_{4}^{1} & \omega_{4}^{2} & \omega_{4}^{3} \\ 1 & \omega_{4}^{3} & \omega_{4}^{2} & \omega_{4}^{1} \end{bmatrix} \cdot \begin{bmatrix} a_{0} \\ a_{2} \\ a_{4} \\ a_{6} \end{bmatrix}$$

$$= \begin{bmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & \omega_{4}^{1} & \omega_{4}^{2} & \omega_{4}^{3} \\ 1 & \omega_{4}^{3} & \omega_{4}^{2} & \omega_{4}^{1} \end{bmatrix} \cdot \begin{bmatrix} a_{0} \\ a_{2} \\ a_{4} \\ a_{6} \end{bmatrix}$$

$$= \begin{bmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & \omega_{4}^{1} & \omega_{4}^{2} & \omega_{4}^{3} \\ 1 & \omega_{4}^{3} & \omega_{4}^{2} & \omega_{4}^{1} \end{bmatrix} \cdot \begin{bmatrix} a_{0} \\ a_{2} \\ a_{4} \\ a_{6} \end{bmatrix}$$

$$= \begin{bmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & \omega_{4}^{1} & \omega_{4}^{2} & \omega_{4}^{3} \\ 1 & \omega_{4}^{3} & \omega_{4}^{2} & \omega_{4}^{1} \end{bmatrix} \cdot \begin{bmatrix} a_{0} \\ a_{2} \\ a_{4} \\ a_{6} \end{bmatrix}$$

$$+a_{1} \cdot \begin{bmatrix} 1 \\ \omega \\ \omega^{2} \\ \omega^{3} \\ \omega^{4} \\ \omega^{5} \\ \omega^{6} \\ \omega^{7} \end{bmatrix} +a_{3} \cdot \begin{bmatrix} 1 \\ \omega^{3} \\ \omega^{6} \\ \omega^{4} \\ \omega^{7} \\ \omega^{2} \\ \omega^{5} \end{bmatrix} +a_{5} \cdot \begin{bmatrix} 1 \\ \omega^{5} \\ \omega^{2} \\ \omega^{7} \\ \omega^{4} \\ \omega^{6} \\ \omega^{3} \\ \omega^{6} \\ \omega^{2} \\ \omega^{5} \end{bmatrix}$$



$$= a_{0} \cdot \begin{bmatrix} 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \end{bmatrix} + a_{2} \cdot \begin{bmatrix} 1 \\ \omega^{2} \\ \omega^{4} \\ 1 \\ \omega^{6} \\ \omega^{4} \\ 1 \end{bmatrix} + a_{4} \cdot \begin{bmatrix} 1 \\ \omega^{4} \\ 1 \\ \omega^{4} \\ 1 \\ \omega^{4} \\ 1 \end{bmatrix} + a_{6} \cdot \begin{bmatrix} 1 \\ \omega^{6} \\ \omega^{4} \\ \omega^{2} \\ 1 \\ \omega^{6} \\ \omega^{4} \\ 0^{2} \end{bmatrix} = DFT_{4} \cdot \begin{bmatrix} a_{0} \\ a_{2} \\ a_{4} \\ a_{6} \end{bmatrix}$$

$$= ditto$$

$$+a_{1} \cdot \begin{bmatrix} 1 \\ \omega \\ \omega^{2} \\ \omega^{3} \\ \omega^{4} \\ \omega^{5} \\ \omega^{6} \\ \omega^{7} \end{bmatrix} +a_{3} \cdot \begin{bmatrix} 1 \\ \omega^{3} \\ \omega^{6} \\ \omega^{4} \\ \omega^{7} \\ \omega^{6} \\ \omega^{7} \\ \omega^{6} \\ \omega^{7} \\ \omega^{6} \\ \omega^{6} \\ \omega^{3} \end{bmatrix} +a_{5} \cdot \begin{bmatrix} 1 \\ \omega^{5} \\ \omega^{2} \\ \omega^{4} \\ \omega^{6} \\ \omega^{6} \\ \omega^{3} \\ \omega^{6} \\ \omega^{2} \\ \omega^{6} \\ \omega^{3} \end{bmatrix}$$

$$= a_0 \cdot \begin{bmatrix} 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \end{bmatrix} + a_2 \cdot \begin{bmatrix} 1 \\ \omega^2 \\ \omega^4 \\ 1 \\ \omega^6 \end{bmatrix} + a_4 \cdot \begin{bmatrix} 1 \\ \omega^4 \\ 1 \\ \omega^4 \\ 1 \end{bmatrix} + a_6 \cdot \begin{bmatrix} 1 \\ \omega^6 \\ \omega^4 \\ \omega^2 \\ 1 \\ \omega^6 \\ \omega^4 \\ 1 \end{bmatrix}$$

$$+a_{1} \cdot \begin{bmatrix} 1 \\ \omega \\ \omega^{2} \\ \omega^{3} \\ \omega^{4} \\ \omega^{5} \\ \omega^{6} \\ \omega^{7} \end{bmatrix} +a_{3} \cdot \begin{bmatrix} 1 \\ \omega^{3} \\ \omega^{6} \\ \omega^{4} \\ \omega^{7} \\ \omega^{6} \\ \omega^{7} \end{bmatrix} +a_{5} \cdot \begin{bmatrix} 1 \\ \omega^{5} \\ \omega^{2} \\ \omega^{4} \\ \omega^{6} \\ \omega^{3} \\ \omega^{6} \\ \omega^{3} \end{bmatrix} +a_{7} \cdot \begin{bmatrix} 1 \\ \omega^{7} \\ \omega^{6} \\ \omega^{4} \\ \omega^{3} \\ \omega^{2} \\ \omega^{2} \\ \omega^{3} \end{bmatrix}$$

$$P(x) = P^{0}(x^{2}) + x P^{1}(x^{2})$$

Computable with 1 application of DFT₄ to (a_0,a_2,a_4,a_6) , and some copying.

Now to get this, apply the above to (a_1,a_3,a_5,a_7) , and then multiply the j^{th} row by ω^j , for $0 \le j < 7$.

Total: 2 applications of DFT₄, plus "O(8)" more operations.

Summary

- Can multiply two polynomials of degree < N
 in O(N log N) time.
- DFT_N reduces Coefficients Representation to Values Representation over roots of unity.
- FFT_N computes DFT_N (and inverse) in O(N log N) time.
- DFT_N has many uses in CS & Engineering.