

$$\begin{pmatrix} F_2 & W_2 F_2 \\ F_2 & -W_2 F_2 \end{pmatrix} \quad (1)$$

$$= \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & \omega & \omega^2 & \omega^3 \\ 1 & \omega^2 & 1 & \omega^2 \\ 1 & \omega^3 & \omega^2 & \omega \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \quad (2)$$

$$F_n = (F_2 \otimes I_m) T_m^{2m} (I_2 \otimes F_m) L_m^{2m} \quad (3)$$

As  $(L_m^{2m})^{-1}$  is the inverse

$$F_n L_m^{2m} = (F_2 \otimes I_m) T_m^{2m} (I_2 \otimes F_m) \quad (4)$$

$L_m^{2m}$  takes stride 2(just the columns). What is this?

$$W_m = \begin{pmatrix} 1 & \dots \\ 0 & \omega \end{pmatrix} \quad (5)$$

etc.

$$\begin{pmatrix} \omega^{i2j} & \omega^{i(2j+1)} \\ \omega^{(i+m)2j} & \omega^{(i+m)(2j+1)} \end{pmatrix} = \begin{pmatrix} \omega^{i2j} & \omega^{2ij}\omega^i \\ \omega^{2ij}\omega^{2mj} & \omega^{2ij}\omega^{2mj}\omega^m\omega^i \end{pmatrix} \quad (6)$$

This is

$$\begin{pmatrix} F_m & W_m F_m \\ F_m & -W_m F_m \end{pmatrix} = \begin{pmatrix} I_m & I_m \\ I_m & -I_m \end{pmatrix} \begin{pmatrix} I_m & 0 \\ 0 & W_m \end{pmatrix} \begin{pmatrix} F_m & 0 \\ 0 & F_m \end{pmatrix} \quad (7)$$

Thus proven

Notes

$$\frac{C[x]}{X^{rs} - 1} \quad (8)$$

with fft  $F_r \otimes I_s$

$$\prod_{i=0}^{r-1} \frac{C[x]}{X^s - \omega_r^i} \quad (9)$$

example

$$x^5 + x^4 + x^3 + x^2 + x + 1 \quad (10)$$

mod  $x^3 - \alpha$

$$\alpha x^2 + \alpha x + \alpha + x^2 + x_1 \quad (11)$$

We are grouping together chunks of size 3.

When we do dft, we evaluate the rs size vector at each  $\omega^i$  for each ith power.

Then we make  $x \rightarrow \omega_R^i X$

$r = 3, s = 2$ .

$$x^6 - 1 = (x^2 - 1)(x^2 - \omega)(x^2 - \omega^2) \quad (12)$$

These polynomials are

$$f_0 + f_x \dots + f_5 x^5 \quad (13)$$

this mod  $x^2 - \omega^i$  then we get

$$f_0 + f_2 + f_4 + (f_1 + f_3 + f_5)x \quad (14)$$

if we have the coefficients as vectors

$$f_0, f_2, f_4, f_1, f_3, f_5 \quad (15)$$

Then we group together as

$$f_0 + f_2 + f_4, f_1 + f_3 + f_5 \quad (16)$$

This is  $1, 1, 1 \otimes I_2$ . This works as when multiplied with  $(f_0, f_1, \dots, f_5)$  we get the vector of size 2 which is the If  $\omega$  we get

$$f_0 + f_2 \omega + f_4 \omega^2 + (f_1 + f_3 \omega + f_5 \omega^2)x \quad (17)$$

This is the same as

$$F_r \otimes I_s \quad (18)$$

$$(x^2 - \omega^i) \quad (19)$$

is

$$\begin{pmatrix} 1 & 0 \\ 0 & \omega^i \end{pmatrix} \begin{pmatrix} f_0 \\ f_1 \end{pmatrix} \quad (20)$$

since after reduction we just have  $f_0 + f_1 \omega^i x$ .

to get rid of  $\omega$

$$\prod_{i=0}^{r-1} \frac{C[x]}{X^s - \omega_r^i} \quad (21)$$

we take it out using the matrix in dfft. Then we can make a matrix

$$\begin{pmatrix} 1 & 0 & \dots & \\ 0 & 1 & \dots & \\ \dots & \dots & \dots & \dots \end{pmatrix} \quad (22)$$

Which is triangle matrix! Once we project this out we get

$$\prod_{i=0}^{r-1} \frac{C[x]}{X^s - 1} \quad (23)$$

which is

$$I_r \otimes F_s \quad (24)$$