Given theorem

$$F_{rs} = (F_r \otimes I_s) T_s^{rs} (I_r \otimes F_s) L_r^{rs} \tag{1}$$

Multipled both sides by $(L_r^{rs})^{-1} = L_r^{rs}$

$$F_{rs} L_r^{rs} \tag{2}$$

L_r^{rs} is permutation of size rs of size r. F_{rs} looks something like

$$F_{rs} = \begin{pmatrix} 1 & 1 & 1 & 1 & ..... & 1 \\ 1 & \omega & \omega^2 & \omega^3 & .... & \omega^{-1} \\ 1 & \omega^2 & \omega^4 & \omega^6 & .... & \omega^{-2} \\ ... & ... & ... & ... & .... & ... \\ 1 & \omega^r & \omega^{2r} & \omega^{3r} & .... & \omega^{-2r} \\ ... & ... & ... & ... & .... & ... \\ 1 & \omega^{2r} & \omega^{4r} & \omega^{6r} & .... & \omega^{-4r} \\ ... & ... & ... & ... & .... & ... \\ 1 & \omega^{-1} & \omega^{-2} & \omega^{-3} & .... & \omega^1 \end{pmatrix} \tag{3}$$

Now,

$$F_{rs} L_r^{rs} = \begin{pmatrix} 1 & 1 & 1 & 1 & ..... & 1 \\ 1 & \omega^r & \omega^{2r} & \omega^{3r} & .... & \omega^{-1} \\ 1 & \omega^{2r} & \omega^{4r} & \omega^{6r} & .... & \omega^{-2} \\ ... & ... & ... & ... & .... & ... \\ 1 & \omega^{r^2} & \omega^{2r^2} & \omega^{3r^2} & .... & \omega^{-2r} \\ ... & ... & ... & ... & .... & ... \\ 1 & \omega^{2r^2} & \omega^{4r^2} & \omega^{6r^2} & .... & \omega^{-4r} \\ ... & ... & ... & ... & .... & ... \\ 1 & \omega^{-r} & \omega^{-2r} & \omega^{-3r} & .... & \omega^1 \end{pmatrix} \tag{4}$$

$$F_{rs} L_r^{rs} = \begin{pmatrix} \omega^{irj} & \omega^{i(rj+1)} & \omega^{i(rj+2)} & ... & \omega^{i(rj+r-1)} \\ \omega^{(i+s)rj} & \omega^{(i+s)(rj+1)} & \omega^{(i+s)(rj+2)} & ... & \omega^{(i+s)(rj+r-1)} \\ \omega^{(i+2s)rj} & \omega^{(i+2s)(rj+1)} & \omega^{(i+2s)(rj+2)} & ... & \omega^{(i+2s)(rj+r-1)} \\ ... & ... & ... & ... & ... \\ \omega^{(i+(r-1)s)rj} & \omega^{(i+(r-1)s)(rj+1)} & \omega^{(i+(r-1)s)(rj+2)} & ... & \omega^{(i+(r-1)s)(rj+r-1)} \end{pmatrix} \tag{5}$$

$$= \begin{pmatrix} \omega^{irj} & \omega^{irj}\omega^{i} & \omega^{irj}\omega^{2i} & ... & \omega^{irj}\omega^{i(r-1)} \\ \omega^{irj}\omega^{rsj} & \omega^{irj}\omega^{i}\omega^{rsj}\omega^{s} & \omega^{irj}\omega^{2i}\omega^{rsj}\omega^{2s} & ... & \omega^{irj}\omega^{si}\omega^{-i}\omega^{rsj}\omega^{sr}\omega^{-s} \\ \omega^{irj}\omega^{2rsj} & \omega^{irj}\omega^{i}\omega^{2rsj}\omega^{2s} & \omega^{irj}\omega^{2i}\omega^{2rsj}\omega^{4s} & ... & \omega^{irj}\omega^{si}\omega^{-i}\omega^{2rsj}\omega^{2sr}\omega^{-2s} \\ ... & ... & ... & ... & ... \end{pmatrix} \tag{6}$$

Now as $\omega^{rs} = 1$,

$$F_{rs} L_r^{rs} = \begin{pmatrix} \omega^{irj} & \omega^{irj}\omega^{i} & \omega^{irj}\omega^{2i} & ... & \omega^{irj}\omega^{i(s-1)} \\ \omega^{irj} & \omega^{irj}\omega^{i}\omega^{s} & \omega^{irj}\omega^{2i}\omega^{2s} & ... & \omega^{irj}\omega^{si}\omega^{-i}\omega^{-s} \\ \omega^{irj} & \omega^{irj}\omega^{i}\omega^{2s} & \omega^{irj}\omega^{2i}\omega^{4s} & ... & \omega^{irj}\omega^{si}\omega^{-i}\omega^{-2s} \\ ... & ... & ... & ... & ... \end{pmatrix} \tag{7}$$

$$\omega_{rs}^{irj} = \omega_s^{ij} = F_r \tag{8}$$

$$\omega_{rs}^{i} = W_r \tag{9}$$

Huh, isn't this the top part of W_{rs}?

$$\omega_{rs}^{s} = \omega_s \tag{10}$$

$$F_{rs}L_r^{rs} = \begin{pmatrix} F_r & F_rW_r & F_rW_r^2 & ... & F_rW_r^(s-1) \\ F_r & F_rW_r\omega_s & F_rW_r^2\omega_s^2 & ... & F_rW_r^{s-1}\omega_s^{-1} \\ F_r & F_rW_r\omega_s^2 & F_rW_r^2\omega_s^4 & ... & F_rW_r^{s-1}\omega_s^{-2} \\ ... & ... & ... & ... & ... \\ F_r & F_rW_r\omega_s^{-1} & F_rW_r^2\omega_s^{-2} & ... & F_rW_r^{s-1}\omega_s \end{pmatrix} \tag{11}$$

There seems to be structure here. Like if we look at the ωs it's almost like in the middle we have F_rW_r with a tensor product of F_s but with W_r to some powers.

Now,

$$I_s \otimes F_r = \begin{pmatrix} F_r & 0 & 0 & ... & \\ 0 & F_r & 0 & ... & \\ ... & ... & ... & ... & \\ 0 & 0 & 0 & ... & F_r \end{pmatrix} \tag{12}$$

$$T_s^{rs} = \begin{pmatrix} W_s^0 & 0 & 0 & .... \\ 0 & W_s^1 & 0 & .... \\ 0 & 0 & W_s^2 & .... \\ .. & .. & .. & ... \\ 0 & 0 & 0 & W_s^{r-1} \end{pmatrix} \tag{13}$$

When these are multiplied together we have

$$T_s^{rs}(I_s \otimes F_r) = \begin{pmatrix} F_r & 0 & 0 & .... \\ 0 & F_rW_s & 0 & .... \\ 0 & 0 & F_rW_s^2 & .... \\ .. & .. & .. & ... \\ 0 & 0 & 0 & F_rW_s^{r-1} \end{pmatrix} \tag{14}$$

Now,

$$F_s \otimes I_r = \begin{pmatrix} I_r & I_r & .... & I_r \\ I_r & \omega_sI_r & ... & \omega_s^{-1}I_r \\ ... & .... & ... & ... \\ I_r & \omega_s^{-1}I_r & ... & \omega_sI_r \end{pmatrix} \tag{15}$$

Now, when we combine this all together we have

$$\begin{pmatrix} F_r & F_rW_r & F_rW_r^2 & ... & F_rW_r^(s-1) \\ F_r & F_rW_r\omega_s & F_rW_r^2\omega_s^2 & ... & F_rW_r^{s-1}\omega_s^{-1} \\ F_r & F_rW_r\omega_s^2 & F_rW_r^2\omega_s^4 & ... & F_rW_r^{s-1}\omega_s^{-2} \\ ... & ... & ... & ... & ... \\ F_r & F_rW_r\omega_s^{-1} & F_rW_r^2\omega_s^{-2} & ... & F_rW_r^{s-1}\omega_s \end{pmatrix} \tag{16}$$

$$\frac{C[x]}{X^{rs}-1} \tag{17}$$

with fft $F_r \otimes I_s$

$$\prod_{i=0}^{r-1} \frac{C[x]}{X^s - \omega_r^i} \tag{18}$$

example

$$x^5 + x^4 + x^3 + x^2 + x + 1 \tag{19}$$

mod $x^3 - \alpha$

$$\alpha x^2 + \alpha x + \alpha + x^2 + x_1 \tag{20}$$

We are grouping together chunks of size 3.

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

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

$r = 3, s = 2.$

$$x^6 - 1 = (x^2 - 1)(x^2 - \omega)(x^2 - \omega^2) \tag{21}$$

These polynomials are

$$f_0 + f_x ... + f_5 x^5 \tag{22}$$

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

$$f_0 + f_2 + f_4 + (f_1 + f_3 + f_5)x \tag{23}$$

if we have the coefficients as vectors

$$f_0, f_2, f_4, f_1, f_3, f_5 \tag{24}$$

Then we group together as

$$f_0 + f_2 + f_4, f_1 + f_3 + f_5 \tag{25}$$

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

$$f_0 + f_2\omega + f_4\omega^2 + (f_1 + f_3\omega + f_5\omega^2)x \tag{26}$$

This is the same as

$$F_r \otimes I_s \tag{27}$$

$$(x^2 - \omega^i) \tag{28}$$

is

$$\begin{pmatrix} 1 & 0 \\ 0 & \omega^i \end{pmatrix} \begin{pmatrix} f_0 \\ f_1 \end{pmatrix} \tag{29}$$

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

to get rid of ω

$$\prod_{i=0}^{r-1} \frac{C[x]}{X^s - \omega_r^i} \tag{30}$$

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

$$\begin{pmatrix} 1 & 0 & .... & \\ 0 & 1 & .... & \\ .. & .. & 1 & 0 \\ .. & .. & 0 & \omega \\ ... & & & \end{pmatrix} \tag{31}$$

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

$$\prod_{i=0}^{r-1} \frac{C[x]}{X^s - 1} \tag{32}$$

which is

$$I_r \otimes F_s \tag{33}$$