

For simplicity, let $n = q - 1$.

Observe that, when $k \neq 0$,

$$\sum_{i=0}^{n-1} \alpha^{ik} = 0, \forall \alpha \in \mathbb{Z}_q^*,$$

and when $k = 0$, obviously

$$\sum_{i=0}^{n-1} \alpha^{ik} = \sum_{i=0}^{n-1} \alpha^0 = n, \forall \alpha \in \mathbb{Z}_q^*.$$

Therefore we have

$$\begin{aligned} f(i) &= \frac{1}{n} \sum_{k,j} f(j) \cdot \alpha^{k(j-i)} \\ &= \frac{1}{n} \sum_{k,j} f(j) \cdot \alpha^{kj-ki} \\ &= \frac{1}{n} \sum_{k,j} f(j) \cdot \alpha^{kj} \cdot \alpha^{-ik} \\ &= \frac{1}{n} \sum_k F(k) \cdot \alpha^{-ik}, \end{aligned}$$

where $F(k) \stackrel{\text{def}}{=} \sum_j f(j) \cdot \alpha^{kj}$.

We can compute $F(k)$ recursively —

$$\begin{aligned} F^{(0)}(k) &= \sum_{j=0}^{n-1} f(j) \cdot \alpha^{kj} \\ &= \sum_{l=0}^{\frac{n}{2}-1} f(2l) \cdot \alpha^{k \cdot 2l} + \alpha^k \cdot \sum_{l=0}^{\frac{n}{2}-1} f(2l+1) \cdot \alpha^{k \cdot 2l} \\ &= F_0^{(1)}(k \bmod \frac{n}{2}) + \alpha^k \cdot F_1^{(1)}(k \bmod \frac{n}{2}), \end{aligned}$$

where $F_0^{(1)}$ and $F_1^{(1)}$ are the NTT's of with halved parameter n .

We can compute $F(k)$ recursively —

$$\begin{aligned} F^{(0)}(k) &= \sum_{j=0}^{n-1} f(j) \cdot \alpha^{kj} \\ &= \sum_{l=0}^{\frac{n}{2}-1} f(2l) \cdot \alpha^{k \cdot 2l} + \alpha^k \cdot \sum_{l=0}^{\frac{n}{2}-1} f(2l+1) \cdot \alpha^{k \cdot 2l} \\ &= F_0^{(1)}(k \bmod \frac{n}{2}) + \alpha^k \cdot F_1^{(1)}(k \bmod \frac{n}{2}). \end{aligned}$$

Notice the computation of $F_0^{(1)}$ uses $f(j)$'s for **even** j 's, and that of $F_1^{(1)}$ uses $f(j)$'s for **odd** j 's.

We can compute $F(k)$ recursively —

$$\begin{aligned} F^{(0)}(k) &= F_0^{(1)}(k') + \alpha^k \cdot F_1^{(1)}(k') \\ &= F_0^{(2)}(k' \bmod \frac{n}{4}) + \alpha^{k'} \cdot F_1^{(2)}(k' \bmod \frac{n}{4}) \\ &\quad + \alpha^k \cdot F_2^{(2)}(k' \bmod \frac{n}{4}) + \alpha^{k+k'} \cdot F_3^{(2)}(k' \bmod \frac{n}{4}) \\ &= \dots, \end{aligned}$$

where $k' = k \bmod \frac{n}{2}$.

We can compute $F(k)$ recursively —

$$\begin{aligned} F^{(0)}(k) &= F_0^{(1)}(k') + \alpha^k \cdot F_1^{(1)}(k') \\ &= F_0^{(2)}(k' \bmod \frac{n}{4}) + \alpha^{k'} \cdot F_1^{(2)}(k' \bmod \frac{n}{4}) \\ &\quad + \alpha^k \cdot F_2^{(2)}(k' \bmod \frac{n}{4}) + \alpha^{k+k'} \cdot F_3^{(2)}(k' \bmod \frac{n}{4}) \\ &= \dots \end{aligned}$$

The computation of $F_0^{(2)}, F_1^{(2)}$ uses $f(j)$'s for **even** j 's, and that of $F_2^{(2)}, F_3^{(2)}$ uses $f(j)$'s for **odd** j 's.

We can compute $F(k)$ recursively —

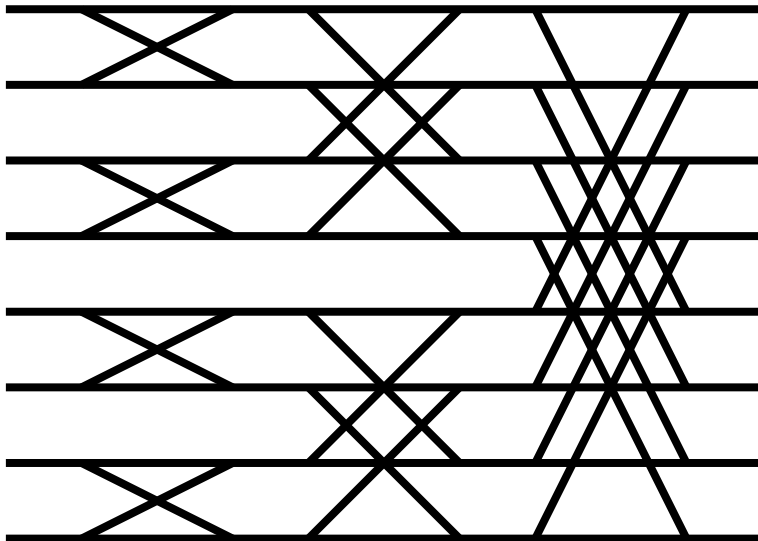
$$\begin{aligned} F^{(0)}(k) &= F_0^{(1)}(k') + \alpha^k \cdot F_1^{(1)}(k') \\ &= F_0^{(2)}(k' \bmod \frac{n}{4}) + \alpha^{k'} \cdot F_1^{(2)}(k' \bmod \frac{n}{4}) \\ &\quad + \alpha^k \cdot F_2^{(2)}(k' \bmod \frac{n}{4}) + \alpha^{k+k'} \cdot F_3^{(2)}(k' \bmod \frac{n}{4}) \\ &= \dots \end{aligned}$$

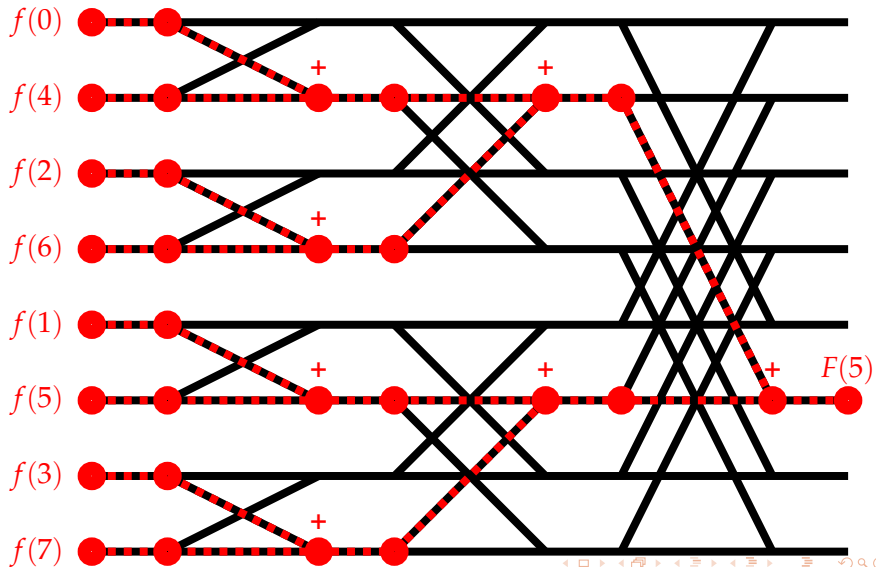
The computation of $F_0^{(2)}, F_1^{(2)}$ uses $f(j)$'s for **even** j 's, and that of $F_2^{(2)}, F_3^{(2)}$ uses $f(j)$'s for **odd** j 's. The computation of $F_0^{(2)}, F_2^{(2)}$ uses $f(j)$'s for the j 's s.t. $(j \bmod 2) \bmod 4 = 0$, and that of $F_1^{(2)}, F_3^{(2)}$ uses $f(j)$'s for the j 's s.t. $(j \bmod 2) \bmod 4 \neq 0$.

We say an index is odder than another if it has 1 in a lower bits.
We place the j 's following the setting (which is the origin of bits-flipping):

**The more even — the upper;
The odder — the lower.**

Hence the butterfly structure —





Terms from odd branches will be multiplied by α^k before addition.