Fast Integer Multiplication

- Fast poly. mult. used the viewpoint: [Functional]
  $f(x)$ is a function that takes values & can be learnt from the values.

- Design auxiliary poly. out of an integer.
- Say, $a, b \in \mathbb{N}$ are $\ell = 2^n$ bit numbers.
- Let $k := 2^{\lceil n/2 \rceil}$, $m := 2^{\lfloor n/2 \rfloor}$. $\triangleright$ $k \cdot m = \ell$
- Define $\hat{a}(x) := \sum_{i=0}^{m-1} \hat{a}_i \cdot x^i$; $\hat{b}(x) := \sum_{i=0}^{m-1} \hat{b}_i \cdot x^i$

▷ $0 \leq \hat{a}_i , \hat{b}_i < 2^k \quad (\forall\, 0 \leq i \leq m-1)$.

▷ $\hat{a}(x)\big|_{x=2^k} = a \;\; ; \;\; \hat{b}(x)\big|_{x=2^k} = b$.

▷ $\deg \hat{a} , \deg \hat{b} < m$.

▷ Coefficient of x^j in $\hat{a} \cdot \hat{b}$ is: $\sum_{i=0}^{j} \hat{a}_i \cdot \hat{b}_{j-i}$.
It has magnitude $< \underline{m \cdot 2^{2k}} < 2^{3k}$

▷ $\hat{a}(x) \cdot \hat{b}(x) \big|_{x=2^k} = a \cdot b$

↳ One cannot invoke Fast Poly. Mult. directly!

- <u>Idea</u>: We compute the polynomial product $\hat{c} := \hat{a}(x) \cdot \hat{b}(x) \mod \langle 2^{3k}+1 \rangle$.
  Finally, evaluate $\hat{c}(2^k)$.

▷ $R := \mathbb{Z}/\langle 2^{3k}+1 \rangle$ has a $(2k)$-th primitive root of unity $\omega := 8$. [$\deg < m < 2k$]

- So, we can follow the poly. mult. algo. based on DFT[ω]:
    1) Do DFT[ω] of $\hat{a}$, $\hat{b}$ in $R[x]$.
    2) Compute m products: $\hat{a}(\omega^i) \cdot \hat{b}(\omega^i) =: \hat{c}(\omega^i)$ in R.

3) Do $DFT[\omega^{-1}]$ of $\{\hat{c}(\omega^i) \mid i\}$ to get $\hat{c}(x)$.

4) Output $\hat{c}(2^k)$. $[= a \cdot b]$

Complexity Analysis:

- Steps (1) & (3) : By fast DFT we do it in $O(m \lg m)$ R-operations.

  $\equiv O(k m \lg m)$ bit-operations [time].

  [$\because$ multiplication is by ω^i in R]

- Step (2) : m multiplications, each $3k$-bits. So, we get the recurrence:

$$T(\ell) \leq m \cdot T(3k) + O(\ell \cdot \lg \ell)$$

$$\Rightarrow \quad T(\ell) \leq O\left(\ell \cdot 3^{\lg \lg \ell}\right) = O(\ell \cdot \lg^{\alpha} \ell)$$

where $\alpha := \lg 3 \in (1,2)$

$$= \tilde{O}(\ell) \text{ time!}$$

<u>State of the art</u>:

Schönhage-Strassen ('71): $O(\ell \cdot \lg \ell \cdot \lg \lg \ell)$-time

Fürer (2007): $O(\ell \cdot \underline{\lg \ell} \cdot 2^{O(\lg^* \ell)})$-time.

Harvey & van der Hoeven (Mar'19): $O(\ell \cdot \lg \ell)$-time.