Fast polynomial multiplication

- Say, f, g are polynomials in $R[x]$ of deg $\leq \ell$.

- We could beat the naive $O(\ell^2)$ time multiplication algorithm, by using evaluations & Gauss' trick.

- Suppose R has a primitive ℓ-th root of unity ω.

- <u>Idea</u>: (1) Evaluate f, g at $\omega^0, \omega^1, \dots, \omega^{\ell-1}$.

  (2) Multiply $f(\omega^i) \cdot g(\omega^i)$ in R.

  (3) Interpolate to get $f(x) \cdot g(x)$.

- Let $f(x) = \sum_{i=0}^{\ell-1} a_i x^i$, a_i's in R.

- Formally, we want to compute the <u>discrete Fourier transform</u>

$$DFT[\omega] : (a_0, \dots, a_{\ell-1}) \mapsto (f(\omega^0), \dots, f(\omega^{\ell-1})),$$

where $\ell := 2^n$, $n \in \mathbb{N}$.

(wlog, "pad" f)

<u>Lemma 1</u>: $\frac{1}{\ell} \cdot DFT[\omega^{-1}] \circ DFT[\omega] = Id$.

<u>Pf</u>: • $DFT[\omega]$ can be seen as the following matrix product

$$\begin{bmatrix} 1, 1, \dots, 1 \\ 1 \quad \omega \dots \omega^{\ell-1} \\ \vdots \\ 1 \quad \omega^{\ell-1} \dots \omega^{(\ell-1)(\ell-1)} \end{bmatrix} \cdot \begin{pmatrix} a_0 \\ \vdots \\ a_{\ell-1} \end{pmatrix} = \begin{pmatrix} f(1) \\ \vdots \\ f(\omega^{\ell-1}) \end{pmatrix}.$$

- Thus, the action $DFT[\omega^{-1}] \circ DFT[\omega]$ is:

$$\begin{bmatrix} 1 & 1 & \cdots & 1 \\ 1 & \omega^{-1} & \cdots & \omega^{-(\ell-1)} \\ \vdots & \vdots & & \vdots \\ 1 & \omega^{-(\ell-1)} & \cdots & \omega^{-(\ell-1)(\ell-1)} \end{bmatrix} \cdot \begin{bmatrix} 1 & 1 & \cdots & 1 \\ 1 & \omega & \cdots & \omega^{\ell-1} \\ \vdots & \vdots & & \vdots \\ 1 & \omega^{\ell-1} & \cdots & \omega^{(\ell-1)(\ell-1)} \end{bmatrix}$$

$$= \ell \cdot I_\ell \qquad \square$$

This requires ℓ to be a nonzerodivisor in R.

- Naively, computing ℓ evaluations takes $O(\ell^2)$ time. But Gauss had a better idea: (recurse!)

<u>Lemma 2</u>: $DFT[\omega]$ can be computed in $O(\ell \cdot \lg \ell)$ R-operations.

<u>Pf</u>: • Write $f(x) = f_0(x^2) + x \cdot f_1(x^2)$ & use divide-and-conquer:

(1) Compute $DFT[\omega^2]: f_0(x) \mapsto (e'_0, \ldots, e'_{\ell/2-1})$ & $DFT[\omega^2]: f_1(x) \mapsto (e''_0, \ldots, e''_{\ell/2-1})$.

(2) Compute $\forall\, 0 \le i \le \ell/2 - 1$,

$e_i := e'_i + \omega^i \cdot e''_i$ &

$e_{i+\frac{\ell}{2}} := e'_i - \omega^i \cdot e''_i$ $(\because \omega^{\ell/2} = -1)$

(3) Output $(e_0, \ldots, e_{\ell-1})$.

- We have the following recurrence for the time taken:

$$T(\ell) = 2 \cdot T(\ell/2) + O(\ell).$$

$$\Rightarrow T(\ell) = O(\ell \cdot \lg \ell). \qquad \square$$

<u>Theorem</u>: $h = f \cdot g$ can be computed in $O(\ell \cdot \lg \ell)$ R-operations.

Pf: • Essentially, compute DFT$[\omega]$ & then DFT$[\omega^{-1}]$.

- $\begin{matrix} f \\ g \end{matrix} \xrightarrow{\text{DFT}[\omega]} \begin{matrix} (f(1), .., f(\omega^{\ell-1})) \\ (g(1), .., g(\omega^{\ell-1})) \end{matrix} \xrightarrow{\text{Mult.}}$

$(f(1)g(1), \ldots\ldots, f(\omega^{\ell-1})\, g(\omega^{\ell-1})) \xrightarrow{\text{DFT}[\omega^{-1}]} \ell \cdot h$

$\square$

- What if R does not have an ℓ-th root of unity, $\ell = 2^n$?

zero & zerodivisors in R

- Say $2 \notin zd(R)$, but R has no ℓ-th root of unity.

We create ω "out of thin air"!
& recurse more.

- Consider $E := R[y]/\langle y^{\ell/2}+1\rangle$ & $\omega := y$ in E.

is irreducible over $\mathbb{Q}$

- Let us rewrite the input as:
$$f = \sum_{i=0}^{m-1} f_i\, x^{ki} \quad \& \quad g = \sum_{i=0}^{m-1} g_i\, x^{ki},$$

where, $k := \lfloor \sqrt{\ell/2} \rfloor$, $m := \lceil \ell/k \rceil$,
f_i, g_i are polynomials of deg $< k$. $\ll \ell/2$

- Idea: Consider the polynomials over E:
$$F(y,x) := \sum_i f_i(y)\cdot x^{ki},$$
$$G(y,x) := \sum_i g_i(y)\cdot x^{ki}$$ & multiply them.

Fact: Let $F(y,x)\cdot G(y,x) = H(y,x)$ in $E[x]$. It is easy to recover $h(x)$ from H.

Pf: • The degree of H wrt y is much smaller than ℓ. $\square$

– Since, E has ω (a 2^n-th root of unity) & $2 \notin zd(E)$, we can compute H using the DFT algorithm.

▷ Relevant computation of $DFT[\omega]$, via recursion, requires $O(\sqrt{\ell}\cdot \lg \ell)$ E-operations

$\rightsquigarrow \sqrt{\ell}\cdot O(\sqrt{\ell}\cdot \lg\ell) = O(\ell \cdot \lg \ell)$ R-operations.

▷ Relevant multiplication in E is like $m = \lceil \ell/k \rceil$ instances of deg$<k$ multiplication over R.

– This gives the recurrence:

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

$\Rightarrow T(\ell) = O(\ell\cdot\lg\ell\cdot\lg\lg\ell)$ R-operations.

- What if R has char $= 2$?

- We could take $\ell = 3^n$, devise a virtual ℓ-th root of unity w & apply $DFT[w]$.

(Schönhage-Strassen'71)-based idea;

Theorem: In all cases, $h = f \cdot g$ in $R[x]$ can be computed in $O(\ell \cdot \lg \ell \cdot \lg\lg \ell)$ R-operations.