~~def The product of ... is $a \cdot b := (c_k)$,~~
~~where $c_k := a_k b_k$.~~

~~def~~ The convolution of $(a_i)_i, (b_i)_i \in \prod_{i \in \mathbb{Z}/n\mathbb{Z}} R$ is $\{a * b\} := (c_i)_i \in \prod_{i \in \mathbb{Z}/n\mathbb{Z}} R$,

where $c_k := \sum_{\substack{i,j \in \mathbb{Z}/n\mathbb{Z}: \\ i+j=k}} a_i b_j$.

Lemma 1.1.6 Assume that ζ_n lies in the center of R (commutes with every $x \in R$).

a) $\mathcal{F}_{\zeta_n}(a * b) = \mathcal{F}_{\zeta_n}(a) \cdot \mathcal{F}_{\zeta_n}(b)$

b) $n \cdot \mathcal{F}_{\zeta_n}(a \cdot b) = \{\mathcal{F}_{\zeta_n}(a) * \mathcal{F}_{\zeta_n}(b)\}$.

Pf a) Let $c = a * b$.

$$\underbrace{\sum_k c_k \zeta_n^{kl}}_{LHS} = \sum_{i,j} a_i b_j \zeta_n^{(i+j)l} = \underbrace{\left(\sum_i a_i \zeta_n^{il}\right)\left(\sum_j b_j \zeta_n^{jl}\right)}_{RHS}.$$

b)

$$RHS = \sum_{\substack{r,s: \\ r+s=l}} \left(\sum_i a_i \zeta_n^{ir}\right)\left(\sum_j b_j \zeta_n^{js}\right)$$

$$= \sum_{i,j} a_i b_j \sum_{\substack{r,s: \\ r+s=l}} \zeta_n^{ir+js}$$

$$= \sum_{i,j} a_i b_j \underbrace{\sum_r \underbrace{\zeta_n^{ir+j(l-r)}}_{\zeta_n^{jl+(i-j)r}}}_{= \begin{cases} n \cdot \zeta_n^{il} & \text{if } i=j \ (\text{mod } n) \\ 0 & \text{else} \end{cases}}$$

$$= n \cdot \sum_i a_i b_i \zeta_n^{il} = RHS$$

1.2. Multiplying polynomials

Thm 1.2.1 Let $r \geq 2$, and n large. Let $k = \lceil \log_r n \rceil$ (so $r^k \geq n$), $t = r^{k+1}$. If r is invertible in R and R contains a root $\zeta = \zeta_t$ of $\Phi_t(X)$, then (given $\frac{1}{r}$, ζ) we can multiply any two pol. $f, g \in R[X]$ of degrees $< n$ in time $O_r(n \log n)$ on an $O(\log n)$-bit RAM.

Alg Let $f(X) = \sum_{i=0}^{t-1} a_i X^i$, $g(X) = \sum_{i=0}^{t-1} b_i X^i$.

Write $a = (a_i)_i \in \prod_{i \in \mathbb{Z}/t\mathbb{Z}} R$, $b = (b_i)_i$

1) Use radix r Cooley–Tukey to compute the FT

$$\hat{a} := \mathcal{F}_\zeta(a), \quad \hat{b} := \mathcal{F}_\zeta(b).$$

2) Compute $\hat{a} \cdot \hat{b}$:

For each $j \in \mathbb{Z}/t\mathbb{Z}$, compute $\hat{a}_j \cdot \hat{b}_j$.

3) Use C-T to compute

$$c := \mathcal{F}_\zeta(\hat{a} \cdot \hat{b}).$$

4) Return $\underbrace{\frac{1}{t}}_{\frac{1}{r^{k+1}}} \cdot \sum_{i=0}^{t-1} c_i X^i.$

Pf Correctness

$$c = \mathcal{F}(\hat{a} \cdot \hat{b}) = \mathcal{F}(\mathcal{F}(a) \cdot \mathcal{F}(b))$$

$$= \mathcal{F}(\mathcal{F}(a * b))$$

Lemma 1.1.6 a)

$$= t \cdot (a * b)$$

Lemma 1.1.2

For $0 \le k < t$,

$$\Rightarrow \frac{1}{t} \cdot c_k = (a * b)_k = \sum_{\substack{i,j \in \mathbb{Z}/t\mathbb{Z}: \\ i+j=k}} a_i b_j = \sum_{\substack{0 \le i,j < t: \\ i+j \equiv k \bmod t}} a_i b_j$$

$$= \sum_{\substack{0 \le i,j < t: \\ i+j=k}} a_i b_j .$$

$a_i, b_i = 0$
unless $0 \le i < n \le r^k < \frac{1}{2} \cdot r^{k+1} = \frac{1}{2} \cdot t$

$$\Rightarrow \frac{1}{t} \cdot \sum_{k=0}^{t-1} c_k x^k = \sum_{i,j} a_i b_j x^{i+j} = f(x) \cdot g(x).$$

Running time

Step 1) $\mathcal{O}_r(n \log n)$
2) $\mathcal{O}(n)$
3) $\mathcal{O}_r(n \log n)$
4) $\mathcal{O}(n)$.

$\square$

How to get rid of the assumption that Φ_t has a root in R?

Idea 1 Work in the ring $S = R[Y]/\Phi_t(Y)$.

$\rightsquigarrow$ $\zeta_t := [Y] \in S$ is a root of Φ_t.

Problem: Adding two el. of S takes time $\Theta(\deg(\Phi_t)) = \Theta(n)$.

In C-T, we do $\Theta(n \log n)$ such additions.

$\rightsquigarrow$ total time $\Theta(n^2 \log n)$, worse than schoolbook multiplication!

Thm 1.2.2 (Schönhage-Strassen)

Let r be a prime number. For large n, ~~you can~~ ~~multiply~~ given two pol. $f, g \in R[X]$ of degree $< n$, you can compute $r^{k+2} \cdot fg$ in time $\mathcal{O}(n \log n \log\log n)$ on an $\mathcal{O}(\log n)$-bit RAM, where $k = \lceil \frac{1}{2} \log_r n \rceil$.

~~Cor 1.2.3~~ Cor 1.3 You can compute $f\cdot g$ in time $O(n \log n \log\log n)$.

[Clear if r is invertible in R (and its inverse known).]

Pf Apply the Thm with $r=2,3$.

$\rightsquigarrow$ can compute $2^{r_2+2}\cdot fg$, $3^{r_3+2}\cdot fg$

for $r_2=\lceil \frac{1}{2}\log_2 n\rceil$, $r_3=\lceil \frac{1}{2}\log_3 n\rceil$.

Since 2^{k_2+2}, 3^{k_3+3} are relatively prime, there exist $u, v\in \mathbb{Z}$ such that

$$1=u\cdot 2^{k_2+2}+v\cdot 3^{k_3+2}$$

(and $0\le u< 3^{k_3+2}=3^{\frac{1}{2}\log_3 n+O(1)}=O(\sqrt{n})$).

You can find u,v by trying all $0\le u<3^{k_3+2}$ in time $O(\sqrt{n})$. (Or use the extended Euclidean algorithm.)

Then, $f\cdot g= u\cdot(2^{r_2+2}\cdot fg)+v\cdot(3^{r_3+2}\cdot fg)$.

$\square$

RETURN

Alg for Thm 1.2.2

If $k \leq 3$, use the schoolbook algorithm.
Otherwise:

Let $m = r^k$, $t = r^{k+2}$

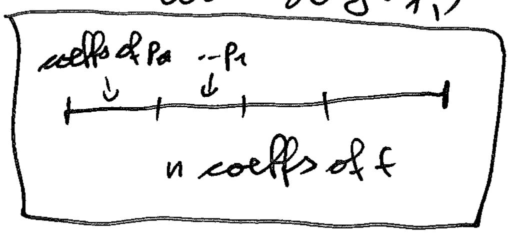
$$m = r^k \;(= \theta_r(\sqrt{n})), \qquad t = r^{k+2} \;(= \theta_r(\sqrt{n}))$$

1) Write $f(X) = \sum_{i=0}^{t-1} p_i(X) \cdot X^{i \cdot m}$

with $\deg(p_i) < m$ (possible because $m \cdot t = r^{2k+2} > r^{2k} \geq n$).

Similarly, $g(X) = \sum_{i=0}^{t-1} q_i(X) \cdot X^{i \cdot m}$

with $\deg(q_i) < m$.



Let $S = \mathbf{R}[Y]/\Phi_t(Y)$ and let $\zeta := \zeta_t := [Y] \in S$.

We have $\Phi_t(Y) = \frac{Y^{r^{k+2}}-1}{Y^{r^{k+1}}-1} = 1 + Y^{r^{k+1}} + \ldots + Y^{(r-1)r^{k+1}}$.

Let $a = (a_i)_i \in \prod_{i \in \mathbb{Z}/t\mathbb{Z}} S$ with $a_i = \underbrace{[p_i(Y)]}_{p_i(Y) \bmod \Phi_t(Y)} \in S$,

$b = (b_i)_i$ $\qquad b_i = [q_i(Y)] \in S$.

(Note that $\deg(p_i), \deg(q_i) < m = r^k < (r-1)r^{k+1} = \deg(\Phi_t)$, so p_i, q_i are already reduced mod Φ_t.)

2) Use radix r Cooley-Tukey to compute the FT

$$\hat{a} = \mathcal{F}_\zeta(a) \in \prod_j S, \qquad \hat{b} = \mathcal{F}_\zeta(b) \in \prod_j S.$$

In the C-T alg., we have to add elements of S and multiply el. of S by powers of $\zeta = [Y] \in S$. We do this by working in the ring

$$S' = \mathbf{R}[Y]/(Y^t - 1)$$

and only reducing modulo $\Phi_t(Y)$ (which divides $Y^t - 1$) in the end.

Addition in S': $\underbrace{\sum_{d=0}^{t-1} u_d Y^d}_{\text{red. mod } Y^t-1} + \underbrace{\sum_{d=0}^{t-1} v_d Y^d}_{\dots} = \underbrace{\sum_{d=0}^{t-1} (u_d + v_d) Y^d}_{\dots}$.

Mult. by powers of Y: $\underbrace{\left(\sum_{d=0}^{t-1} u_d Y^d\right)}_{\dots} \cdot Y^l \equiv \sum_{d=0}^{t-1} u_d Y^{d+l}$

$$\equiv \underbrace{\sum_{d=0}^{t-1} u_d Y^{(d+l) \bmod t}}_{\text{reduced mod } Y^t-1} \mod Y^t - 1.$$

3) ~~Compute $(\hat{a}\cdot\hat{b})$~~

For all $j \in \mathbb{Z}/t\mathbb{Z}$, compute $\hat{a}_j \cdot \hat{b}_j \in S$ as follows:

Let $\hat{a}_j = [A_j] \in S$, $\hat{b}_j = [B_j] \in S$

with $A_j, B_j \in R[Y]$, $\deg(A_j), \deg(B_j) < \deg(\Phi_t) = (r-1)\cdot r^{k+1} < r^{k+2} \underset{k \geq 4}{\leq} r^{2k-2} < n$.

a) Recursively apply the mult. alg. to compute $A_j(Y)\cdot B_j(Y) \in R[Y]$.

b) Reduce $A_j(Y)\cdot B_j(Y)$ mod $\Phi_t(Y) = 1 + Y^{r^{k+1}} + \dots + Y^{(r-1)r^{k+1}}$ using the schoolbook algorithm.

4) Use Cooley-Tukey (like before) to compute the FT

$$c = \mathcal{F}_\zeta(\hat{a}\cdot\hat{b}) \in \prod_{i\in\mathbb{Z}/t\mathbb{Z}} S.$$

5) Let $c_i = [C_i] \in S$ with $C_i \in R[Y]$, $\deg(C_i) < \deg(\Phi_t)$.

Return $\displaystyle\sum_{i=0}^{t-1} C_i(X)\cdot X^{im}$ $\quad (= t\cdot f(X)\cdot g(X))$.