Lec26B Review

April 15, 2021 12:17 PM

Complexity of Classical Algorithms for $\mathbb{Z}$ and $F[x]$.

Michael Monagan

Let $a, b \in \mathbb{Z}$, B be a constant, $0 < a < B^n$, $0 < b < B^m$, $n \geq m$.
In the tables EEA = Extended Euclidean Algorithm.

$a \pm b$	$O(n)$
$a \times b$	$O(nm)$
$a \div b$	$O((n-m+1)m)$
$\gcd(a,b)$	$O(nm)$
$\mathrm{EEA}(a,b)$	$O(nm)$

Table 1: Complexity for integer operations

$O((n-1+1)\cdot 1)$
$= O(n)$

Let f, g be non-zero polynomials in $F[x]$, F a field.
Let $n = \deg f$, $m = \deg g$, $n \geq m$, $\alpha \in F$.

$f \pm g$	$O(n)$
$f \times g$	$O(nm)$
$f \div g$	$O((n-m+1)m)$
$\gcd(f,g)$	$O(nm)$
$\mathrm{EEA}(f,g)$	$O(nm)$
$f(\alpha)$	$O(n)$ Horner's rule.
interpolate f	$O(n^2)$

Table 2: Number of arithmetic operations in F for polynomials

Modular Determinant Algorithm.

Input: A an $n \times n$ matric of polynomials $\mathbb{Z}[x]$.
Ouput: $\det(A) \in \mathbb{Z}[x]$.
$\deg(A_{ij}) \leq d$
$\|A_{ij}\|_\infty < B^m$ where $B = 2^{64}$.

Homomorphism Diagram.

$$
\begin{tikzcd}
\text{Input } A \in \mathbb{Z}[x]^{n\times n} \arrow[rr] \arrow[d, "\phi_{p_i}"'] & & D = \det(A) \in \mathbb{Z}[x] \\
A_i \in \mathbb{Z}_{p_i}[x]^{n\times n} \arrow[d, "\phi_{x=\alpha_{ij}}"'] & & D_i = \det(A_i) \in \mathbb{Z}_{p_i}[x] \arrow[u, "\text{CRT: } \le (nd+1)\cdot O(M^2)"'] \\
A_{ij} \in \mathbb{Z}_{p_i}^{n\times n} \arrow[rr, "\text{Gaussian Elim}", "M\cdot(nd+1)\,O(n^3)"'] & & D_{ij} = \det(A_{ij}) \in \mathbb{Z}_{p_i} \arrow[u, "\text{Interpolate } O((nd+1)^2)\cdot M"']
\end{tikzcd}
$$

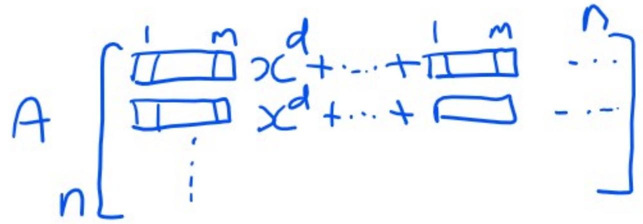
$\prod p_i > 2\|D\|_\infty \le ?$

$\le n^2(d+1)M \cdot O(m)$
$= O(dmn^2M).$

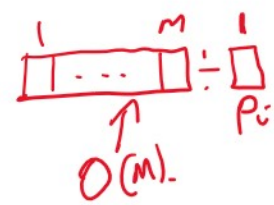
Horner's rule

$n^2M(nd+1)O(d)$

$\phi_{x=\alpha_{ij}} = 0,1,2,\dots,\deg(D) \le nd$



$\deg A_{ij} \le d$
$|\text{coeffs}| < B^m$
$p_i > B.$



Let M be the # of primes.

Are there any conditions on the primes?

$p_i \nmid lc(A)$

Are there any conditions on the eval points α_{ij}'s?

Are there any conditions on the input?

C.Z. $\gcd(a, a') = 1.$

Gcd $\quad \mathbb{Z}_p[t][x] \quad \underline{\mathbb{Z}}[x]$

$\phi_{t=\alpha}. \qquad lc(A)(\alpha) \neq 0.$

$$A = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix} \qquad \det(A) = \underline{a_{11}a_{22}} - \underline{a_{12}a_{21}}$$

2 terms 2 factors.

$$A = \begin{bmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{bmatrix} \qquad \begin{aligned} \det(A) = {} & a_{11}a_{22}a_{33} - a_{11}a_{23}a_{32} \\ & - a_{21}a_{12}a_{33} + a_{21}a_{13}a_{32} \\ & + a_{31}a_{12}a_{23} - a_{31}a_{13}a_{22}. \end{aligned}$$

6 terms 3 factors

$n \times n \qquad n!$ terms $\quad n$ factors.

$$\underline{\| a_{31} a_{12} \|_\infty} \leq \| a_{31} \|_\infty \| a_{12} \|_\infty \cdot \underline{\min}(\underline{\#\text{terms } a_{31}, a_{12}})$$
$$< B^m \cdot B^m \cdot (d+1)$$

$$\|(\underline{a_{31} \; a_{12}})\underline{a_{23}}\|_\infty \leq \underline{\|a_{31}a_{12}\|_\infty} \cdot \underline{\|a_{23}\|_\infty} \cdot \underline{\min(\overset{2d+1}{\#(a_{31}a_{12})}, \overset{d+1}{\#a_{23}})}$$
$$< B^{2m}(d+1) \; B^m \; (d+1) = B^{\underline{3}m}(d+1)^2$$

$$\| \prod_{k=1}^{n} a_{ij} \|_\infty < B^{nm} \cdot (d+1)^{n-1}.$$

$$\| \det(A) \|_\infty < n! \; \underline{B^{nm}(d+1)^{n-1}}$$

$p_i > B \qquad M = \#\text{primes} \quad \left\lceil \log_B (n! \underline{B^{nm}} (d+1)^{n-1} \cdot \overset{\pm \text{ coefficients.}}{2}) \right\rceil$

$$= \lceil nm + \log_B n! + (n-1)\log_B(d+1) + \log_B 2 \rceil$$

$$\underline{n!} \leq n^n$$
$$\log_B n! \leq n \log_B n.$$

$$< nm + n\underbrace{\log_B n}_{\ll 1} + (\underline{n-1})\underbrace{\log_B(d+1)}_{\ll 1} + \underbrace{\log_B 2}_{\ll 1.}$$

$$< nm + n + n + 1$$
$$= nm + 2n + 1 \in \underline{O(nm)}.$$