Lec6A Complexity of algorithms in F[x]

January 27, 2021 10:04 PM

Assignment #1 Solutions posted (15 minutes ago)
Assignment #2 posted — due Mon. Feb 8th.

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

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

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

Table 2: Number of arithmetic operations in F for polynomials

2.5 Univariate Polynomial Rings.

Let $a = a_n x^n + \cdots + a_0$, $b = b_m x^m + \cdots + b_0$ with $n \geq m \geq 0$
and $a_i, b_m \in F$ a field.

$a+b$ and $a-b$ cost $O(\max(n,m)) = O(n)$.
$a \times b$ costs $(n+1)(m+1)$ mults in F $= O(nm+n+m+1) = O(nm)$.
$a \div b$ does $\leq (n-m+1)\cdot m$ mults in F —

gcd(a,b) does $\le n \cdot m$ mults in F is $O(nm)$

Proof ($\div$).

$n \ge m$

$$q_1 \to \frac{a_n}{b_m}\cdot x^{n-m} + q_2 + \cdots \quad q_0 \cdot 1$$

one $\div$ in F

$$b = b_m x^m + \cdots + b_0 \;\big)\; a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0 = a \leftarrow r$$

$$q_1 \cdot b = q_1 [b_m x^m + b_{m-1}x^{m-1} + \cdots + b_0]$$

$$- \quad = a_n x^n + \square \cdot x^{n-1} + \cdots + \square$$

$$= 0 \cdot x^n + \square x^{n-1} + \cdots + a_0 \leftarrow r$$

$q_1 \cdot b$ can be done using $\le m$ mults.

$-$ does $\le m$ subs.

Total # mults in F $\le (\overbrace{n-m+1}^{\text{max \# of division steps.}})m$

CASE $n=m$: $\le m. \in O(m)$.

E.A. CASE $n=m+1$: $\le (m+1-m+1)m = 2m. \in O(m)$

$a = b q$: $\le (2m-m+1)m = (m+1)m \in O(m^2)$.

(deg $2m$, deg m, deg m)

Proof (Euc. Alg.) Assuming $n \ge m$.

deg.		
n	$r_0 = a_n x^n + \cdots$	$\Big\} \leftarrow \le (n-m+1)\underline{m}$ mults in F
m	$r_1 = b_m x^m + \cdots$	
$m-1$	$r_2 = \square \cdot x^{m-1} + \cdots$	$\} \; 2(m-1)$
$m-2$	$r_3 = \square \cdot x^{m-2} + \cdots$	$\} \; 2(m-2)$
$\vdots$		$\vdots$
	$r_m = \square \cdot x^1 + \square$	
0	$r_{m+1} = \square \cdot x^0$	$2 \cdot 0$

normal degree sequence. gcd $= 1$.

$$\text{Total \# mults is } \underline{(n-m+1)m} + \sum_{k=0}^{m-1} 2k = 2\,\frac{m(m-1)}{2} = m^2 - m$$

$$= nm - m^2 + m + m^2 - m$$

$$= nm.$$

Is nm representative of the time the EA takes? **No**

This does not account for the cost of arithmetic in F.

Consider. $\displaystyle\int \frac{x}{(x-1)(x^2+2)}\,dx = \int\left(\frac{A}{(x-1)} + \frac{Bx+C}{(x^2+2)}\right)dx$

$$\frac{A}{x-1} + \frac{Bx+C}{x^2+2} = \frac{x}{(x-1)(x^2+2)} \Rightarrow \overset{\sigma(x)\,a(x)\;+\;\tau(x)\,\cdot\,b(x)\;=\;c(x)}{A(x^2+2)+(Bx+C)(x-1) = x}$$

$$\{A+B=0,\ C-B=1,\ 2A-C=0\} \Rightarrow \underline{(A+B)}x^2 + \underline{(C-B)}x + \underline{(2A-C)} = \underline{x}$$

$A = 1/3 \quad B = -1/3 \quad C = 2/3.$

This equation $\sigma a + \tau b = c$ is a polynomial diophantine equation.

Theorem 2.6 Let F be a field and $a, b, c \in F[x]$, $a \neq 0$, $b \neq 0$. Let $g = \gcd(a,b)$. If $g | c$ there exist ($\uparrow$ gives existence.) unique polynomials $\sigma, \tau \in F[x]$ satisfying

(i) $\sigma a + \tau b = c$ ($\leftarrow$ imposes uniqueness.)

(ii) $\sigma = 0$ or $\deg \sigma < \deg\left(\frac{b}{g}\right) = \deg b - \deg g$.

Proof (existence). From the EEA, $\exists\, s, t, g \in F[x]$ such that

$$s \cdot a + t \cdot b = g = \gcd(a,b). \quad (1)$$

$g | c \Rightarrow c = d \cdot g$ for some $d \in F[x]$.

$d \times (1)$: $\quad \underline{(ds)}\,\underline{a} + \underline{(dt)}\,\underline{b} = d \cdot g = \underline{c} \qquad ds \div \frac{b}{g}$

$/g$: $\quad (ds) \cdot \frac{a}{g} + (dt)\frac{b}{g} = d. \qquad \Rightarrow ds = \frac{b}{g} q + \sigma$

$$\left(\frac{b}{g} \cdot q + \sigma\right)\frac{a}{g} + dt\,\frac{b}{g} = d \qquad \deg \sigma < \deg \frac{b}{g} \text{ or } \sigma = 0.$$

$$\sigma \frac{a}{g} + \left(q\frac{a}{g} + dt\right)\frac{b}{g} = d.$$

$\times g$. $\quad \sigma a + \underbrace{\left(q\frac{a}{g} + dt\right)}_{\tau} b = c$

Proof of uniqueness:

Suppose (1) $\sigma_1 a + \tau_1 b = c$ with $\deg \sigma_1 < \deg(\frac{b}{g})$ or $\sigma_1 = 0$

(2) $\sigma_2 a + \tau_2 b = c$ with $\deg \sigma_2 < \deg(b/g)$ or $\sigma_2 = 0$.

(1)−(2) $(\sigma_1 - \sigma_2)\frac{a}{g} = (\tau_2 - \tau_1)\frac{b}{g}$. $g = \gcd(a,b)$.

$F[x]$

$\Rightarrow \frac{b}{g} \mid \sigma_1 - \sigma_2$ because $\gcd(\frac{a}{g}, \frac{b}{g}) = 1$

$\deg(\sigma_1 - \sigma_2) < \deg(\frac{b}{g})$

$\Rightarrow \sigma_1 - \sigma_2 = 0. \Rightarrow \sigma_1 = \sigma_2.$

$\Rightarrow 0 = (\tau_2 - \tau_1)\frac{b}{g} \Rightarrow \tau_2 - \tau_1 = 0 \Rightarrow \tau_2 = \tau_1.$

no z.d.s

Suppose $a \cdot 10 = b \cdot 21$ in $\mathbb{Z}$

$\Rightarrow 21 \mid 10 \cdot a$

$\Rightarrow 21 \mid a.$ since $\gcd(21, 10) = 1.$