Computational Algebra: List 4

Manuel Ledo Sánchez

$\boxed{1}$ Let R be a commutative ring with $1 \in R$, $f, g \in R[x,y]$. Assume f and g have degrees bounded by m in y and by n in x. Let $h = f \cdot g$.

a) Using classical univariate polynomial multiplication, and viewing $R[x,y]$ as $R[y][x]$ bound the number of arithmetic operations in R to compute h.

If we view $R[x,y]$ as $R[y][x]$, then $f, g \in R[y][x]$ under the stated conditions are of the form $f = \sum_{i=0}^{n} f_i x^i$, $g = \sum_{j=0}^{n} g_j x^j$ where f_i's, g_i's $\in R[y]$.

The naive multiplication of algorithm implies $O(n^2)$ operations in $R[y]$ of the form $f_i \cdot g_j$ where $f_i = \sum_{i=0}^{m} a_i y_i$, $g_j = \sum_{j=0}^{m} b_j y_j$ a_i's, b_j's $\in R$ and again we know that $f_i \cdot g_j$ is $O(m^2)$ in R. Therefore, for $f, g \in R[y][x]$ $f \cdot g$ arithmetic operations is $O(n^2 m^2)$. Observe that $+$ is bounded by $\cdot$.

b) Use Karatsuba's algorithm to bound the # of operations in R to compute h.

(*) We know that given $f, g \in R[x]$ with degrees less than $n = 2^k$ the number of ring operations is bounded by $O(9 n^{\log 3})$

Suppose $R = R[y]$ and take $\tilde{n} = 2^{\lceil \log(n) \rceil}$, for computing h, by (*) we need less than $9 \cdot (2^{\lceil \log_2(n) \rceil})^{\log 3} \leq 27 \cdot 3^{\log(n)}$ arithmetic operations in $R[y]$.

Moreover, each of those operations corresponds with a multiplication of two polynomials over R with coefficients in y which degrees are bounded by m. Therefore, by an analogous argument, for each of the latter multiplications, we have that the # of arith. op in R is bounded by $27 \cdot 3^{\log(m)}$ which in terms of big O notation ~~can be~~ is

$$O(3^{\log(n) + \log(m)})$$

c) Generalize parts a) and b) for an arbitrary number of variables. Suppose $f, g \in R[x_1, \dots x_n]$ in $R[x_i]$ the deg bounded by m_i

We proceed in both cases by induction.

a) $\boxed{O\left(\prod_{i=1}^{n} m_i^{\,2}\right)}$ $\checkmark$

b) $\boxed{O\left(3^{\sum_{i=0}^{n} \log_2(m_i)}\right)}$

Base case $n=2$ $\checkmark$

General case Assume $n-1$ works

The case $f, g \in R[x_1 \dots x_n]$ is $g, f \in R[x_1 \dots x_{n-1}][x_n]$ and the proof is the same as in a) case 2 $\longrightarrow$ Idem.

Base case $n=2$ $\checkmark$

General case Assume $n-1$ works

[8] Prove that for a prime power q and $m \in \mathbb{N}$, a finite field contains a primitive root of the unity if and only if $m \mid q-1$.

Lemma: $m \in \mathbb{N}$ and $\mathbb{F}_p$ field with characteristic p. Then if $p \nmid m$ ($\mathcal{U}^{(m)}$ the set of mth roots of the unity), then $\mathcal{U}^{(m)}$ is a cyclic group of order m with respect to $\cdot$ in the splitting field of $x^m - 1$ over $\mathbb{F}_p$. (classic result) only sketch of the proof

Sketch: 1) Case $m=1$ trivial

2) $m \geq 2$ $x^m - 1$ and mx^{m-1} do not share common roots, and therefore $x^m = 1$ does not have multiple roots, and hence m elements

3) group under $\cdot$; $\alpha, \beta \in \mathcal{U}^{(m)}$ $(\alpha\beta^{-1})^m = \alpha^m (\beta^m)^{-1} = 1 \Rightarrow \alpha\beta^{-1} \in \mathcal{U}^{(m)}$

4) Proving that $\mathcal{U}^{(m)}$ is cyclic

Then; the proof of the excercise is as follows:

$\Leftarrow$] $m \mid q-1 \Rightarrow m \nmid q \Rightarrow$ $\mathcal{U}^{(m)}$ cyclic group under multiplication by the lemma above and so $\mathcal{U}^{(m)} = \langle x \rangle$ with x of order m $\Rightarrow x^m \equiv 1 \bmod (q) \Rightarrow$ $x^m - 1 \equiv 0 \bmod (q)$ $\Rightarrow$ x mth root of the unity in $\mathbb{F}_q$ ~~...~~ ~~...~~ (✱)

$\Rightarrow$] $\exists x \in \mathbb{F}_q$ s.t. $x^m \equiv 1 \bmod (q)$, since primitive $\langle x \rangle$ order is m.

$\langle x \rangle \leq \mathbb{F}_q^*$ so $[\langle x \rangle : \mathbb{F}_q^*] = \dfrac{|\mathbb{F}_q^*|}{|\langle x \rangle|}$, and in particular then $|\langle x \rangle| \mid |\mathbb{F}_q^*| \Rightarrow m \mid q-1$. ☐

(✱) x mth root of the unity in $\mathbb{F}_q$ $\forall t$ $t \mid m$, $\frac{m}{t} < m$ and so since $\langle x \rangle$ cyclic of order m $x^{m/t} \not\equiv 1 \bmod (q)$ and since $\mathbb{F}_q$ is a field $x^{m/t} - 1 \not\equiv 0 \bmod (q)$ and $x^{m/t} - 1 \in \mathbb{F}_q$ it is not a zero divisor.

[5] R be a ring, $m \in \mathbb{Z}_{>0}$ and $w \in R$ a primitive mth root of the unity

a) Show that w^{-1} is also a primitive mth root of the unity

b) m even $\Rightarrow w^2$ is a $m/2$th root of the unity. m odd $\Rightarrow w^2$ mth root of the unity

c) $k \in \mathbb{Z}$ $d = m/\gcd(m,k)$. Show that w^k is a primitive dth root of the unity

Observation c) $\Rightarrow$ a) and b)

$k = -1 \Rightarrow d = m/\gcd(m,-1) \rightarrow w^{-1}$ mth root of the unity

$k = 2 \Rightarrow d = m/\gcd(m,2)$ → even $d = m/2$ $m/2$th root of the unity; → odd $d = m$ mth root of the unity

c) Let $k = m \cdot \gcd(m,k) \Rightarrow (w^k)^d = (w^m)^m = 1^m = 1 \Rightarrow w^k$ is a dth root of the unity. $d = m/\gcd(m,k)$ and so since m is a unit d is so. ~~and~~ the latter fact plus noticing ~~...~~ that $\forall t < d$ ~~...~~ ~~since~~ $tk = qm + r$ with $0 < r < m$ since $tk \nmid m$, and hence $(w^k)^t - 1 = (w^m)^q w^r - 1 = w^r - 1$ which is not a zero divisor since $0 < r < m$ and ~~...~~ w is an mth root of the unity prove that w^k is a dth root of the unity.