Polynomial Multiplication Algorithms

September 15, 2021 9:42 PM

Let f, g be non-zero polynomials in $R[x_1, \dots, x_n]$.
Let $f = a_1 \cdot X_1 + a_2 X_2 + \cdots + a_{\#f} X_{\#f}$ and $g = b_1 Y_1 + b_2 Y_2 + \cdots + b_{\#g} Y_{\#g}$.
Where $a_i, b_i \in R \setminus \{0\}$ and X_i, Y_i are monomials in $x_1, x_2, \dots, x_n$. and
$X_1 > X_2 > \cdots > X_{\#f}$ and $Y_1 > Y_2 > \cdots > Y_{\#g}$ in a monomial order.
We'll also write $f = f_1 + f_2 + \cdots + f_{\#f}$.

How can we compute $h = fxg = c_1 Z_1 + c_2 Z_2 + \cdots + c_{\#h} Z_{\#h}$ with $c_i \in R \setminus \{0\}$ and $Z_1 > Z_2 > \cdots > Z_{\#h}$.

A classical algorithm does $\#f \cdot \#g$ coeff. mults and mon. mults. and ??? monomial comparisons.

$$h = fxg = (((f_1 g + f_2 g) + f_3 g) + f_4 g + \cdots$$

MERGE

$\Rightarrow$ add using merging $\Rightarrow$ #comps $\in (\#g + \#g - 1) + \cdots$

Univariate Dense: $f = \cdot x^m + \cdot x^{m-1} + \cdots + \cdot x$ (m terms.) $g = \cdot x^m + \cdots + \cdot x^2 + \cdot x$

$$f_1 \cdot g + f_2 \cdot g = (\cdot x^{2m} + \cdots + \cdot x^{m+1}) + (\cdot x^{2m-1} + \cdots \cdot x^m)$$
$$= \cdot x^{2m} + \cdots + \cdot x^m \quad (m+1 \text{ terms})$$
$$2m-1 \text{ comps.}$$
$$+ f_3 g$$

$$\#\text{comparisons} = (m + m - 1) + (m + 1 + m - 1) + (2m + 1) + \cdots + (2m - 1 + m - 1)$$
$$= \sum_{i=1}^{m-1} (m + i - 1) + m - 1 = \frac{5}{2}m^2 - \frac{9}{2}m + 2 \in O(m^2).$$

Sparse case $f = \cdot x^m + x^{m-1} + \cdots + x^1$, $g = \cdot y^l + \cdot y^{l-1} + \cdots + \cdot y^1$.

$fg = h = \cdot x^m y^l + \cdots + x^1 y^1$. $\quad 2l$ terms.

$$f_1 \cdot g + f_2 g = (\cdot x^m y^l + \cdot x^m y^{l-1} + \cdots + \cdot x^m y^1)(\cdot x^{m-1} y^l + \cdots + \cdot x \cdot y^2 + x^{m-1} y^1)$$

$$\#\text{comparisons} = (l + l - 2) + (2l + l - 2)(3l + l - 2) + \cdots$$

comparisons = $(\ell+\ell-2)+(2\ell+\ell-2)(3\ell+\ell-2)+\cdots$ + $f_3 g$
grlex.

$$= \sum_{i=1}^{m-1}(i\ell+\ell-2) = \ell\left(\tfrac{1}{2}m^2+\tfrac{1}{2}m-1\right)-2(m-1).$$

$$\in O(\ell m^2) = O(\#g\cdot\#f^2)$$

cubic.

Note: if $\#f > \#g$ e.g. $\#g=2$ we should interchange f & g.

Instead of $h = f_1 g + f_2 g + \cdots + f_{\#f}\cdot g$ we do

$h = g_1 f + g_2 f$ with one merge.

How do we fix x.? Use divide and conquer.

Let $k = \lfloor \frac{m}{2} \rfloor$ where $m = \#f$.

$$h = fxg = \underbrace{(f_1+f_2+\cdots+f_k)\cdot g}_{\le \frac{m\ell}{2}\text{ terms}} + \underbrace{(f_{k+1}+\cdots+f_m)\cdot g}_{\le \frac{m\ell}{2}\text{ terms}}.$$

↑ merge

$\le \frac{m\ell}{2}+\frac{m\ell}{2}-1 = m\ell-1$ comps.

Let $C(m,\ell)$ be the # of monomial comparisons. where $m=\#f$ and $\ell=\#g$. For $m=2^k$. $\quad \leftarrow$ (i), (ii)

$$C(m,\ell) = 2C(\tfrac{m}{2},\ell) + m\ell - 1 \quad \text{and} \quad C(1,\ell) = 0.$$

```
> rsolve( { C(m) = 2 C(m/2) + m*l - 1, C(1) = 0 } )
```

$$1\ C(m) \le 2C(m/2) + \frac{m\ell}{2}+\frac{m\ell}{2}-1 = m\ell-1$$

$$2\ C(m/2) \le 2^2 C(m/4) + 2\left(\frac{m\ell}{4}+\frac{m\ell}{4}-1\right) = m\ell-2$$

$$4\ C(m/4) \le 2^3 C(m/8) + 4\left(\frac{m\ell}{8}+\frac{m\ell}{8}-1\right) = m\ell-4$$

$$\vdots$$

$$\frac{m}{2}\ C(2) \le m\,C(1) + \frac{m}{2}(2\ell-1) = m\ell-\frac{m}{2}$$

$$m\,C(1) \le 0.$$

↙

$m\,C(1) \le 0.$

Adding $C(m) \le (ml-1)+(ml-2)+\cdots+(ml-\frac{m}{2})$

$= \log_2 m \; ml + m-1. \in O(ml \log m)$

Note we can $f \leftrightarrow g$.

Therefore $C(m,l) \in O(ml \log \min(m,l))$.

Division in $R[x_1,\ldots,x_n]$

Let $f,g \in R[x_1,\ldots,x_n]$. Test if $g|f$. If so output $q = f/g$ the quotient. In Maple divide(f,g,'q');

$$g \;\overline{)\; ((f - q_1 g) - q_2 g) - q_3 g \cdots} \qquad q_1+q_2+q_3+\cdots$$

$$f - q_1 g - q_2 g - \cdots - q_{\#q}\, g = f - q\cdot g$$

The $\div$ alg does $\#q$ divisions in R and $\#q(\#g-1)$ mults plus ?? monomial comps.

Univariate Dense: $O(\#g \cdot \#q)$ monomial comparisons.

Sparse Case: $O(\#g \cdot \#q^2)$ " " CUBIC.

Can we do $\div$ in $O(\#g\,\#q \log \#q)$ " " ?