# Complexity of Multiplication using Merging

October 23, 2023 1:45 PM

Let $R$ be an integral domain, $f, g$ be non-zero polynomials in $R[x_1, \ldots, x_n]$.

Let $f = a_1 \cdot X_1 + a_2 X_2 + \cdots + a_{\#f} \cdot X_{\#f}$ where $a_i, b_i \in R$ and
$g = b_1 Y_1 + b_2 Y_2 + \cdots + b_{\#g} \cdot Y_{\#g}$ $X_i, Y_i$ are monomials in $x_1, \ldots, x_n$.

and the terms in $f$ & $g$ are sorted in some monomial ordering $\succ$.

i.e. $X_1 > X_2 > X_3 > \cdots > X_{\#f}$ and $Y_1 > Y_2 > \cdots > Y_{\#g}$.

We'll also write $f = f_1 + f_2 + \cdots + f_{\#f}$ where $f_i = a_i \cdot X_i$.

How should we compute $h = f \cdot g = c_1 Z_1 + c_2 Z_2 + \cdots + c_{\#h} Z_{\#h}$ where $c_i \in R$ and $Z_1 > Z_2 > \cdots > Z_{\#h}$ ??

A classical multiplication algorithm does $\#f \cdot \#g$ coefficient mults and monomial mults PLUS ?? monomial comparisons.

$$h = f \times g = (\cdots((f_1 \cdot g \underset{\text{merge}}{+} f_2 g) + f_3 \cdot g) \cdots) + f_n g$$

Univariate Dense case:

$$f = a_m x^m + a_{m-1} x^{m-1} + \cdots + a_1 x^1 \in R[x].$$
$$g = b_m x^m + b_{m-1} x^{m-1} + \cdots + b_1 x^1.$$

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

$m+1$ terms.

$\#$ comparisons $\leq m + m - 1 = 2m - 1$.

The total # comparisons is

$$\overset{m+1}{\rightarrow}((\underbrace{f_1 g + f_2 g}_{m+m-1}) + f_3 g \overset{m}{\leftarrow}) \overset{m+2 \text{ terms.}}{\leftarrow} + f_4 g \cdots$$

$$m + m - 1 + (m+1+m-1) + (m+2+m-1) + \cdots + 2m-1 + m - 1.$$

\# additions

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

The # of coefficient mults is $m^2$ as is the # of monomial mults.

Good.

Sparse case: $f = x^m + x^{m-1} + \cdots + x^1$

$g = y^\ell + y^{\ell-1} + \cdots + y^1$

$h = fg = x^m y^\ell + \cdots + x^1 \cdot y^1$ has $m\ell$ terms in $h$.

$$f_1 g + f_2 g = x^m \cdot g + x^{m-1} \cdot g$$

using grlex >

$$= (x^m y^\ell + x^m y^{\ell-1} + \cdots + x^m y^1) + (\underbrace{x^{m-1} y^\ell + \cdots + x^{m-1} y^2 + x^{m-1} y}_{=2\ell \text{ terms}})$$

$$= x^m y^\ell + x^m y^{\ell-1} + x^{m-1} y^\ell + \cdots x^m y^1 + \text{copied.}$$

$\#$ monomial comparisons $= \ell + \ell - 2$.

$$(\underbrace{f_1 g + f_2 g}_{2\ell \text{ terms}}) + \underbrace{f_3}_{=x^{m-2}} g = (x^m y^\ell + \cdots + x^{m-1} y^1) + (\underbrace{x^{m-2} y^\ell + \cdots + x^{m-2} y^2 + x^{m-2} y}_{\ell \text{ terms}})$$

$\#$comparisons is $2\ell + \ell - 2$.

$$\text{Total \# comparisons} = (\ell + \ell - 2) + (2\ell + \ell - 2) + \cdots + ((m-1)\ell + \ell - 2)$$

$$= \sum_{i=1}^{m-1} i\ell + \ell - 2 = \frac{1}{2}\ell m^2 + \frac{1}{2}\ell m - 2m - \ell + 2$$

$\in O(\ell m^2)$ i.e. cubic !!

$\#$ coeff mults $m \cdot \ell = \#$ monomial mults.

Bad if $m = \#f$ is big.

If $\#f \gg \#g$ e.g. $\#g = 2$ we should switch $f \times g$ to $g \times f$.

Instead use $h = g \times f = g_1 f + g_2 f$.

one merge.

How can we "fix" multiplication?

$$(\cdots(\underbrace{((f_1 g + f_2 g) + f_3 g)}) + f_4 g) + \cdots +) f_n g$$

$$((\underbrace{(f_1 g + f_2 g)}_{=x^m} + \underbrace{(f_3 g + f_4 g)}_{k\ell \text{ terms}})) \quad ((\underbrace{(f_5 g + f_6 g) + (f_7 g + f_8 g)}_{(m-k)\ell \text{ terms}})) ?$$

$$h = f\cdot g = (\underbrace{\overbrace{f_1 g}^{x^m} + \overbrace{f_2 g + \cdots + f_k g}^{k\ell \text{ terms}}}) + (\overbrace{f_{k+1} g + \cdots + f_m g}^{(m-k)\ell \text{ terms}}).$$

Let $k = \lfloor \frac{m}{2} \rfloor$

$m = \#f$

recursively divied $\#f$ into two halves.

one big merge. $k\ell + (m-k)\ell - 2$ comps.

$\leq m\ell - 1$ comps.

Use $h = \left(\sum_{i=1}^{k} f_i\right) g + \left(\sum_{i=k+1}^{m} f_i\right) g$

Let $C(m,\ell)$ be the #monomial comparisons where $m = \#f$, $\ell = \#g$.

For $m = 2^k$. $C(m,\ell) = 2C(\frac{m}{2},\ell) + m\ell - 1$.

for $f_i \cdot g$: $C(1,\ell) = 0$.

> rsolve( { C(m) = 2C(m/2) + mℓ − 1, C(1)=0 }, C(m) );

$$\ell m \log_2 m - m + 1 \in O(\ell m \log_2 m).$$

$m = 2^k$

$$\begin{aligned}
2^0 C(m) &= \cancel{2C(m/2)} + \tfrac{m}{2}\ell + \tfrac{m}{2}\ell \,\boxed{-1} \\
\cancel{2C(m/2)} &= \cancel{2^2 C(m/4)} + 2\left(\tfrac{m}{4}\ell + \tfrac{m}{4}\ell - 1\right) = \tfrac{m}{2}\ell + \tfrac{m}{2}\ell \,\boxed{-2} \\
\cancel{2^2 C(m/4)} &= \cancel{2^3 C(m/8)} + 4\left(\tfrac{m}{8}\ell + \tfrac{m}{8}\ell - 1\right) = \tfrac{m}{2}\ell + \tfrac{m}{2}\ell \,\boxed{-4} \\
&\ \vdots \\
\cancel{\tfrac{m}{2} C(2)} &= \cancel{\tfrac{m}{2}} 2C(1) + \tfrac{m}{2}(\ell + \ell - 1) = \tfrac{m}{2}\ell + \tfrac{m}{2}\ell \,\boxed{-\tfrac{m}{2}} \\
+\ \cancel{m C(1)} &= 0
\end{aligned}$$

$k$ lots.

$2^k$

$$C(m) = k(m\ell) - (m-1) = m\ell \log_2 m - m + 1 \in O(m\ell \log m).$$

If $m > \ell$ we can interchang $f \times g = g \times f$ so that we can do $O(m\ell \min(\log m, \log \ell))$.

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

Let $f, g \in R[x_1, \ldots, x_n]$. Test if $g | f$ in $R[x_1, \ldots, x_n]$ with 0 remainder.

?

$q_1 + q_2 + q_3 + \cdots + q_{\#q}$

merge

remainder.

merge

?

$LT(g) \mid LT(f)$

$LT(g) \mid LT(f - q_1 g)$

$$\begin{array}{r} q_1 + q_2 + q_3 + \cdots + q_{\#q} \\ g \overline{\big)\, (\cdots((f - q_1 \cdot g) - q_2 \cdot g) - q_3 g - \cdots) - q_{\#q} \cdot g} \end{array}$$

$$f - \sum_{i=1}^{\#q} q_i g = f - q \cdot g.$$

In the worst case this does $O(\#g \, \#q^2)$ comparisons.

Can we make it $O(\#g \, \#q \log \#q)$ ?

Yes ① Yan's geobuckets (1997) $\rightarrow$ Singular comp. alg. system.

② Johson's heaps (1974) $\rightarrow$ in Altran & Maple.

Can we make it $O(\#g \cdot \#q \cdot \min(\log \#g, \log \#q))$

Yes ① Monagan & Pearce (2008) $\rightarrow$ in Maple.