Divide-and-Conquer: Polynomial Multiplication

Neil Rhodes

Department of Computer Science and Engineering
University of California, San Diego

Data Structures and Algorithms
Algorithmic Toolbox

Outline

Uses of multiplying polynomials

- Error-correcting codes
- Large-integer multiplication
- Generating functions
- Convolution in signal processing

Multiplying Polynomials

Example

$$\begin{aligned} A(x) &= 3x^2 + 2x + 5 \\ B(x) &= 5x^2 + x + 2 \\ A(x)B(x) &= 15x^4 + 13x^3 + 33x^2 + 9x + 10 \end{aligned}$$

Multiplying polynomials

Input: Two $n-1$ degree polynomials:

$a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \cdots + a_1 x + a_0$

$b_{n-1}x^{n-1} + b_{n-2}x^{n-2} + \cdots + b_1 x + b_0$

Output: The product polynomial:

$c_{2n-2}x^{2n-2} + c_{2n-3}x^{2n-3} + \cdots + c_1 x + c_0$

where:

$c_{2n-2} = a_{n-1}b_{n-1}$

$c_{2n-3} = a_{n-1}b_{n-2} + a_{n-2}b_{n-1}$

...

$c_2 = a_2 b_0 + a_1 b_1 + a_0 b_2$

$c_1 = a_1 b_0 + a_0 b_1$

$c_0 = a_0 b_0$

Multiplying Polynomials

Example

Input: $n = 3, A = (3, 2, 5), B = (5, 1, 2)$

$$
\begin{aligned}
A(x) &= 3x^2 + 2x + 5 \\
B(x) &= 5x^2 + x + 2 \\
A(x)B(x) &= 15x^4 + 13x^3 + 33x^2 + 9x + 10
\end{aligned}
$$

Output: $C = (15, 13, 33, 9, 10)$

Outline

MultPoly(A, B, n)

```
pair ← Array[n][n]
for i from 0 to n − 1:
  for j from 0 to n − 1:
    pair[i][j] ← A[i] ∗ B[j]
product ← Array[2n − 1]
for i from 0 to 2n − 1:
  product[i] ← 0
for i from 0 to n − 1:
  for j from 0 to n − 1:
    product[i + j] ← product[i + j] + pair[i][j]
return product
```

Multiplying Polynomials

Naïve Solution: $O(n^2)$

- Multiply all $a_i b_j$ pairs (n^2 multiplications)
- Sum needed pairs (n^2 additions)

Outline

1. Problem Overview
2. Naïve Algorithm
3. Naïve Divide and Conquer Algorithm
4. Faster Divide and Conquer

Multiplying Polynomials

- Let $A(x) = D_1(x)x^{\frac{n}{2}} + D_0(x)$ where
  $D_1(x) = a_{n-1}x^{\frac{n}{2}-1} + a_{n-2}x^{\frac{n}{2}-2} + \ldots + a_{\frac{n}{2}}$
  $D_0(x) = a_{\frac{n}{2}-1}x^{\frac{n}{2}-1} + a_{\frac{n}{2}-2}x^{\frac{n}{2}-2} + \ldots + a_0$
- Let $B(x) = E_1(x)x^{\frac{n}{2}} + E_0(x)$ where
  $E_1(x) = b_{n-1}x^{\frac{n}{2}-1} + b_{n-2}x^{\frac{n}{2}-2} + \ldots + b_{\frac{n}{2}}$
  $E_0(x) = b_{\frac{n}{2}-1}x^{\frac{n}{2}-1} + b_{\frac{n}{2}-2}x^{\frac{n}{2}-2} + \ldots + b_0$
- $AB = (D_1x^{\frac{n}{2}} + D_0)(E_1x^{\frac{n}{2}} + E_0)$
  $= (D_1E_1)x^n + (D_1E_0 + D_0E_1)x^{\frac{n}{2}} + D_0E_0$
- Calculate D_1E_1, D_1E_0, D_0E_1, and D_0E_0

Recurrence: $T(n) = 4T(\frac{n}{2}) + kn$.

Polynomial Mult: Divide & Conquer

$$A(x) = 4x^3 + 3x^2 + 2x + 1$$

$$B(x) = x^3 + 2x^2 + 3x + 4$$

$$D_1(x) = 4x + 3 \qquad D_0(x) = 2x + 1$$

$$E_1(x) = x + 2 \qquad E_0(x) = 3x + 4$$

$$D_1E_1 = 4x^2 + 11x + 6 \qquad D_1E_0 = 12x^2 + 25x + 12$$

$$D_0E_1 = 2x^2 + 5x + 2 \qquad D_0E_0 = 6x^2 + 11x + 4$$

$$\begin{aligned} AB = {} & (4x^2 + 11x + 6)x^4 + \\ & (12x^2 + 25x + 12 + 2x^2 + 5x + 2)x^2 + \\ & 6x^2 + 11x + 4 \\ = {} & 4x^6 + 11x^5 + 20x^4 + 30x^3 + 20x^2 + 11x + 4 \end{aligned}$$

Function $\texttt{Mult2}(A, B, n, a_l, b_l)$

$R =$ `array`$[0..2n-2]$

`if` $n = 1$:

  $R[0] = A[a_l] * B[b_l]$; `return` R

$R[0\,..\,n-2]$ = $\texttt{Mult2}(A, B, \frac{n}{2}, a_l, b_l)$

$R\,[n\,..\,2n-2]$ = $\texttt{Mult2}(A, B, \frac{n}{2}, a_l + \frac{n}{2}, b_l + \frac{n}{2})$

D_0E_1 = $\texttt{Mult2}(A, B, \frac{n}{2}, a_l, b_l + \frac{n}{2})$

D_1E_0 = $\texttt{Mult2}(A, B, \frac{n}{2}, a_l + \frac{n}{2}, b_l)$

$R[\frac{n}{2} \ldots n + \frac{n}{2} - 2]$ += $D_1E0 + D_0E_1$

`return` R

level		#	work
0	$\boxed{n}$	1	kn
1	$\boxed{n/2}\ \boxed{n/2}\ \boxed{n/2}\ \boxed{n/2}$	4	$4k\frac{n}{2} = k2n$
$\vdots$	$\vdots$	$\vdots$	$\vdots$
i	$\cdots\ \boxed{n/2^i}\ \cdots$	4^i	$4^i k \frac{n}{2^i} = k2^i n$
$\vdots$	$\vdots$	$\vdots$	$\vdots$
$\log_2 n$	$\boxed{1}\ \cdots\ \boxed{1}$	$4^{\log_2 n}$	$k4^{\log_2 n} = kn^2$

Total: $\sum_{i=0}^{\log_2 n} 4^i k \frac{n}{2^i} = \Theta(n^2)$

Outline

Karatsuba approach

$$
\begin{aligned}
A(x) &= a_1 x + a_0 \\
B(x) &= b_1 x + b_0 \\
C(x) &= a_1 b_1 x^2 + (a_1 b_0 + a_0 b_1)x + a_0 b_0
\end{aligned}
$$

Needs 4 multiplications

Rewrite as:

$$
\begin{aligned}
C(x) = &a_1 b_1 x^2 + \\
&((a_1 + a_0)(b_1 + b_0) - a_1 b_1 - a_0 b_0)x + \\
&a_0 b_0
\end{aligned}
$$

Needs 3 multiplications

Karatsuba Example

$$A(x) = 4x^3 + 3x^2 + 2x + 1$$

$$B(x) = x^3 + 2x^2 + 3x + 4$$

$$D_1(x) = 4x + 3 \qquad D_0(x) = 2x + 1$$

$$E_1(x) = x + 2 \qquad E_0(x) = 3x + 4$$

$$D_1E_1 = 4x^2 + 11x + 6 \qquad D_0E_0 = 6x^2 + 11x + 4$$

$$\begin{aligned}(D_1 + D_0)(E_1 + E_0) &= (6x + 4)(4x + 6)\\ &= 24x^2 + 52x + 24\end{aligned}$$

$$\begin{aligned}AB = {} & (4x^2 + 11x + 6)x^4 + \\ & (24x^2 + 52x + 24 - (4x^2 + 11x + 6) \\ & \qquad - (6x^2 + 11x + 4))x^2 + \\ & 6x^2 + 11x + 4 \\ = {} & 4x^6 + 11x^5 + 20x^4 + 30x^3 + 20x^2 + 11x + 4\end{aligned}$$

level		#	work
0	$\boxed{n}$	1	kn
1	$\boxed{n/2}\ \boxed{n/2}\ \boxed{n/2}$	3	$3k\frac{n}{2} = k\frac{3}{2}n$
$\vdots$	$\vdots$	$\vdots$	$\vdots$
i	$\cdots \boxed{n/2^i} \cdots$	3^i	$3^i k\frac{n}{2^i} = k(\frac{3}{2})^i n$
$\vdots$	$\vdots$	$\vdots$	$\vdots$
$\log_2 n$	$\boxed{1} \quad \cdots \quad \boxed{1}$	$3^{\log_2 n}$	$k3^{\log_2 n} = kn^{\log_2 3}$

$$\text{Total: } \sum_{i=0}^{\log_2 n} 3^i k \frac{n}{2^i} = \Theta(n^{\log_2 3})$$

$$= \Theta(n^{1.58})$$