計算機数学I (2019)
第14回

照井 章（筑波大学 数理物質系 数学域）
Akira Terui (Institute of Mathematics, University of Tsukuba)

第13回のまとめ

- 除算の計算量
- （拡張）Euclid互除法の計算量
- 中国剰余算法の計算量

第14回の内容

- 高速乗算法:

  Karatsuba（カラツバ）の乗算アルゴリズム

  - 整数の乗算アルゴリズム
  - 1変数多項式の乗算アルゴリズム

Karatsuba（カラツバ）の乗算アルゴリズム（整数編）

10進2桁の整数の乗算

- $a = a_1 a_0 = a_1 \cdot 10 + a_0, \quad a_0, a_1 \in [0, \ldots, 9]$
- $b = b_1 b_0 = b_1 \cdot 10 + b_0, \quad b_0, b_1 \in [0, \ldots, 9]$

通常の方法で乗算を行う

$$(a_1 \cdot 10 + a_0)(b_1 \cdot 10 + b_0)$$

$$= a_1 b_1 \cdot 10^2 + (a_1 b_0 + a_0 b_1) \cdot 10 + a_0 b_0$$

Karatsubaの方法で乗算を行う

$$(a_1 \cdot 10 + a_0)\,(b_1 \cdot 10 + b_0)$$

$$= a_1 b_1 \cdot 10^2 + ((a_1 - a_0)(b_0 - b_1) + a_1 b_1 + a_0 b_0) \cdot 10 + a_0 b_0$$

10進 2*N* 桁の整数の乗算 (*N*>0)

通常の方法: $O(N^2)$ (👉第6回)

多倍長整数どうしの乗算:計算量

Algorithm 多倍長整数どうしの乗算 (a, b)

入力: $a = [a_0, a_1, \ldots, a_{k-1}], a_{k-1} \neq 0, b \in [b$ $\neq 0$

出力: $c =$ s.t. $c = a \cdot b$

乗算 O(len(a))

ループ *m*-1 回

1. $[c_0, c_1, \ldots, c_k] \leftarrow$ 多倍長・単精度乗算(a, b_0);
2. for $i \in [1..m\text{-}1]$ do
   $[c_i, \ldots, \gamma_{k+i}] \leftarrow [c_i, \ldots, \gamma_{k+i-1}]$
   $+$ 多倍長・単精度乗算(a, b_i);
3. return $[c_0, c_1, \ldots, c_{k+m-1}]$

加算 O(len(*a*))

乗算 O(len(*a*))

合計: $O(m \text{ len}(a)) = O(\text{len}(a) \text{ len}(b))$

21

10進 2*N* 桁の整数の乗算 (*N*>0)

Karatsubaの方法:

$$a = a_1 \cdot 10^N + a_0, \quad b = b_1 \cdot 10^N + b_0$$

$$(0 \leqq a_0, a_1, b_0, b_1 < 10^N)$$

$$ab \leftarrow a_1 b_1 \cdot 10^{2N} + ((a_1 - a_0)(b_0 - b_1) + a_1 b_1 + a_0 b_0) \cdot 10^N + a_0 b_0$$

*N*桁の整数の乗算: 3回

10進 2N 桁の整数の乗算 (N>0)

Karatsubaの方法:

さらに $(a_1 - a_0)(b_0 - b_1), a_1 b_1, a_0 b_0$ の乗算を**再帰的に分割して**行う

分割統治 (Divide and conquer)

Karatsuba乗算の計算量

定理: 10進 n 桁の整数の乗算の計算量は $O(n^{\lg 3})$.

証明: 2^n 桁の整数 a, b の乗算の計算量を$T(2^n)$とする. ただし $T(1) := 1$. $N := 2^{n-1}$ とする.

$$a = a_1 \cdot 10^N + a_0, \quad b = b_1 \cdot 10^N + b_0$$

$$0 \leqq a_0, a_1, b_0, b_1 < 10^N$$

Karatsuba乗算の計算量

このとき

$$ab \leftarrow a_1 b_1 \cdot 10^{2N} + ((a_1 - a_0)(b_0 - b_1) + a_1 b_1 + a_0 b_0) \cdot 10^N + a_0 b_0$$

- 2^{n-1} 桁の整数乗算: 3回 ⇒ 計算量 $3\,T(2^{n-1})$
- 2^n 桁の整数加算: 4回 ⇒ 計算量 $\leqq 8 \cdot 2^n$

よって、漸化式 $T(2^n) = 3\,T(2^{n-1}) + 8 \cdot 2^n$ を解く

Karatsuba乗算の計算量

「2^n 桁の整数加算: 4回 」の内訳

$$ab \leftarrow a_1 b_1 \cdot 10^{2N}$$
$$+ ((a_1 - a_0)(b_0 - b_1) + a_1 b_1 + a_0 b_0) \cdot 10^N + a_0 b_0$$

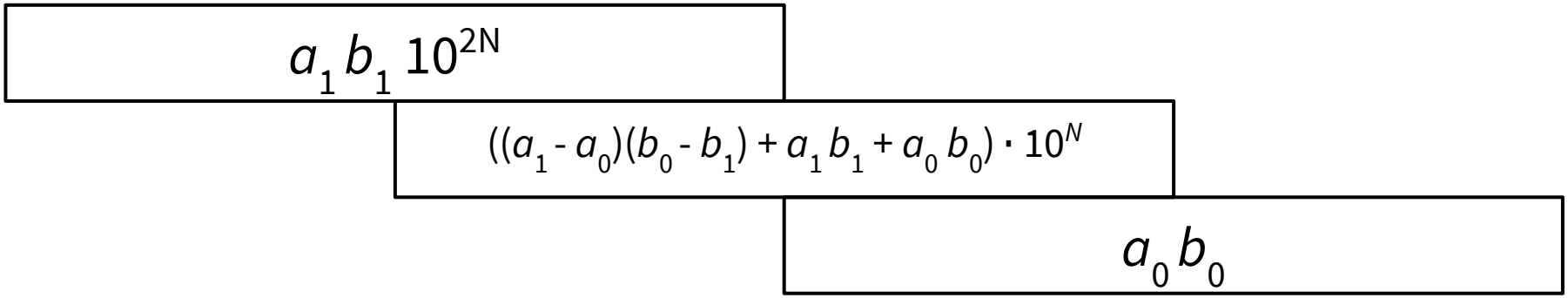
$a_1 - a_0, b_0 - b_1 : 2^{n-1}$ 桁の加算2回 = 2^n 桁の加算1回

$((a_1 - a_0)(b_0 - b_1) + a_1 b_1 + a_0 b_0)$: 2^n 桁の加算2回

Karatsuba乗算の計算量

$$ab \leftarrow a_1 b_1 \cdot 10^{2N}$$

$$+ ((a_1 - a_0)(b_0 - b_1) + a_1 b_1 + a_0 b_0) \cdot 10^N + a_0 b_0$$



☝ 実質的に2^n桁の加算1回

以上で2^n桁の加算4回分 ⇒ 計算量 ≦ $8 \cdot 2^n$)

Karatsuba乗算の計算量

$$T(2^n) = 3\,T(2^{n-1}) + 8 \cdot 2^n$$

$$= 3(3\,T(2^{n-2}) + 8 \cdot 2^{n-1}) + 8 \cdot 2^n$$

$$= 3^2\,T(2^{n-2}) + (3 \cdot 8 \cdot 2^{n-1} + 8 \cdot 2^n)$$

$$= 3^3\,T(2^{n-3}) + (3^2 \cdot 8 \cdot 2^{n-2} + 3 \cdot 8 \cdot 2^{n-1} + 8 \cdot 2^n)$$

$$= \cdots$$

$$= 3^n\,T(2^0) + 8\,(3^{n-1} \cdot 2 + 3^{n-2} \cdot 2^2 + \cdots + 3^0 \cdot 2^n)$$

Karatsuba乗算の計算量

$T(2^n) = 3\,T(2^{n-1}) + 8 \cdot 2^n$

$= 3^n\,T(2^0) + 8\,(3^{n-1} \cdot 2 + 3^{n-2} \cdot 2^2 + \cdots + 3^0 \cdot 2^n)$

$T(1) = 1$

公比 2/3 の等比数列の和
$= 16\,(3^n - 2^n)$

よって　$T(2^n) = 3^n + 16\,(3^n - 2^n) = 17 \cdot 3^n - 16 \cdot 2^n = O(3^n)$

Karatsuba乗算の計算量

$T(2^n) = 3^n + 16\,(3^n - 2^n) = 17 \cdot 3^n - 16 \cdot 2^n = O(3^n)$

$2^{\lg n} = n$ より $T(n) = T(2^{\lg n}) = O(3^{\lg n})$

$$\lg n = \frac{\log_3 n}{\log_3 2} = (\log_3 n)(\lg 3)$$

より

$$O(3^{\lg n}) = O(3^{(\log_3 n)(\lg 3)}) = O(n^{\lg 3}) < O(n^{1.59})$$

Karatsubaの乗算アルゴリズム（1変数多項式編）

Karatsubaの乗算アルゴリズム(1変数多項式)

基本的な方法は整数の乗算と同じ

$$f(x) = f_1(x) \cdot x^N + f_0(x), \qquad g(x) = g_1(x) \cdot x^N + g_0(x)$$

$$(N = 2^n,\ 0 \leqq \deg(f_1), \deg(f_0), \deg(g_1), \deg(g_0) < N)$$

のとき

$$f(x)\, g(x) \leftarrow f_1(x)\, g_1(x)\, x^{2N}$$

$$+ ((f_1 - f_0)(g_0 - g_1) + f_1 g_1 + f_0 g_0) \cdot x^N + f_0 g_0$$

Karatsubaの乗算アルゴリズム(1変数多項式)

Algorithm Karatsuba-poly (f, g)

入力: $f(x) = f_1(x) \cdot x^N + f_0(x)$, $g(x) = g_1(x) \cdot x^N + g_0(x)$

$N = 2^n$, $0 \leqq \deg(f_1), \deg(f_0), \deg(g_1), \deg(g_0) < N$

出力: $f(x)\, g(x)$

Karatsubaの乗算アルゴリズム(1変数多項式)

Algorithm Karatsuba-poly (f, g)

1. if $N = 1$ then return $f(x)\, g(x)$ (通常の多項式の積)
2.
   a. $a \leftarrow$ Karatsuba-poly (f_1, g_1);
   b. $b \leftarrow$ Karatsuba-poly (f_0, g_0);
   c. $c \leftarrow$ Karatsuba-poly $(f_1 - f_0, g_0 - g_1)$;
3. return $a\, x^{2N} + (a + b + c)\, x^N + b$;

Karatsuba乗算の計算量(1変数多項式)

定理: $N = 2^n$, $f, g \in \mathrm{R}[x]$, $\deg(f), \deg(g) < n$ のとき

Karatsuba乗算による f と g の乗算の計算量

(R の四則演算の回数) は $O(n^{\lg 3})$.

第14回のまとめ

- 高速乗算法:

  Karatsuba（カラツバ）の乗算アルゴリズム

  - 整数の乗算アルゴリズム
  - 1変数多項式の乗算アルゴリズム

第15回の内容

- 高速乗算法：高速フーリエ変換 (FFT)
  - 離散フーリエ変換 (DFT)
  - 高速フーリエ変換 (FFT)
  - FFTを用いた1変数多項式の高速乗算法