Toom-Cook 法

梅谷 武

作成：2001-02-24 更新：2006-01-12

多倍長整数の高速乗算法である Toom-Cook 法についてわかりやすく解説する。
IMS:20010224001; NDC:418; keywords:Toom-Cook 法;

目　　次

1　離散数学からの準備

1.1　順列と組み合わせ

Toom-Cook 法を理解するには、ほんの少しですが組み合わせ数学の知識があった方がいいかもしれません。記号の定義も兼ねて、順列と組み合わせから復習してみましょう。

補題 1.1 (順列) n 個のものから、k 個とる順列の個数は、

$$P(n,k) = \frac{n!}{(n-k)!}$$

に等しい。

定義 1.2 (第 1 種 Stirling 数) $P(n,k)$ を n に関する多項式として考えて展開する。

$$\begin{aligned} P(x,k) &= x(x-1)\cdots(x-k+1) \\ &= s(k,k)x^k + s(k,k-1)x^{k-1} + \cdots + s(k,1)x + s(k,0) \end{aligned}$$

この係数 $s(k,i), i = 0, \cdots, k$ を第 *1* 種 *Stirling* 数と呼ぶ。

補題 1.3 (第 1 種 Stirling 数の性質) 第 *1* 種 *Stirling* 数について次式が成り立つ。

$$\begin{aligned} s(n,0) &= 0,\ n \geqq 1 \\ s(n,n) &= 1,\ n \geqq 1 \\ s(n+1,k) &= s(n,k-1) - ns(n,k),\ n \geqq k \geqq 1 \end{aligned}$$

補題 1.4 (組み合わせ) n 個のものから、k 個とる組み合わせの個数は、

$$C(n,k) = \frac{n!}{k!(n-k)!}$$

に等しい。

定理 1.5 (２項定理) 正の整数 $n > 0$ について、x, y を変数とする恒等式

$$(x+y)^n = \sum_{k=0}^{n} C(n,k) x^{n-k} y^k$$

が成り立つ。この式により $C(n,k)$ を 2 項係数と呼ぶ。

補題 1.6 (２項係数の性質) 2 項係数について次式が成り立つ。

$$\begin{aligned} C(n,0) &= 1,\ n \geqq 1 \\ C(n,n) &= 1,\ n \geqq 1 \\ C(n,k) &= C(n-1,k) + C(n-1,k-1),\ n \geqq k \geqq 1 \end{aligned}$$

この性質によって、任意の 2 項係数を加法だけを使って計算することができます。この算法を図形的に表現したものが、いわゆる Pascal の三角形です。Toom の算法を図形的に表現すると、やはり Toom の三角形ともいえる図形になります。

1.2 第 2 種 Stirling 数

定義 1.7 (第 2 種 Stirling 数) n 個のものを k 個に分割する仕方の個数を第 *2* 種 *Stirling* 数と呼び、$S(n,k)$ と書く。$n \geqq k \geqq 1$ 以外のときは $S(n,k) = 0$ と約束する。

補題 1.8 (第 2 種 Stirling 数の性質) 第 *2* 種 *Stirling* 数について次式が成り立つ。

$$\begin{aligned} S(n,1) &= 1,\ n \geqq 1 \\ S(n,n) &= 1,\ n \geqq 1 \\ S(n+1,k) &= S(n,k-1) + kS(n,k),\ n \geqq k \geqq 1 \end{aligned}$$

補題 1.9 第 *2* 種 *Stirling* 数について次式が成り立つ。

$$S(n,k) = \sum_{i=0}^{n-1} C(n-1,i)S(i,k-1),\ n \geqq 1$$

補題 1.10 第 *2* 種 *Stirling* 数について次式が成り立つ。

$$x^n = \sum_{k=1}^{n} S(n,k)P(x,k),\ n \geqq 1,\ x \text{ は変数}$$

補題 1.11 第 *2* 種 *Stirling* 数について次式が成り立つ。

$$S(n,k) = \frac{1}{k!}\sum_{i=1}^{k} (-1)^{k-i}C(k,i)i^n,\ n \geqq k \geqq 1$$

2 Toom-Cook 法

2.1 Toom の三角形

Knuth[S2] によれば、Toom-Cook 法は Karatsuba 法が発表された翌年の 1963 年にやはりソ連の A. L. Toom によって基本的な考え方が発表され、その後、1966 年にハーバード大学の S. A. Cook により実際の計算機で作譜する方法が示されました。米ソ冷戦時代のこの時期、この分野においてはソ連が先行し、米国が追いかけていたようにも見えます。

$K > 0$ とし、正の整数 a, b が、基数 $P = 2^K$ により次のように P 進表現されるものとします。

$$a = a_r P^r + \cdots + a_1 P + a_0, 0 \leqq a_i < P$$
$$b = b_r P^r + \cdots + b_1 P + b_0, 0 \leqq b_i < P$$

ここで、多項式

$$a(x) = a_r x^r + \cdots + a_1 x + a_0$$
$$b(x) = b_r x^r + \cdots + b_1 x + b_0$$

を考え、その積を

$$\begin{aligned} c(x) &= a(x)b(x) \\ &= c_{2r}x^{2r} + \cdots + c_1 x + c_0 \end{aligned}$$

とします。Toom-Cook 法は $2r+1$ 個の値、

$$c(i) = a(i)b(i),\ i = 0, \cdots, 2r$$

から $c(x)$ の係数を計算し、それに基数 $P = 2^K$ を代入することによって積 ab を求めます。

まず、$m = 2r + 1$ とおき多項式 $c(x)$ を

$$\begin{aligned} c(x) &= c_{m-1}x^{m-1} + \cdots + c_1 x + c_0 \\ &= \sum_{i=1}^{m-1} c_i x^i + c_0 \\ &= \sum_{i=1}^{m-1} c_i (\sum_{k=1}^{i} S(i,k)P(x,k)) + c_0 \\ &= \sum_{i=0}^{m-1} \theta_i P(x,i) \end{aligned}$$

と $P(x,i)$ で展開します。ここで、$a(x), b(x)$ の係数が負でないことから $c(x)$ の係数も負ではなく、さらに $\theta_i, i = 0, \cdots m-1$ も負でないことに注意してください。このことが Toom-Cook 法の途中の計算結果が負でないことを保証することになります。

補題 2.1 $P(x,k)$ に関して次式が成り立つ。

$$P(x+1,k) - P(x,k) = kP(x,k-1),\ k \geqq 1$$

証明 $k = 1$ のとき、

$$\begin{aligned} P(x+1,1) - P(x,1) &= x + 1 - x \\ &= 1 = P(x,0) \end{aligned}$$

$k > 1$ のとき、

$$\begin{aligned} P(x+1,k) - P(x,k) &= (x+1)x(x-1)\cdots(x-k+2) - x(x-1)\cdots(x-k+1) \\ &= x(x-1)\cdots(x-k+2)(x+1-(x-k+1)) \\ &= kP(x,k-1) \end{aligned}$$

■

補題 2.2 $c(x)$ に関して次式が成り立つ。

$$c(x+1) - c(x) = \sum_{i=1}^{m-1} i\theta_i P(x,i-1)$$

証明

$$\begin{aligned} c(x+1) - c(x) &= \sum_{i=1}^{m-1} \theta_i (P(x+1,i) - P(x,i)) \\ &= \sum_{i=1}^{m-1} i\theta_i P(x,i-1) \end{aligned}$$

■

定義 2.3 多項式 $c(x) = c_{m-1}x^{m-1} + \cdots + c_1 x + c_0$ が与えられたとき、

$$\Psi_c(x,k) = \frac{1}{k!}\sum_{i=0}^{k}(-1)^i C(k,i)c(x+k-i),\ k \geqq 0$$

と定義する。

補題 2.4 これまでの仮定の下で次式が成り立つ。

$$\Psi_c(x,k+1) = \frac{1}{k+1}(\Psi_c(x+1,k) - \Psi_c(x,k)),\ k \geqq 0$$

証明 定義から、

$$\Psi_c(x,k+1) = \frac{1}{(k+1)!}\sum_{i=0}^{k+1}(-1)^i C(k+1,i)c(x+k+1-i),\ k \geqq 0$$

である。

$$C(k+1,i) = C(k,i) + C(k,i-1)$$

を使って、

$$\begin{aligned}
\Psi_c(x,k+1) &= \frac{1}{(k+1)!}(\sum_{i=1}^{k}(-1)^i(C(k,i)+C(k,i-1))c(x+k+1-i) + (-1)^{k+1}c(x) + (-1)^0 c(x+k+1)) \\
&= \frac{1}{(k+1)!}(\sum_{i=0}^{k}(-1)^i C(k,i)c(x+k+1-i) - \sum_{j=0}^{k}(-1)^j C(k,j)c(x+k-j)) \\
&= \frac{1}{k+1}(\frac{1}{k!}\sum_{i=0}^{k}(-1)^i C(k,i)c((x+1)+k-i) - \frac{1}{k!}\sum_{j=0}^{k}(-1)^j C(k,j)c(x+k-j))
\end{aligned}$$

■

定理 2.5 (Toom-Cook 法の原理) これまでの仮定の下で次式が成り立つ。

$$\Psi_c(x,k) = \sum_{i=k}^{m-1} C(i,k)\theta_i P(x,i-k),\ k \geqq 0$$

証明 帰納法による。$k = 0$ のとき

$$\begin{aligned}
\Psi_c(x,0) &= c(x) \\
&= \sum_{i=0}^{m-1}\theta_i P(x,i)
\end{aligned}$$

$k = 1$ のときは補題 *[2.2]* を使う。

$$\begin{aligned}
\Psi_c(x,1) &= c(x+1) - c(x) \\
&= \sum_{i=1}^{m-1} i\theta_i P(x,i-1) \\
&= \sum_{i=1}^{m-1} C(i,1)\theta_i P(x,i-1)
\end{aligned}$$

k で正しいとして $k+1$ で成り立つことを示す。

$$\begin{aligned}\Psi_c(x,k+1) &= \frac{1}{k+1}(\Psi_c(x+1,k)-\Psi_c(x,k)) \\ &= \frac{1}{k+1}(\sum_{i=k}^{m-1} C(i,k)\theta_i P(x+1,i-k) - \sum_{i=k}^{m-1} C(i,k)\theta_i P(x,i-k)) \\ &= \frac{1}{k+1}\sum_{i=k+1}^{m-1} C(i,k)\theta_i (P(x+1,i-k)-P(x,i-k) \\ &= \frac{1}{k+1}\sum_{i=k+1}^{m-1} C(i,k)\theta_i (i-k) P(x,i-(k+1)) \\ &= \sum_{i=k+1}^{m-1} C(i,k+1)\theta_i P(x,i-(k+1))\end{aligned}$$

■

系 2.6 これまでの仮定の下で次式が成り立つ。

$$\Psi_c(0,k) = \theta_k,\ k \geqq 0$$

これで Toom の三角形を描く準備ができました。$r=2$ のときを考えます。まず

$$c(0), c(1), c(2), c(3), c(4)$$

を計算し、これを利用して次の行列を計算します。

$$\begin{pmatrix} c(0)=\Psi_c(0,0) & \Psi_c(0,1) & \Psi_c(0,2) & \Psi_c(0,3) & \Psi_c(0,4) \\ c(1)=\Psi_c(1,0) & \Psi_c(1,1) & \Psi_c(1,2) & \Psi_c(1,3) & 0 \\ c(2)=\Psi_c(2,0) & \Psi_c(2,1) & \Psi_c(2,2) & 0 & 0 \\ c(3)=\Psi_c(3,0) & \Psi_c(3,1) & 0 & 0 & 0 \\ c(4)=\Psi_c(4,0) & 0 & 0 & 0 & 0 \end{pmatrix}$$

１列目はすでに計算されています。２列目以降は

$$\Psi_c(x,k+1) = \frac{1}{k+1}(\Psi_c(x+1,k)-\Psi_c(x,k))$$

によって計算します。k+1 列目の値は、k 列目の２つの値の差を k+1 で割ることによって得られます。この結果得られた行列の第１行が

$$\theta_0, \theta_1, \theta_2, \theta_3, \theta_4$$

となっています。

参考文献

離散数学

[D1] 高橋 巖郎, 藤重 悟, “離散数学”, 岩波書店, 1981

算法

[S1] 野下 浩平, 高岡 忠雄, 町田 元, “基本的算法”, 岩波書店, 1983

[S2] D. E. Knuth(中川 圭介訳), “準数値算法/算術演算”, サイエンス社, 1986