多項式の乗算を高速に計算する方法

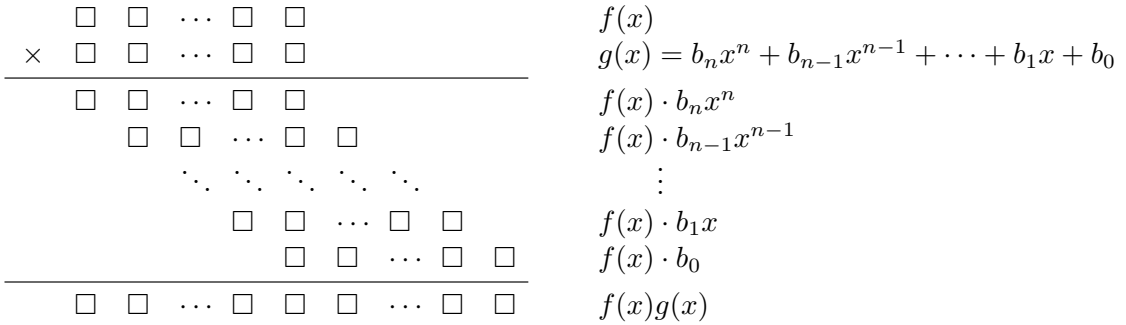
関川 浩（理学部第一部応用数学科）

1　はじめに

多項式の乗算は科学技術計算を始め，あらゆる場面に現れる基本的な計算です．たとえば，ある種の暗号を設計する際には，かなり次数の高い多項式の乗算を大量に行うことになります．多項式の乗算には係数の乗算，加算が数多く必要なので，これらの演算の回数を減らすことにより計算を速くできないか考えてみましょう．計算速度の向上やコンピュータのメモリ消費量の削減など，計算の効率を考えることも応用数学では重要なテーマです．

2　普通の計算法

二つの n 次多項式 $f(x)$ と $g(x)$ の積 $f(x)g(x)$ を計算するには係数の乗算，加算が何回必要でしょうか？普通に $f(x)g(x)$ を計算するときの様子を書いてみましょう．



左側は $f(x)g(x)$ の計算，右側はその説明です．左側では，イメージをつかみやすいよう係数はすべて □ で表し，また，場所をきちんとそろえて書けば x^k や $+$ の記号は不要なので係数のみを書いています．二本の横線ではさまれた各行を得るには乗算が $n+1$ 回必要です（加算は 0 回）．全部で $n+1$ 行ありますから，乗算は合計 $(n+1)^2$ 回です．二本の横線ではさまれた部分の □ を縦方向に足したものが $f(x)g(x)$ の各係数です．加算の回数は左から $0, 1, \ldots, n-1, n, n-1, \ldots, 1, 0$ ですから，合計 n^2 回です（乗算は 0 回）．つまり，合計で係数の乗算が $(n+1)^2$ 回, 加算が n^2 回必要となります．一部の項がなければ乗算，加算の回数は減りますが，ここでは回数が一番多い場合を考えます．

3　カラツバ法

係数の演算回数を減らして多項式の乗算を速くできないか考えてみましょう．アイディアが分かりやすいよう，次数 n が奇数の場合で説明することにして $n = 2m - 1$ とおきます．多項式 $f(x)$, $g(x)$ を次数が m 以上の部分と m 未満の部分に分割して，

$$f(x) = f_1(x)x^m + f_2(x), \qquad g(x) = g_1(x)x^m + g_2(x) \tag{1}$$

と書きます．このとき，四つの多項式 $f_1(x)$, $f_2(x)$, $g_1(x)$, $g_2(x)$ は $m - 1$ 次であることに注意してください．たとえば，$f(x) = x^5 - 2x^4 + 3x^3 - 4x^2 + 5x - 6$ なら $n = 5$, $m = 3$ ですから，

$$f(x) = (x^2 - 2x + 3)x^3 + (-4x^2 + 5x - 6)$$

と書きます．$f_1(x) = x^2 - 2x + 3$, $f_2(x) = -4x^2 + 5x - 6$ はともに 2 次です．

さて，式 (1) から，

$$\begin{aligned} f(x)g(x) &= (f_1(x)x^m + f_2(x))(g_1(x)x^m + g_2(x)) \\ &= f_1(x)g_1(x)x^{2m} + (f_1(x)g_2(x) + f_2(x)g_1(x))x^m + f_2(x)g_2(x) \end{aligned}$$

です．ここで，$f_2(x)g_2(x)$ の項は 0 次から $2m - 2$ 次までの範囲，$(f_1(x)g_2(x) + f_2(x)g_1(x))x^m$ の項は m 次から $3m - 2$ 次までの範囲，$f_1(x)g_1(x)x^{2m}$ の項は $2m$ 次から $4m - 2$ 次までの範囲にあります．このことに注意して係数の演算回数を数えると以下のとおりとなります．

- $m - 1$ 多項式の積 $f_1(x)g_1(x)$, $f_1(x)g_2(x)$, $f_2(x)g_1(x)$, $f_2(x)g_2(x)$ の計算に，それぞれ乗算 m^2 回，加算 $(m - 1)^2$ 回．
- $2m - 2$ 多項式 $f_1(x)g_2(x)$ と $f_2(x)g_1(x)$ の和の計算に加算 $2m - 1$ 回．
- m 次から $2m - 2$ 次の項は $(f_1(x)g_2(x) + f_2(x)g_1(x))x^m$ と $f_2(x)g_2(x)$ にあり，また，$2m$ 次から $3m - 2$ 次の項は $(f_1(x)g_2(x) + f_2(x)g_1(x))x^m$ と $f_1(x)g_1(x)x^{2m}$ にあり，それらの項の係数の計算に，それぞれ加算が $m - 1$ 回．

合計すると乗算 $4m^2$ 回，加算 $4(m - 1)^2 + 4m - 3$ 回です．普通に計算すると乗算 $4m^2$ 回，加算 $4(m - 1)^2$ 回ですから，分割したことにより加算が $4m - 3$ 回増えてしまいました．

では，次のように計算したらどうでしょうか．まず，

$$u(x) = (f_1(x) + f_2(x))(g_1(x) + g_2(x)), \qquad v(x) = f_1(x)g_1(x), \qquad w(x) = f_2(x)g_2(x)$$

を計算します．次に，

$$v(x)x^{2m} + (u(x) - v(x) - w(x))x^m + w(x)$$

を計算すると $f(x)g(x)$ になります．係数の演算回数を数えましょう．

- $m - 1$ 次多項式 $f_1(x) + f_2(x)$ と $g_1(x) + g_2(x)$ の計算に加算がそれぞれ m 回．

- 二つの $m-1$ 次多項式の積が 3 回あり，それぞれ，乗算 m^2 回，加算 $(m-1)^2$ 回.
- $u(x)-v(x)-w(x)$ の減算の計算に係数の減算 $4m-2$ 回.
- m 次から $2m-2$ 次の項は $w(x)$ と $(u(x)-v(x)-w(x))x^m$ にあり，また，$2m$ 次から $3m-2$ 次の項は $(u(x)-v(x)-w(x))x^m$ と $w(x)x^{2m}$ にあり，それらの項の係数の計算に，そえぞれ加算が $m-1$ 回.

合計で乗算が $3m^2$ 回，加減算が $3(m-1)^2+8m-4$ 回となり，乗算が m^2 回減っています．乗算は加減算より手間のかかる計算であることを考えると乗算が m^2 回減る効果は大きく，計算は速くなっているといえます（$10 \leqq m$ のとき $8m-4<(m-1)^2$ であり，加減算の回数も減ります）．これを「二分割する方法」と呼ぶことにしましょう．

もっと速い方法はあるでしょうか？ここでも説明を分かりやすくするため，多項式の次数 n は 2^m-1 であるとします（m は自然数）．二分割した多項式の積を計算する際に，二分割した各多項式をさらに二分割，さらに二分割，と二分割する方法を 1 次式になるまで繰り返し用います．二分割する方法で二つの 2^m-1 次式の積を計算する際，$2^{m-1}-1$ 次式の積が 3 回で，係数の乗算はそこにしか現われないこと，1 次式の積を計算する際，係数の乗算は 3 回であることから，最初が 2^m-1 次の場合，係数の乗算は 3^m 回となります．二分割を繰り返す方法は発見者の名前をとってカラツバ法と呼ばれます．普通の計算法では n 次のとき乗算は $(n+1)^2$ 回ですから，$n=2^m-1$ のとき 4^m 回となります．たとえば，n が 127 $(=2^7-1)$, 511 $(=2^9-1)$, 1023 $(=2^{10}-1)$ のとき，m は 7, 9, 10 で，4^m は 16384, 262144, 1048576（約 105 万）です．一方，3^m は 2187, 19683, 59049 ですから，普通の計算法にくらべてカラツバ法は非常に速いことが分かります．

なお，多項式が 2^m-1 次ではないとき，たとえば x^2-2x+3 のときは $x^2-2x+3=0\cdot x^3+x^2-2x+3$ と見て，次数を 3 $(=2^2-1)$ と思って計算します．

4　おわりに

整数の乗算にも二分割する方法が利用できます．たとえば，12345678×87654321 の計算は，

$$12345678=1234\cdot 10^4+5678, \qquad 87654321=8765\cdot 10^4+4321$$

と二分割して書き，

$$u=(1234+5678)(8765+4321), \qquad v=1234\times 8765, \qquad w=5678\times 4321$$

を計算すれば，

$$12345678\times 87654321=v\cdot 10^8+(u-v-x)\cdot 10^4+w$$

です．したがって，二分割する方法を繰り返すカラツバ法も使えます．ここで，10^8 や 10^4 を掛ける計算は 0 を書き足すだけでよいことに注意してください．ただし，整数の場合は繰り上がり，繰り下がりが生じるので，多項式の場合よりも計算はやや複雑になります．

カラツバ法や，高速フーリエ変換と呼ばれる手法を用いた，さらに高速な計算法は，応用数学科の 2 年生の科目「コンピュータ数学基礎 2 及び演習」で学習する内容です．