ショートノート

多項式の前処理つき計算の複雑さについて†

野崎 昭弘††

変数 $x_1, x_2, \cdots, x_p$ の多項式で，その係数が他の変数 $a_1, a_2, \cdots, a_q$ の多項式であるようなものの複数個の組が与えられたとき，それらの値を計算するのに必要な乗算の回数のひとつの下限を与えた．すなわち，$x_1, \cdots, x_p$ の多項式として積和型に展開したときの定数項以外の係数（a についての多項式）で，"多項式に関して独立" なものが s 個あれば，それらの値の計算には，$a_1, \cdots, a_q$ についての前処理を許しても，少なくとも $s/2$ 回の乗算が必要である．

1. まえがき

多項式の計算の複雑さについては，すでに基本的な結果が数多く得られており，その方面の入門的な解説書も現われている[1]．しかし係数に対する前処理を許す場合については，不満足な部分が多い．たとえば必要な乗算回数の下界は，1変数多項式に対しては与えられているが（文献[1]，定理 12.4），多変数の場合にどうなるかはあまりよくわかっていない．そこで我々は多変数の多項式が複数個与えられた場合の乗算回数の下界を考えてみたが，従来の考え方が簡単な工夫で拡張できることがわかったので，主要な結果と応用例を述べてみたい．

なお本文では実係数の多項式のみを論じているが，全く同じことが複素係数の多項式についても成りたつ．

2. 用語と記号

すべての実数の集合を記号 $\boldsymbol{R}$ であらわす．また変数 $u_1, \cdots, u_k$（記号は何でもよい）に関する実係数多項式の全体を $\boldsymbol{R}[u_1, \cdots, u_k]$ であらわす．

変数 $x_1, \cdots, x_p$, $a_1, \cdots, a_q$ に関する多項式

$$Q \in \boldsymbol{R}[x_1, \cdots, x_p, a_1, \cdots, a_q]$$

を考えよう．Q を変数 $x_1, \cdots, x_p$ について展開し，同類項を整理すれば，次の形に書くことができる．

$$Q = \Sigma H(i(1), \cdots, i(p)) x_1^{i(1)} \cdots x_p^{i(p)}$$

ここで

$$H(i(1), \cdots, i(p)) \in \boldsymbol{R}[a_1, \cdots, a_q].$$

以下これらの $H(\cdots)$ を，Q の変数 $\{x_k\}$ **に関する係数**と呼ぶ．また特に $H(0, \cdots, 0)$ を変数 $\{x_k\}$ **に関する定数項**と呼ぶことにする．

［定義］ 変数 $a_1, \cdots, a_q$ についての多項式 $H_1, \cdots, H_s$ が **P-独立** (polynomially independent) であるとは，すべての $a_1, \cdots, a_q \in \boldsymbol{R}$ に対して

$$F(H_1(a_1, \cdots, a_q), \cdots, H_s(a_1, \cdots, a_q)) = 0$$

となる実係数の多項式 $F(X_1, \cdots, X_s)$ は，実はすべての $X_1, \cdots, X_s \in \boldsymbol{R}$ に対して恒等的に 0 に等しいことをいう．また P-独立でないことを **P-従属**という．

［例 1］ $H_1(a_1, a_2) = (a_1 + a_2)^2$,

$$H_2(a_1, a_2) = a_1 + a_2 - 1$$

とおくと，H_1 と H_2 とは P-独立でなく，P-従属である．実際，恒等的には 0 でない多項式

$$F(X, Y) = X - (Y+1)^2$$

に対して，次の式が成り立つ．

$$F(H_1(a_1, a_2), H_2(a_1, a_2)) = 0$$

［例 2］ $H_i(a_1, \cdots, a_q) = a_i$ $(1 \leqq i \leqq q)$ とおくと，$H_1, \cdots, H_q$ は P-独立である．

［例 3］ $a_1, \cdots, a_q$ の多項式

$$H_1, \cdots, H_s$$

は，$s > q$ のとき，P-従属である．

これは Aho-Hopcraft-Ullman[1] の補題 12.2 のいいかえにすぎない．

［例 4］ n 変数 $\alpha_1, \cdots, \alpha_n$ の基本対称式

$$S_1 = \alpha_1 + \alpha_2 + \cdots + \alpha_n$$

$$S_2 = \alpha_1\alpha_2 + \alpha_1\alpha_3 + \cdots + \alpha_{n-1}\alpha_n,$$

$$\cdots\cdots,$$

$$S_n = \alpha_1\alpha_2\cdots\alpha_n$$

は P-独立である（これは自明ではないが，複素数の範囲で考えれば初等的に示せるので，証明は省略する）．

† A Note on the Complexity of Evaluation of Polynomials with Preconditioning by AKIHIRO NOZAKI (Department of Computer Science, Faculty of Engineering, Yamanashi University).

†† 国際基督教大学理学科

3. 乗算回数の下界

変数 $x_1, \cdots, x_p$ および $a_1, \cdots, a_q$ に関するいくつかの多項式

$Q_1, \cdots, Q_N$

が与えられたとしよう．そして変数 $a_1, \cdots, a_q$ に対する前処理を許したときの，これらの多項式の計算に必要な乗算回数の下界について考える．

定理 多項式

$Q_1, \cdots, Q_N \in \boldsymbol{R}[x_1, \cdots, x_p, a_1, \cdots, a_q]$

の，変数 $\{x_k\}$ に関する係数

$H_j(i(1), \cdots, i(p)) \in \boldsymbol{R}[a_1, \cdots, a_q]$

のうち，定数項を除くある s 個

$H^{(1)}, \cdots, H^{(s)}$

が P-独立であるならば，多項式 $Q_1, \cdots, Q_N$ の値を求めるのに，変数 $a_1, \cdots, a_q$ に対するどのような前処理を許しても，$\lceil s/2 \rceil$ 回の乗算が必要である．

［証明］ 適当な前処理の後，t 回の乗算で $Q_1, \cdots, Q_N$ を求める任意の計算法を考える．その計算法における乗算の結果を，求めた順に $f_1, \cdots, f_t$ とおくと，各 f_i の値は次のようにあらわされる．

$$f_i = [L_{2i-1}(x_1, \cdots, x_p, f_1, \cdots, f_{i-1}) + \alpha_i] \times [L_{2i}(x_1, \cdots, x_p, f_1, \cdots, f_{i-1}) + \beta_i]$$

ここで L_k はある1次式で，α_i, β_i は $a_1, \cdots, a_q$ のみによって定まるパラメータである．さらに，各 Q_j の値も次のようにあらわされる．

$$Q_j = M_j(x_i, \cdots, x_p, f_1, \cdots, f_t) + r_j$$

ここで M_j はある1次式，r_j は $a_1, \cdots, a_q$ のみによって定まるパラメータである．M_j の中の $f_t, f_{t-1}, \cdots$ に，前の等式を順次代入してゆけば，最終的には $x_1, \cdots, x_p$ および $\alpha_1, \beta_1, \cdots, \alpha_t, \beta_t, \gamma_1, \cdots, \gamma_N$ に関する多項式が得られるであろう．それを $x_1, \cdots, x_p$ についての多項式として

$$\Sigma G_j(i(1), \cdots, i(p)) x_1^{i(1)} \cdots x_p^{i(p)}$$

の形に整理すれば，これが Q_j に等しいことから，係数の間の関係

$$H_j(i(1), \cdots, i(p)) = G_j(i(1), \cdots, i(p))$$

が得られる．

ここで，P-独立な係数 $H^{(1)}, \cdots, H^{(s)}$ を左辺とする等式に注目しよう．以下それらを

$$H^{(j)} = G^{(j)} \quad (1 \leqq j \leqq s) \qquad (*)$$

であらわす．明らかに，パラメータ $\gamma_1, \cdots, \gamma_N$ は定数項にしか関係しないから，

$G^{(j)} \in \boldsymbol{R}[\alpha_1, \beta_1, \cdots, \alpha_t, \beta_t]$

と考えてよい．そこで，

$s > 2t$

と仮定して矛盾を導くことにしよう．

前章［例 3］で述べたように $s > 2t$ ならば多項式

$G^{(1)}, \cdots, G^{(s)}$

は P-従属である．すなわち，恒等的には0でない多項式 F が存在して，すべての $\alpha_1, \cdots, \beta_t$ に対して

$F(G^{(1)}(\alpha_1, \cdots), \cdots, G^{(s)}(\cdots, \beta_t)) = 0$ となる．一方，$H^{(j)}$ 等は仮定によって P-独立であるから，ある $a_1, \cdots, a_q$ の値に対して

$F(H^{(1)}(a_1, \cdots), \cdots, H^{(s)}(\cdots, a_q)) \neq 0$

となる．したがってそのような $\{a_k\}$ の値に対しては，パラメータ $\alpha_1, \cdots, \beta_t$ の値をどのように定めても，係数の間の等式(*)を成りたたせることができない．これは矛盾であるから，$s \leqq 2t$ でなければならない．t は整数だから，

$\lceil s/2 \rceil \leqq t.$

したがって $Q_1, \cdots, Q_N$ を求めるどんな計算法も，少なくとも $\lceil s/2 \rceil$ 回の乗算を含む． ［証明終］

［応用 1］ n 次多項式

$P(x) = x^n + ax^{n-1} + \cdots + cx + d$

の計算には，一般に $\lceil (n-1)/2 \rceil$ 回の乗算が必要である[1]．では，

$P(x) = 0$

の根がすべて実数でしかも既知と仮定した場合にも，同じことがいえるであろうか？この問は次のように答えられる．n 個の実根を $\alpha_1, \cdots, \alpha_n$ とおくと

$P(x) = (x-\alpha_1) \cdots (x-\alpha_n)$

と因数分解できる．この式を展開すると，x の係数として基本対称式が現われるが，それらは P-独立である．定数項 S_n を除いても P-独立であるから，$P(x)$ の計算には，根がすべて実数であるとしても，$\lceil (n-1)/2 \rceil$ 回の乗算が必要である．

なお $n=4$ の場合，Todd の方法によれば，$\lceil (n-1)/2 \rceil = 2$ 回の乗算で多項式の値が求められる（最高次の係数が1であることに注意）[2]．

［応用 2］ k 個の n 次多項式

$$a_{1n}x^n + \cdots + a_{11}x + a_{10},$$
$$a_{2n}x^n + \cdots + a_{21}x + a_{20},$$
$$\cdots,$$
$$a_{kn}x^n + \cdots + a_{k1}x + a_{k0}$$

を考える．定数項以外の係数

$a_{1n}, \cdots, a_{11}, \cdots, a_{kn}, \cdots, a_{k1}$

は kn 個あるが，これらは $a_{1n}, \cdots, a_{k1}$ の多項式とし

て P-独立である（前章 [例 2]）．したがってこれらの計算には，少なくとも $\lceil kn/2 \rceil$ 回の乗算が必要である．

なおこれらの多項式は，Belaga の方法[3]によれば

$$k \times \lfloor (n+3)/2 \rfloor - k + 1$$

回の乗算で求めることができる．n が偶数の場合には，この数と我々の下界との差はわずかである．

[応用 3] 3変数の一般の多項式

$$\sum_{i,j,k=0}^{n} a_{i,j,k} x^i y^j z^k$$

を求めるには，少なくとも

$$\lceil ((n+1)^3 - 1)/2 \rceil$$

回の乗算が必要である（証明は [応用 2] と同様）．

4. むすび

上に述べた定理は，一般性があり，また応用例で示したようによい下界も与える場合もある．しかしこれでは精密な下界が得られない場合も多い．それはこの定理が基本的には係数の“自由度”にしか注目しておらず，変数 $x_1, \cdots, x_r$ の性質（次数など）が無視されているので，やむをえないところである．さらに精密な下界を与えることは，一般にはむずかしいであろうが，今後の課題である．

参考文献

1) Aho, A. V., Hopcroft, J. E., and Ullman, D.: The Design and Analysis of Computer Algorithms, Addison-Wesley (1974).
2) Todd, J.: Motivation for Working in Numerical Analysis, Comm. Pure and Appl. Math., Vol. 8, p. 97 (1955).
3) Belaga, E. G.: Some Problems Involved in the Calculation of Polynomials, Dokladi Akademii Nauk, SSSR, Vol. 123, p. 775 (1958).

（昭和53年12月7日受付）
（昭和54年3月15日採録）