有理関数補間を用いた近似 GCD 計算

甲斐 博

愛媛大学大学院理工学研究科

1 はじめに

近似 GCD の研究は Sasaki,Noda[4] により最初の近似 GCD アルゴリズムが提案されて以来多くの研究がされてきた．一変数と多変数の近似 GCD の研究があるが，本研究では一変数の場合を扱う．

計算法としては多項式剰余列計算や QR 分解などが用いられるが，主係数が小さい場合には近似 GCD の係数の相対誤差が大きくなることがある．本研究では有理関数近似を用いる方法を検討する．有理関数近似を用いる方法としては，Kai,Noda [2] や Pan[3] により Padé 近似を用いる方法が考えられているが，ここでは有理関数補間を用いる．多変数の近似 GCD を求める計算に多項式補間が用いられることはあったが，有理関数補間を近似 GCD の計算に用いた例は例がない．いくつかの例題に適用し，主変数が小さい場合にも比較的良い結果を与えることを示す．

2 近似 GCD の問題点

近似 GCD の計算の難しさは，主係数が小さい多項式を入力とする場合である．この場合，近似 GCD の係数の桁落ち誤差が問題になる．

例えば，安定な解を与えると言われる Zeng により提案された方法 (uvGcd)[5][6] を用いて，次の多項式 $p(x)$ と $q(x)$ の近似 GCD を求めることを考える．

$$p(x) = (g(x) + 10^{-4})(x^4 + 7x^2 - x + 1),$$

$$q(x) = g(x)(x^3 - x^2 + 4x - 2).$$

ここで，

$$g(x) = \alpha x^3 + 2\alpha x^2 - x + 5$$

とし，パラメータ $\alpha = 10^{-10}$ とする．計算は Maple 11 上で行い，多倍長浮動小数の桁を 20 桁と設定し計算する．精度 10^{-3} での uvgcd を求めると，

$$\hat{g}(x) = 2.490\times 10^{-6}x^3 + 3.149\times 10^{-6}x^2 - 1.000x + 5.000,$$

という結果が得られる．高次項の微小係数の桁が大きく異なることが分かる．$p(x)$ の因子 $g(x) + 10^{-4}$ と，$q(x)$ に含まれる因子 $g(x)$ が近似 GCD として得られるが，前者の多項式の根は，

$$-100003.4999, 5.000100017, 99996.49984$$

であり，後者の多項式の根は，

$$-100003.4999, 5.000000017, 99996.49989$$

である．よって，得られる近似 GCD の根も $-100003.5, 5.0, 99996.5$ 近傍の値がそれぞれ期待される．しかし uvgcd により得られた $\hat{g}(x)$ の根は，

$$-636.7, 5.000, 630.5$$

であり大きく値が異なる．

3 有理関数補間を用いた近似 GCD

$p(x), q(x) \in F[x]$ を一変数多項式とする．m と n をそれぞれの多項式の次数とする．$r(x) = p(x)/q(x)$ 上の $M := m + n + 1$ 個の点を，分子が m 次で分母が n 次の有理関数で補間すると，結果として当然ながら $r(x)$ と同じ有理関数が得られる．しかし，$p(x)$ と $q(x)$ が自明でない GCD $g(x)$ を持つ場合は（つまり，$p(x) = g(x)\tilde{p}(x)$, $q(x) = g(x)\tilde{q}(x)$ と表される場合)，有理関数補間の解が複数個存在することになる．一意に解を決定するには既約な有理関数 $\tilde{p}(x)/\tilde{q}(x)$ を求める必要がある．規約な有理関数が得られれば，$g(x) = p(x)/\tilde{p}(x)$ (または，$g(x) = q(x)/\tilde{q}(x)$) により GCD を計算することができる．

変数 x について M 個の異なる点 $X := \{x_i | i = 1, \cdots, M\}$ を適当に取り，それらの点上での有理関数

Approximate GCD using rational interpolation
Hiroshi KAI
Graduate School of Science and Engineering,
Ehime University,
Bunkyo-cho 3, Matsuyama, Ehime, 790-8577 Japan
kai@hpc.cs.ehime-u.ac.jp

$p(x)/q(x)$ の値 $Y := \{r_i := p(x_i)/q(x_i) | i = 1, \cdots, M\}$ を求める．X と Y を用いて連立一次方程式をたてると有理関数補間を求めることができる．ここで，

$$p(x) = a_m x^m + a_{m-1} x^{m-1} + \cdots + a_0$$

$$q(x) = b_n x^n + b_{n-1} x^{n-1} + \cdots + b_1 x + 1$$

とすると，

$$p(x_i) - r_i q(x_i) = 0, i = 1, \cdots, m+n+1$$

という同次方程式ができる．いま，

$$A := \begin{pmatrix} x_1^m & x_1^{m-1} & \cdots & 1 & -x_1^n & -x_1^{n-1} & \cdots & -x_1 \\ x_2^m & x_2^{m-1} & \cdots & 1 & -x_2^n & -x_2^{n-1} & \cdots & -x_2 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ x_M^m & x_M^{m-1} & \cdots & 1 & -x_M^n & -x_M^{n-1} & \cdots & -x_M \end{pmatrix}$$

$$B := (r_1, r_2, \cdots, r_{m+n+1})^T$$

$$C := (a_m, a_{m-1}, \cdots, a_0, b_n, b_{n-1}, \cdots, b_1)$$

とする．このとき，$AC = B$ を解くことにより有理関数補間の係数が決定する．$p(x)$ と $q(x)$ の GCD の次数 k は，A のランクを s とすると，$k = m + n + 1 - s$ である．これより，分子が $m - k$ 次，分母が $n - k$ 次の有理関数補間を求め，除算により近似 GCD を得ることができる．

つまり次のような方法で，近似 GCD を求める．

入力: $p(x)$, $q(x)$, ϵ

出力: $p(x)$ と $q(x)$ の精度 ϵ での近似 GCD

方法:

1. 行列 A を作り，A の特異値分解を行う．特異値が ϵ 以下となる部分を 0 とみなし，近似的なランク s を決定する．
2. 分子が $m - k$ 次，分母が $n - k$ 次として，$\tilde{p}(x)$ と $\tilde{q}(x)$ を求める．
3. $p(x)/\tilde{p}(x)$ を求める．

この提案法で 2 節の例を 10^{-3} の精度で解くと，

$$\tilde{g}(x) = 1.000 \times 10^{-10} x^3 + 2.000 \times 10^{-10} x^2 - 1.000x + 5.000$$

となり，桁落ちがほとんど起きない．従来の方法と異なり，多項式の係数を直接用いないため，微小主係数の問題は起こりにくいと考えられる．

参考文献

[1] D. A. Bini and P. Boito: Structured Matrix-Based Methods for Polynomial ϵ-gcd: Analysis and Comparisons, Proceedings of the 2007 International Symposium on Symbolic and Algebraic Computation, pp.9-16, 2007.

[2] H. Kai and M. T. Noda: Approximate-GCD and Pade' Approximation, Proceedings of Asian Symposium on Computer Mathematics, pp.81-89, 1995.

[3] V. Y. Pan: Computation of Approximate Polynomial GCDs and an Extension, Information and Computation Volume 167, Issue 2, pp. 71-85, 2001.

[4] T. Sasaki and M. T. Noda: Approximate Square-free Decomposition and Root-finding of Ill-conditioned Algebraic Equations, Journal of Information Processing, Volume 12, No. 2, pp.159-168, 1989.

[5] Z. Zeng: The approximate GCD of inexact polynomials. Part I: a univariate algorithm. To appear.

[6] Z. Zeng: http://www.neiu.edu/~zzeng/apatools.htm (ApaTools - A software toolbox for Approximate Polynomial Algebra)