数理解析研究所講究録
第1652巻 2009年 63-70



# Ruppert行列による近似GCDの算出

長坂耕作
KOSAKU NAGASAKA
神戸大学人間発達環境学研究科
GRADUATE SCHOOL OF HUMAN DEVELOPMENT AND ENVIRONMENT, KOBE UNIVERSITY*

## 1 はじめに

本講演では，Ruppert行列を用いて一変数多項式のGCD(最大公約因子)を求めることが可能[6]との結果を受け，実際にRuppert行列で近似GCDを計算し，従来の方法との比較を行った．結論から言えば，求めることは確かに可能であるが，近似GCDの計算を従来の方法ではなく，Ruppert行列を使って計算することに利点はないことが実験で確認できた．

**定義 1 (近似 GCD)**
$n = \deg(u)$, $m = \deg(v)$ なる $u(x)$, $v(x) \in \mathbb{Z}[x]$ と $\varepsilon(\in \mathbb{R}_{>0}) \ll 1$ に対して，$g(x) \in \mathbb{Z}[x]$ が次式を満たす $\hat{u}(x)$, $\hat{v}(x) \in \mathbb{Z}[x]$ を割り切るとき，$g(x)$ は $u(x)$ と $v(x)$ の *$\varepsilon$-divisor* という．このとき，次数最大の $u(x)$ と $v(x)$ の *$\varepsilon$-divisor* を *$\varepsilon$-gcd(近似 GCD)* という．

$$\| \hat{u}(x) - u(x) \| \leq \varepsilon \| u(x) \|, \ \deg(\hat{u}) \leq n, \ \| \hat{v}(x) - v(x) \| \leq \varepsilon \| v(x) \|, \ \deg(\hat{v}) \leq m$$

なお，$\| \cdot \|$ は任意のノルムを表す． ◁

**例 1 (近似 GCD の例)**
次の $u(x)$ と $v(x)$ の *$\varepsilon$-gcd* は，$1.0006x + 1.0001$ となる ( 近似 *GCD* は複数存在することに注意 ).

$$u(x) = 1.0001x^3 - 0.0003x^2 + 0.001x + 0.9999, \ v(x) = 0.9999x^3 + 3.0001x^2 + 3.0001x + 1.0001$$

◁

## 2 QR分解による近似GCDの復習

近似GCDについては多くの研究 (例えば，[1, 2, 9] など) が行われており，その方法も唯一ではないが，ここではQR分解による近似GCD算法[2]について簡単に述べておく．Corlessらのアルゴリズムの基本は，Sylvester行列のQR分解とGCDの関係を用いている．参考のため，$u(x) = u_n x^n + u_{n-1} x^{n-1} + \cdots + u_1 x + u_0$, $v(x) = v_m x^m + v_{m-1} x^{m-1} + \cdots + v_1 x + v_0$ としたときの，$u(x)$ と $v(x)$ の Sylvester 行列 $\mathrm{Syl}(u, v)$ を以下に示す．

*nagasaka@main.h.kobe-u.ac.jp

$$\mathrm{Syl}(u,v)=\begin{pmatrix} u_n & u_{n-1} & \cdots & u_1 & u_0 & 0 & \cdots & 0 \\ 0 & u_n & u_{n-1} & \cdots & u_1 & u_0 & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & \cdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & u_n & u_{n-1} & \cdots & u_1 & u_0 \\ v_m & v_{m-1} & \cdots & v_1 & v_0 & 0 & \cdots & 0 \\ 0 & v_m & v_{m-1} & \cdots & v_1 & v_0 & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & \cdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & v_m & v_{m-1} & \cdots & v_1 & v_0 \end{pmatrix}$$

Sylvester 行列の QR 分解による近似 GCD の計算は，$\mathrm{Syl}(u,x)=QR$ と分解されたときに，$R$ のゼロベクトルでない最後の行ベクトルが，$u(x)$ と $v(x)$ の GCD の係数ベクトルになるという良く知られている性質に基づいている．これに関する証明は古くから与えられている [8, 4]．この性質を用いた，Corless らのアルゴリズム [2] の概要を下記に示す．なお，$\|\cdot\|$ は 2-norm を表す．

**アルゴリズム 1 (Corless らのアルゴリズム [2])**
(*Step 1*) 初期化

*1-1.* $u(x)$ と $v(x)$ の *2-norm* を正規化，主係数を正に．

(*Step 2*) *QR* 分解

*2-1.* $\mathrm{Syl}(u,v)$ の構成と $\mathrm{Syl}(u,v)=QR$ の計算．

*2-2.* $R=\begin{pmatrix} R_{11} & R_{12} \\ R_{21} & R_{22}^{(k)} \end{pmatrix}$ と 4 つの部分行列に分割する．
ただし，$R_{22}^{(k)}$ は $(k+1)\times(k+1)$ 行列で，$\| R_{22}^{(k)} \| > \varepsilon$ かつ $\| R_{22}^{(k-1)} \| < \varepsilon$ を満たすものとする．

*2-3.* $\| R_{22}^{(k_1)} \| / \| R_{22}^{(k_1-1)} \| > 0.1/\varepsilon$ なる最大の $k_1$ に対し，$\| R_{22}^{(k_1)} \|$ の最初の行から多項式 $d_1(x)$ を構成．

(*Step 3*) 確認

*3-1.* $d_1(x)$ に関する余因子 $u_1(x)$ と $v_1(x)$ の計算．

*3-2.* $x^{\deg(u_1)}u_1(x^{-1})$ と $x^{\deg(v_1)}v_1(x^{-1})$ に対して同じ操作を行うことで $d_2(x)$ を計算．

$d(x)=d_1(x)d_2(x)$ が近似 *GCD*. ◁

## 3 Ruppert 行列の復習

二変数あるいはそれ以上の変数を持つ多項式の近似因数分解で利用される Ruppert 行列とは，次の Ruppert による既約判定法で使われる偏微分方程式を線形化した際に表れる係数行列を指す．

**定理 2 (Ruppert, W.M., 1999)**
$f(x,y)\in\mathbb{C}[x,y]$ が絶対既約であることと，次の微分方程式が自明でない解 $g(x,y),h(x,y)\in\mathbb{C}[x,y]$ を持たないことは同値である．

$$f\frac{\partial g}{\partial y}-g\frac{\partial f}{\partial y}+h\frac{\partial f}{\partial x}-f\frac{\partial h}{\partial x}=0,$$

$$\deg_x g \leq \deg_x f - 1,\ \deg_y g \leq \deg_y f,\ \deg_x h \leq \deg_x f,\ \deg_y h \leq \deg_y f - 2.$$

◁

具体的には，この偏微分方程式から $g(x,y)$ と $h(x,y)$ の係数を未知数とする線形方程式を作り，その係数行列を Ruppert 行列 $R(f)$ とおく．ここで，$n = \deg_x(f)$ かつ $m = \deg_y(f)$ とすれば，Ruppert 行列 $R(f)$ のサイズは，$(4nm) \times (2nm + m - 1)$ となる．なお，この定理の拡張としては，解 $g(x,y)$ と $h(x,y)$ に対する次数上限を Newton polytope で与えるもの [3]，多変数多項式に対応させたもの [5] がある．

# 4 Ruppert 行列と GCD の関係についての復習

$u(x)$ と $v(x)$ が互いに素であることと，$f_0(x) = u(x), f_1(x) = v(x)$ としたときの $f(x,y) = f_0(x) + f_1(x)y$ が絶対既約であることの同値性を用いて，Ruppert 行列と一変数多項式の GCD の関係が導き出されている [6]．これについて簡単に復習しておく．

**補題 3 (Lemma 1 in [6])**
多項式 $f_0(x)$ と $f_1(x)$ に対して，$f_0(x)$ と $f_1(x)$ の *Sylvester* 行列と $f(x,y) = f_0(x) + f_1(x)y$ の *Ruppert* 行列は，*GCD* の計算に必要な同じ情報を含んでいる．ただし，*Ruppert* 行列は *Ruppert* オリジナルの微分方程式と次数条件によるものとする．

◁

**例 2 (Sylvester 行列と Ruppert 行列)**
$f_0(x) = \sum_{i=0}^{5} a_i x^i$ と $f_1(x) = \sum_{i=0}^{5} b_i x^i$ の *Sylvester* 行列 $\mathrm{Syl}(f_0, f_1)$ と *Ruppert* 行列 $R(f)$ を示す．

$$\mathrm{Syl}(f_0, f_1) = \begin{pmatrix}
a_5 & a_4 & a_3 & a_2 & a_1 & a_0 & 0 & 0 & 0 & 0 \\
0 & a_5 & a_4 & a_3 & a_2 & a_1 & a_0 & 0 & 0 & 0 \\
0 & 0 & a_5 & a_4 & a_3 & a_2 & a_1 & a_0 & 0 & 0 \\
0 & 0 & 0 & a_5 & a_4 & a_3 & a_2 & a_1 & a_0 & 0 \\
0 & 0 & 0 & 0 & a_5 & a_4 & a_3 & a_2 & a_1 & a_0 \\
b_5 & b_4 & b_3 & b_2 & b_1 & b_0 & 0 & 0 & 0 & 0 \\
0 & b_5 & b_4 & b_3 & b_2 & b_1 & b_0 & 0 & 0 & 0 \\
0 & 0 & b_5 & b_4 & b_3 & b_2 & b_1 & b_0 & 0 & 0 \\
0 & 0 & 0 & b_5 & b_4 & b_3 & b_2 & b_1 & b_0 & 0 \\
0 & 0 & 0 & 0 & b_5 & b_4 & b_3 & b_2 & b_1 & b_0
\end{pmatrix}$$

$$R(f) = \begin{pmatrix}
0 & a_5 & 0 & a_4 & 0 & a_3 & 0 & a_2 & 0 & a_1 & 0 & a_0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & -b_5 & 0 & -b_4 & 0 & -b_3 & 0 & -b_2 & 0 & -b_1 & 0 & -b_0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & a_5 & 0 & a_4 & 0 & a_3 & 0 & a_2 & 0 & a_1 & 0 & a_0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & -b_5 & 0 & -b_4 & 0 & -b_3 & 0 & -b_2 & 0 & -b_1 & 0 & -b_0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & a_5 & 0 & a_4 & 0 & a_3 & 0 & a_2 & 0 & a_1 & 0 & a_0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & -b_5 & 0 & -b_4 & 0 & -b_3 & 0 & -b_2 & 0 & -b_1 & 0 & -b_0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & a_5 & 0 & a_4 & 0 & a_3 & 0 & a_2 & 0 & a_1 & 0 & a_0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & -b_5 & 0 & -b_4 & 0 & -b_3 & 0 & -b_2 & 0 & -b_1 & 0 & -b_0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & a_5 & 0 & a_4 & 0 & a_3 & 0 & a_2 & 0 & a_1 & 0 & a_0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -b_5 & 0 & -b_4 & 0 & -b_3 & 0 & -b_2 & 0 & -b_1 & 0 & -b_0
\end{pmatrix}$$

◁

**定理 4 (Theorem 1 in [6])**
$f_0(x)$ と $f_1(x)$ の *GCD* は，$f(x,y)$ が $\mathbb{C}(y)$ 上で無平方ならば，$f(x,y) = f_0(x) + f_1(x)y$ の *Ruppert* 行列の特異値分解で計算可能．ただし，*Ruppert* 行列は *May* による多変数版の微分方程式と次数条件 *[5]* によるものとする (*Ruppert* と *May* の微分方程式と次数条件の違いは，変数 $x$ と $y$ の役割が入れ替わっているだけである )． ◁

**定理 5 (Theorem 2 in [6])**
$f_0(x)$ と $f_1(x)$ の *GCD* は，$f(x,y) = f_0(x) + f_1(x)y$ の *Ruppert* 行列の最後の $3n_0$ 行の転置行列の *QR* 分解で計算可能．三角行列 $R$ のゼロベクトルでない最後の行ベクトルが *GCD* の係数ベクトルとなる．ただし，*Ruppert* 行列は *May* による多変数版の微分方程式と次数条件 *[5]* によるものとし，$n_0 = \deg(f_0)$ とする． ◁

**例 3 (May の方法による Ruppert 行列)**
$f_0(x) = \sum_{i=0}^{5} a_i x^i$ と $f_1(x) = \sum_{i=0}^{5} b_i x^i$ の *May* による微分方程式を使った *Ruppert* 行列 $R(f)$ を示す．なお，行列中の横線よりも下部が $3n_0$ 行 (= 15 行 ) となっている．

$$R(f) = \left(\begin{array}{cccccccccccccc}
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
-b_4 & b_5 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
-2b_3 & 0 & 2b_5 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
-3b_2 & -b_3 & b_4 & 3b_5 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
-4b_1 & -2b_2 & 0 & 2b_4 & 4b_5 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
\hline
-5b_0 & -3b_1 & -b_2 & b_3 & 3b_4 & 5b_5 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & -4b_0 & -2b_1 & 0 & 2b_3 & 4b_4 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & -3b_0 & -b_1 & b_2 & 3b_3 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & -2b_0 & 0 & 2b_2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & -b_0 & b_1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
-a_4 & a_5 & 0 & 0 & 0 & 0 & -a_5 & 0 & 0 & 0 & b_5 & 0 & 0 & 0 \\
-2a_3 & 0 & 2a_5 & 0 & 0 & 0 & -a_4 & -a_5 & 0 & 0 & b_4 & b_5 & 0 & 0 \\
-3a_2 & -a_3 & a_4 & 3a_5 & 0 & 0 & -a_3 & -a_4 & -a_5 & 0 & b_3 & b_4 & b_5 & 0 \\
-4a_1 & -2a_2 & 0 & 2a_4 & 4a_5 & 0 & -a_2 & -a_3 & -a_4 & -a_5 & b_2 & b_3 & b_4 & b_5 \\
-5a_0 & -3a_1 & -a_2 & a_3 & 3a_4 & 5a_5 & -a_1 & -a_2 & -a_3 & -a_4 & b_1 & b_2 & b_3 & b_4 \\
0 & -4a_0 & -2a_1 & 0 & 2a_3 & 4a_4 & -a_0 & -a_1 & -a_2 & -a_3 & b_0 & b_1 & b_2 & b_3 \\
0 & 0 & -3a_0 & -a_1 & a_2 & 3a_3 & 0 & -a_0 & -a_1 & -a_2 & 0 & b_0 & b_1 & b_2 \\
0 & 0 & 0 & -2a_0 & 0 & 2a_2 & 0 & 0 & -a_0 & -a_1 & 0 & 0 & b_0 & b_1 \\
0 & 0 & 0 & 0 & -a_0 & a_1 & 0 & 0 & 0 & -a_0 & 0 & 0 & 0 & b_0
\end{array}\right)$$

◁

## 5 Sylvester 行列と Ruppert 行列の QR 分解の比較

Corless らの論文 [2] で使われている次の多項式 $f_0(x)$ と $f_1(x)$ に対して，Sylvester 行列と Ruppert 行列の QR 分解による近似 GCD の計算を行い，結果を比較する．なお，実際に使用した多項式は，展開後の各係数を倍精度に変換したものである．

$$\begin{aligned}
f_0(x) &= (x-5)\left(x-\tfrac{1}{2}\right)\left(56x^8+83x^7+91x^4-92x^2+93x-91\right) \\
f_1(x) &= (x-5)\left(x-\tfrac{1}{2}\right)\left(32x^8-37x^6+93x^5+58x^4+90x^2+53\right)
\end{aligned}$$

それぞれの QR 分解で得られた三角行列 $R$ の右下の部分のみを引用する.

Sylvester 行列

$$\begin{pmatrix} 0. & 0.0250173 & -0.137596 & 0.0625434 \\ 0. & 0. & 5.74888\times10^{-6} & -2.87444\times10^{-6} \\ 0. & 0. & 0. & 2.20675\times10^{-17} \end{pmatrix}$$

$$\gcd(f_0,f_1) = 0.0250173x^2 - 0.137596x + 0.0625434 \approx (x-0.5)(x-5.00001)$$

Ruppert 行列

$$\begin{pmatrix} -0.0249898 & 0.147421 & -0.117346 & 0.0249417 \\ 0. & 0.0250112 & -0.137562 & 0.0625284 \\ 0. & 0. & -1.14565\times10^{-6} & 5.72827\times10^{-7} \end{pmatrix}$$

$$\gcd(f_0,f_1) = 0.0250112x^2 - 0.137562x + 0.0625284 \approx (x-0.5)(x-5.00002)$$

この結果を見てわかるように, Sylvester 行列の方が良い結果になっている. また, 特異値分解などで GCD の次数が判明している場合などは, QR 分解を行う行列を, 終結式に対応する Sylvester 行列でなく, 部分終結式に対応するよりサイズの小さい行列を使うことが多い. そこで, サイズを落とした Sylvester 行列に対しても計算した結果を以下に示す.

Sylvester 行列 (1 サイズダウン)

$$\begin{pmatrix} -0.0249898 & 0.147421 & -0.117346 & 0.0249417 \\ 0. & 0.0250112 & -0.137562 & 0.0625284 \\ 0. & 0. & -1.14565\times10^{-6} & 5.72827\times10^{-7} \end{pmatrix}$$

$$\gcd(f_0,f_1) = 0.0250112x^2 - 0.137562x + 0.0625284 \approx (x-0.5)(x-5.00002)$$

Sylvester 行列 (2 サイズダウン)

$$\begin{pmatrix} 0.0237317 & -0.143672 & 0.131644 & -0.0328705 \\ 0. & -0.0220921 & 0.121507 & -0.0552304 \end{pmatrix}$$

$$\gcd(f_0,f_1) = -0.0220921x^2 + 0.121507x - 0.0552304 \approx (x-0.5)(x-5.00001)$$

## 6 Sylvester 行列と Ruppert 行列の特異値の比較

近似 GCD のアルゴリズムによっては, Sylvester 行列の特異値 (これを大きい順に $\sigma_1,\sigma_2,\ldots,\sigma_r$ とする) を計算し, 前後の特異値の比 $(\sigma_2/\sigma_1,\sigma_3/\sigma_2,\ldots,\sigma_r/\sigma_{r-1})$ の変化から近似 GCD の次数を推定することもある (比が大きく変化した部分に近似 GCD が存在する). そこで, 実際にランダムに生成した各 1000 個の多項式ペアに対して, Sylvester 行列と Ruppert 行列の特異値を計算し, 前後の特異値の比がどのような関係にあるかを実験した.

実験で使った 20 次の GCD を持つ 50 次の多項式ペアは, 各係数が区間 $[0,1]$ に収まるようランダムに生成した密な多項式を因子に持つ 50 次の多項式で, 10 次の因子 2 つの積を GCD に持ち, 30 次の GCD を持つ 100 次の多項式ペアは, 各係数が区間 $[0,1]$ に収まるようランダムに生成した密な多項式を因子に持つ 100 次の多項式で, 10 次の因子 3 つの積を GCD に持ち, 55 次の GCD を持つ 200 次の多項式ペアは, 各係数が区間 $[0,1]$ に収まるようランダムに生成した密な多項式を因子に持つ 200 次の多項式で, 1 次から 10 次までの因子 10 個の積を GCD に持ち, 10 次の GCD を持つ 200 次の多項式ペアは, 各係数が区間 $[0,1]$ に収まるようランダムに生成した密な多項式を因子に持つ 200 次の多項式で, 10 次の因子 1 つを GCD に持つ. どの多項式も有理係数として生成し, 因子の積を計算してから倍精度で係数を近似している.

それぞれの実験結果が，図 1, 2, 3, 4 である．図は全て常用対数グラフであり，縦軸は特異値の比 $(\sigma_i/\sigma_{i-1})$ の平均を表し，横軸は特異値の小さい順に各比を並べている．記号「S」は Sylvester 行列の結果を表し，記号「R」は Ruppert 行列の結果を表している．実験結果のどの図においても，もっとも下部に打たれている点は Sylvester 行列のものであり，Ruppert 行列よりも旧来の Sylvester 行列の方が優れていることがわかる．

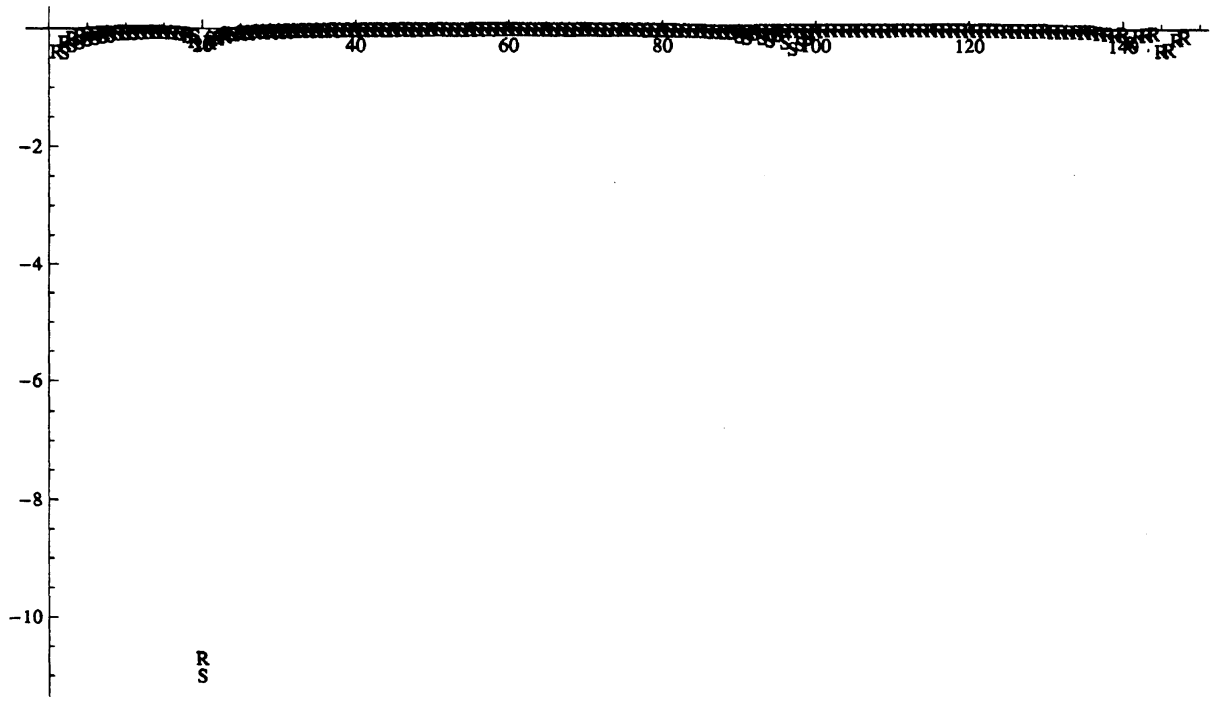


図 1: 20 次の GCD を持つ 50 次の多項式ペア

## 7 まとめ

本講演では，Sylvester 行列の QR 分解を用いる近似 GCD アルゴリズムを取り上げ，その Sylvester 行列を Ruppert 行列で代替した場合の数値実験を行った．結果は，Ruppert 行列と一変数多項式の GCD の関係を明らかにした論文 [6] でも示唆されていたように，旧来の Sylvester 行列を用いた方が良いことが実験からも判明した．

## 参 考 文 献

[1] D. A. Bini and P. Boito. Structured Matrix-Based Methods for Polynomial $\varepsilon$-gcd: Analysis and Comparisons. *Proceedings of the 2007 International Symposium on Symbolic and Algebraic Computation, ISSAC 2007.* 2007, 17–24.

[2] R. M. Corless, S. M. Watt and L. Zhi. *QR* factoring to compute the GCD of univariate approximate polynomials. *IEEE Trans. Signal Process.*, **52**(12). 2004, 3394–3402.

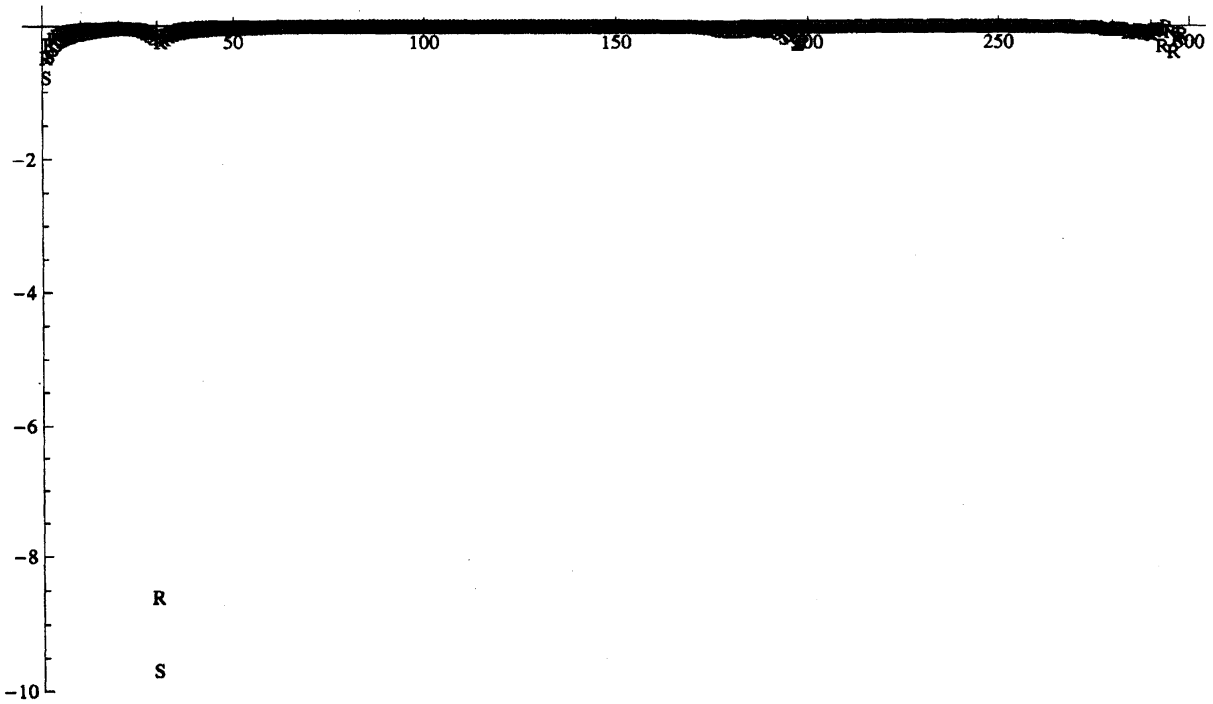


図 2: 30 次の GCD を持つ 100 次の多項式ペア

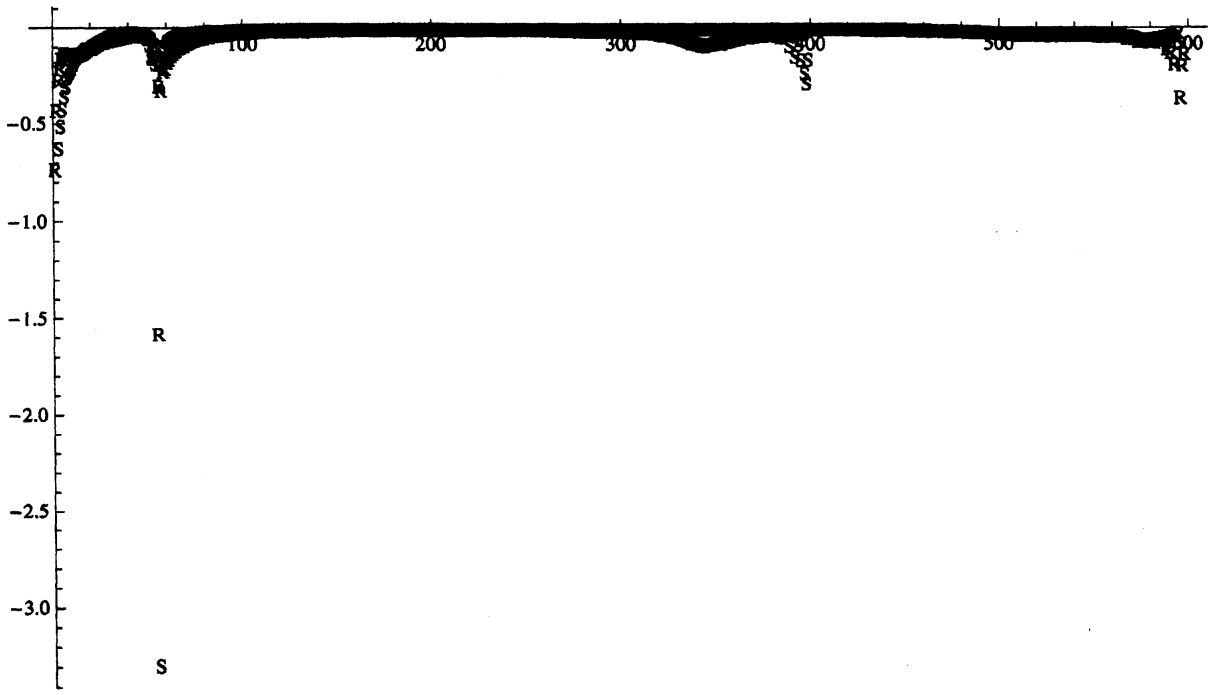


図 3: 55 次の GCD を持つ 200 次の多項式ペア

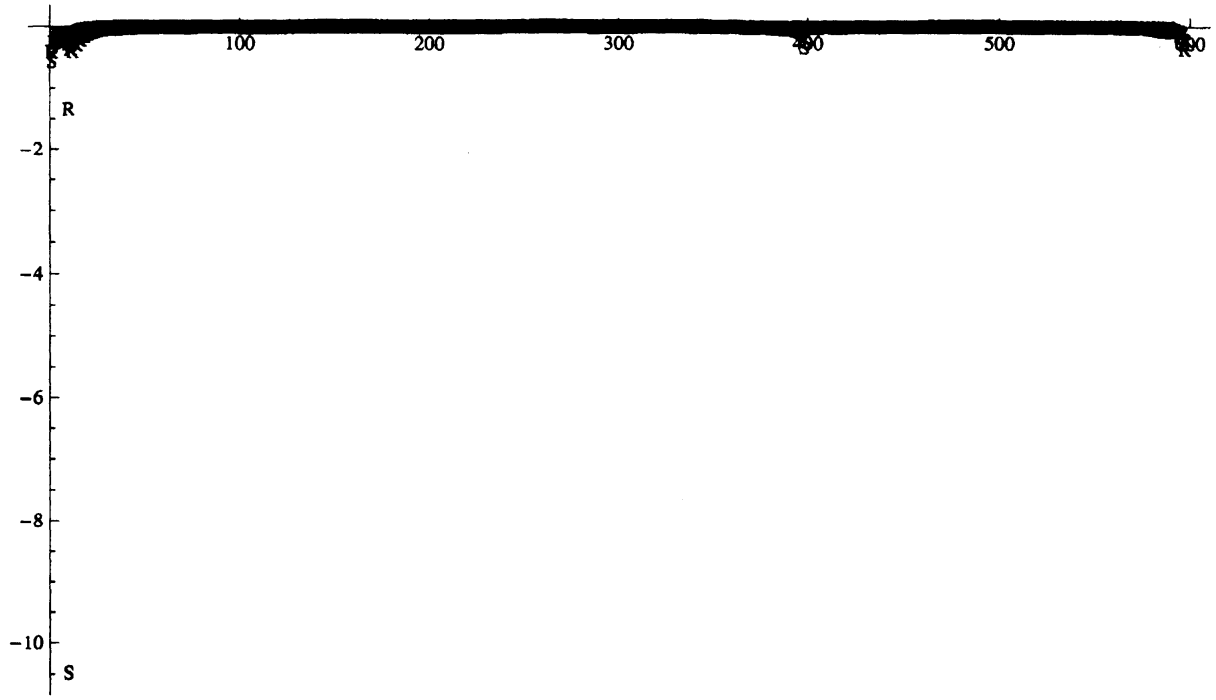


図 4: 10 次の GCD を持つ 200 次の多項式ペア

[3] S. Gao and V. M. Rodrigues. Irreducibility of polynomials modulo p via newton polytopes. *J. Number Theory*, **101**. 2003, 32–47.

[4] M. A. Laidacker. Another theorem relating Sylvester's matrix and the greatest common divisor. *Math. Mag.*, **42**. 1969, 126–128.

[5] J. P. May. Approximate Factorization of Polynomials in Many Variables and Other Problems in Approximate Algebra via Singular Value Decomposition Methods. *PhD thesis*, North Carolina State Univ., Raleigh, North Carolina. 2005, 84 pages.

[6] K. Nagasaka. Ruppert matrix as subresultant mapping. *Lecture Notes in Computer Science*, **4770**. *Computer Algebra in Scientific Computing: 10th International Workshop, CASC 2007*. 2007, 316–327.

[7] W. M. Ruppert. Reducibility of polynomials $f(x, y)$ modulo $p$. *J. Number Theory*, **77**. 1999, 62–70.

[8] J. M. Thomas. Differential Systems. *AMS Colloquium Publications* **XXI**, AMS. 1937.

[9] Z. Zeng. The approximate GCD of inexact polynomials. Part I: a univariate algorithm. *Preprint*. 2004, 8 pages.