Ruppert matrix as subresultant mapping

Kosaku Nagasaka
Kobe University
JAPAN

This presentation is powered by *Mathematica* 6.

Outline of this talk

- **How to compute polynomial GCDs**
- **Sylvester matrix and Subresultant mapping**
- **Ruppert matrix and factoring polynomials**
- **Ruppert matrix for GCD of two polynomials**
- **Ruppert matrix for GCD of several polynomials**
- **Conclusion**

How to compute polynomial GCDs

Euclidean Algorithm

Eculidean algorithm for polynomials $f(x)$ and $g(x)$ over reals.

```
function GCD(f(x), g(x))
  if  g(x) = 0  return  f(x)
  else  return  GCD( g(x),  remainder  of  f(x)  by  g(x) )
```

QR factoring of Sylvester matrix

The usual subresultant mapping is important. See the next slide...

Lots of other powerful approximate algorithms

QR factoring of Sylvester matrix

Sylvester matrix of the following $f(x)$ and $g(x)$:
$f(x) = f_n x^n + f_{n-1} x^{n-1} + \cdots + f_1 x + f_0,$
$g(x) = g_m x^m + g_{m-1} x^{m-1} + \cdots + g_1 x + g_0.$

$$\mathrm{Syl}(f, g) = \begin{pmatrix} f_n & f_{n-1} & \cdots & f_1 & f_0 & 0 & \cdots & 0 \\ 0 & f_n & f_{n-1} & \cdots & f_1 & f_0 & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & \cdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & f_n & f_{n-1} & \cdots & f_1 & f_0 \\ g_m & g_{m-1} & \cdots & g_1 & g_0 & 0 & \cdots & 0 \\ 0 & g_m & g_{m-1} & \cdots & g_1 & g_0 & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & \cdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & g_m & g_{m-1} & \cdots & g_1 & g_0 \end{pmatrix}.$$

Well known relation between GCD and QR factoring of Sylvester matrix.

The last non-zero row vector of R where $\mathrm{Syl}(f, g) = Q\,R$,
is the coefficient vector of GCD of $f(x)$ and $g(x)$.
(See: Laidacker, M.A. , 1969 and others)

Subresultant mapping

Subresultant mapping S_r of $f_0(x)$ and $f_1(x)$

$$S_r : \begin{cases} \mathcal{P}_{n_1-r-1} \times \mathcal{P}_{n_0-r-1} & \longrightarrow & \mathcal{P}_{n_0+n_1-r-1} \\ (u_0,\ u_1) & \longmapsto & u_1\, f_0 + u_0\, f_1 \end{cases}$$

where $\begin{cases} f_0(x) = f_{0,n_0}\, x^{n_0} + \cdots + f_{0,1}\, x + f_{0,0} \\ f_1(x) = f_{1,n_1}\, x^{n_1} + \cdots + f_{1,1}\, x + f_{1,0} \end{cases}$

- **Sylvester subresultant matrix $S_r(f_0, f_1)$**

$$S_r(f_0,\ f_1) = \left(C_{n_0-r}(f_1) \quad C_{n_1-r}(f_0) \right)$$

where $C_k(p)$ is a k-th convolution matrix of $p(x)$
and $S_0(f_0,\ f_1)$ is the transpose of Sylvester matrix of $f_0(x)$ and $f_1(x)$.

Convolution matrix

k-th convolution matrix of polynomial $p(x)$.

$$C_k(p) = \begin{pmatrix} p_n & 0 & \cdots & 0 & 0 \\ p_{n-1} & p_n & \ddots & \vdots & \vdots \\ \vdots & p_{n-1} & \ddots & 0 & \vdots \\ p_0 & \vdots & \ddots & p_n & 0 \\ 0 & p_0 & \ddots & p_{n-1} & p_n \\ \vdots & 0 & \ddots & \vdots & p_{n-1} \\ \vdots & \vdots & \ddots & p_0 & \vdots \\ 0 & 0 & \cdots & 0 & p_0 \end{pmatrix}$$

where $p(x) = p_n x^n + \cdots + p_1 x + p_0$.

Subresultant mapping and Sylvester matrix

$$S_r : \begin{cases} \mathcal{P}_{n_1-r-1} \times \mathcal{P}_{n_0-r-1} & \longrightarrow & \mathcal{P}_{n_0+n_1-r-1} \\ (u_0, u_1) & \longmapsto & u_1 f_0 + u_0 f_1 \end{cases}$$

$$S_r(f_0, f_1) = \begin{pmatrix} C_{n_0-r}(f_1) & C_{n_1-r}(f_0) \end{pmatrix}, \quad S_0(f_0, f_1) = {}^t\mathrm{Syl}(f_0, f_1)$$

Subresultant mapping and GCD

Well known fact (see Rupprecht, D. (1999) and so on)

(1) If r is the largest integer that
the subresultant mapping S_r is not injective,
we can compute the GCD of $f_0(x)$ and $f_1(x)$ from
the right null vector of $S_r(f_0, f_1)$.

(2) The dimension of the null space is
the degree of the polynomial GCD.

Ruppert criterion

- **Reducibility of bivariate polynomials (Ruppert, W.M., 1999)**

$f(x, y)$ is absolutely irreducible
$\Longleftrightarrow$ the following differential equation
does not have any non-trivial solutions $g(x, y)$ and $h(x, y)$.

$$f \frac{\partial g}{\partial y} - g \frac{\partial f}{\partial y} + h \frac{\partial f}{\partial x} - f \frac{\partial h}{\partial x} = 0, \quad g, h \in \mathbb{C}[x, y]$$

with degree constraints:

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

- **Newton polytope ver. by Gao, S. and Rodrigues, V.M. (2003)**
- **Multivariate version by May, J.P. (2005)**

Ruppert matrix $R(f)$

- **The differential equation w.r.t. $g(x, y)$ and $h(x, y)$ $\Longrightarrow$ a linear equation w.r.t. unknown coefficients.**

$$f \frac{\partial g}{\partial y} - g \frac{\partial f}{\partial y} + h \frac{\partial f}{\partial x} - f \frac{\partial h}{\partial x} = 0, \; g, h \in \mathbb{C}[x, y],$$

$$\deg_x g \leq \deg_x f - 1, \; \deg_y g \leq \deg_y f,$$

$$\deg_x h \leq \deg_x f, \; \deg_y h \leq \deg_y f - 2$$

$$R(f)^t(\text{ coefficient vectors of } g, h) = \emptyset$$

- **SVD of Ruppert matrix: irreducibility radius.**
- **Ruppert matrix depends term orders: lexicographic in this talk.**

Factoring with Ruppert and Gao's matrix

■ Known Algorithms using Corollary 1

Corollary 1

For a given $f(x, y) \in \mathbb{C}[x, y]$ that is square-free over $\mathbb{C}(y)$, the dimension (over $\mathbb{C}$) of the null space of $R(f)$ is equal to "(the number of absolutely irreducible factors of $f(x, y)$ over $\mathbb{C}$) -1".

and others by Kaltofen, Gao and so on.

■ Correction: Corollary 1 from `John May's thesis.`

Kaltofen, E., May, J., Yang, Z., and Zhi, L.
Approximate factorization of multivariate polynomials using singular value decomposition. Manuscript, 22 pages. Submitted, Jan. 2006.

Purpose of this talk

GCD and Factorization

Primitive operations in Symbolic (and Numeric) computations.

Common Properties

Can be computed by some matrix decompositions.

Sylvester and Ruppert matices

Is there any relation between them?

How to link them

$f(x, y) = f_0(x) + f_1(x)\, y$

- $f(x, y)$ is reducible if $f_0(x)$ and $f_1(x)$ have a non-trivial GCD.
- $f(x, y)$ is irreducible if they don't have any non-trivial GCD.

Coprimeness of $f_0(x)$ and $f_1(x)$ can be tested
by a rank deficiency of their Sylvester matrix.

Irreducibility of $f(x, y) = f_0(x) + f_1(x)\, y$ can be tested
by a rank deficiency of its Ruppert matrix.

Simple Result

Lemma 1

For any polynomials $f_0(x)$ and $f_1(x)$,
the Sylvester matrix of $f_0(x)$ and $f_1(x)$
and the Ruppert matrix of $f(x, y) = f_0(x) + f_1(x)\,y$
have the same information for computing their GCD,
with the Ruppert's original differential equation and degree constraints.

The proof is in the proceedings.

Simple Result (Sylvester and Ruppert)

$$\begin{pmatrix}
fa5 & fa4 & fa3 & fa2 & fa1 & fa0 & 0 & 0 & 0 & 0 \\
0 & fa5 & fa4 & fa3 & fa2 & fa1 & fa0 & 0 & 0 & 0 \\
0 & 0 & fa5 & fa4 & fa3 & fa2 & fa1 & fa0 & 0 & 0 \\
0 & 0 & 0 & fa5 & fa4 & fa3 & fa2 & fa1 & fa0 & 0 \\
0 & 0 & 0 & 0 & fa5 & fa4 & fa3 & fa2 & fa1 & fa0 \\
fb5 & fb4 & fb3 & fb2 & fb1 & fb0 & 0 & 0 & 0 & 0 \\
0 & fb5 & fb4 & fb3 & fb2 & fb1 & fb0 & 0 & 0 & 0 \\
0 & 0 & fb5 & fb4 & fb3 & fb2 & fb1 & fb0 & 0 & 0 \\
0 & 0 & 0 & fb5 & fb4 & fb3 & fb2 & fb1 & fb0 & 0 \\
0 & 0 & 0 & 0 & fb5 & fb4 & fb3 & fb2 & fb1 & fb0
\end{pmatrix}$$

$$\begin{pmatrix}
0 & fa5 & 0 & fa4 & 0 & fa3 & 0 & fa2 & 0 & fa1 & 0 & fa0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & -fb5 & 0 & -fb4 & 0 & -fb3 & 0 & -fb2 & 0 & -fb1 & 0 & -fb0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & fa5 & 0 & fa4 & 0 & fa3 & 0 & fa2 & 0 & fa1 & 0 & fa0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & -fb5 & 0 & -fb4 & 0 & -fb3 & 0 & -fb2 & 0 & -fb1 & 0 & -fb0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & fa5 & 0 & fa4 & 0 & fa3 & 0 & fa2 & 0 & fa1 & 0 & fa0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & -fb5 & 0 & -fb4 & 0 & -fb3 & 0 & -fb2 & 0 & -fb1 & 0 & -fb0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & fa5 & 0 & fa4 & 0 & fa3 & 0 & fa2 & 0 & fa1 & 0 & fa0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & -fb5 & 0 & -fb4 & 0 & -fb3 & 0 & -fb2 & 0 & -fb1 & 0 & -fb0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & fa5 & 0 & fa4 & 0 & fa3 & 0 & fa2 & 0 & fa1 & 0 & fa0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -fb5 & 0 & -fb4 & 0 & -fb3 & 0 & -fb2 & 0 & -fb1 & 0 & -fb0
\end{pmatrix}$$

09 : 29 : 36 (16) – Ruppert matrix as subresultant mapping – [Prev⟸] [⟹Next]

Alternative Result 1

Theorem 1

The polynomial GCD of $f_0(x)$ and $f_1(x)$ can be computed by Singular Value Decomposition (SVD) of Ruppert matrix of $f(x, y) = f_0(x) + f_1(x)\, y$ with the J.P.May's differential equation and degree constraints, if $f(x, y)$ is square-free over $\mathbb{C}(y)$.

The proof is in the proceedings.

■ Difference between Ruppert and May's

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

$$g \le \deg_x f - 1, \ \deg_y g \le \deg_y f,$$

$$h \le \deg_x f, \ \deg_y h \le \deg_y f - 2$$

Alternative Result 1(Ruppert with May)

$$
\left(\begin{array}{cccccccccccccc}
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
-fb4 & fb5 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
-2\,fb3 & 0 & 2\,fb5 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
-3\,fb2 & -fb3 & fb4 & 3\,fb5 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
-4\,fb1 & -2\,fb2 & 0 & 2\,fb4 & 4\,fb5 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
-5\,fb0 & -3\,fb1 & -fb2 & fb3 & 3\,fb4 & 5\,fb5 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & -4\,fb0 & -2\,fb1 & 0 & 2\,fb3 & 4\,fb4 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & -3\,fb0 & -fb1 & fb2 & 3\,fb3 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & -2\,fb0 & 0 & 2\,fb2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & -fb0 & fb1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
-fa4 & fa5 & 0 & 0 & 0 & 0 & -fa5 & 0 & 0 & 0 & fb5 & 0 & 0 & 0 \\
-2\,fa3 & 0 & 2\,fa5 & 0 & 0 & 0 & -fa4 & -fa5 & 0 & 0 & fb4 & fb5 & 0 & 0 \\
-3\,fa2 & -fa3 & fa4 & 3\,fa5 & 0 & 0 & -fa3 & -fa4 & -fa5 & 0 & fb3 & fb4 & fb5 & 0 \\
-4\,fa1 & -2\,fa2 & 0 & 2\,fa4 & 4\,fa5 & 0 & -fa2 & -fa3 & -fa4 & -fa5 & fb2 & fb3 & fb4 & fb5 \\
-5\,fa0 & -3\,fa1 & -fa2 & fa3 & 3\,fa4 & 5\,fa5 & -fa1 & -fa2 & -fa3 & -fa4 & fb1 & fb2 & fb3 & fb4 \\
0 & -4\,fa0 & -2\,fa1 & 0 & 2\,fa3 & 4\,fa4 & -fa0 & -fa1 & -fa2 & -fa3 & fb0 & fb1 & fb2 & fb3 \\
0 & 0 & -3\,fa0 & -fa1 & fa2 & 3\,fa3 & 0 & -fa0 & -fa1 & -fa2 & 0 & fb0 & fb1 & fb2 \\
0 & 0 & 0 & -2\,fa0 & 0 & 2\,fa2 & 0 & 0 & -fa0 & -fa1 & 0 & 0 & fb0 & fb1 \\
0 & 0 & 0 & 0 & -fa0 & fa1 & 0 & 0 & 0 & -fa0 & 0 & 0 & 0 & fb0
\end{array}\right)
$$

Alternative Result 2

Theorem 2

The polynomial GCD of $f_0(x)$ and $f_1(x)$ can be computed by QR factoring of the transpose of the last $3\,n_0$ rows of their Ruppert matrix $R(f) = R(f_0(x) + f_1(x)\,y)$ with J.P.May's equation.

The last non-zero row vector of the triangular matrix is the coefficient vector of their polynomial GCD.

The proof is in the proceedings.

Alternative Result 2(Last $3n_0$ rows)

$$
\begin{pmatrix}
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
-fb4 & fb5 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
-2\,fb3 & 0 & 2\,fb5 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
-3\,fb2 & -fb3 & fb4 & 3\,fb5 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
-4\,fb1 & -2\,fb2 & 0 & 2\,fb4 & 4\,fb5 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
-5\,fb0 & -3\,fb1 & -fb2 & fb3 & 3\,fb4 & 5\,fb5 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & -4\,fb0 & -2\,fb1 & 0 & 2\,fb3 & 4\,fb4 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & -3\,fb0 & -fb1 & fb2 & 3\,fb3 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & -2\,fb0 & 0 & 2\,fb2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & -fb0 & fb1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
-fa4 & fa5 & 0 & 0 & 0 & 0 & -fa5 & 0 & 0 & 0 & fb5 & 0 & 0 & 0 \\
-2\,fa3 & 0 & 2\,fa5 & 0 & 0 & 0 & -fa4 & -fa5 & 0 & 0 & fb4 & fb5 & 0 & 0 \\
-3\,fa2 & -fa3 & fa4 & 3\,fa5 & 0 & 0 & -fa3 & -fa4 & -fa5 & 0 & fb3 & fb4 & fb5 & 0 \\
-4\,fa1 & -2\,fa2 & 0 & 2\,fa4 & 4\,fa5 & 0 & -fa2 & -fa3 & -fa4 & -fa5 & fb2 & fb3 & fb4 & fb5 \\
-5\,fa0 & -3\,fa1 & -fa2 & fa3 & 3\,fa4 & 5\,fa5 & -fa1 & -fa2 & -fa3 & -fa4 & fb1 & fb2 & fb3 & fb4 \\
0 & -4\,fa0 & -2\,fa1 & 0 & 2\,fa3 & 4\,fa4 & -fa0 & -fa1 & -fa2 & -fa3 & fb0 & fb1 & fb2 & fb3 \\
0 & 0 & -3\,fa0 & -fa1 & fa2 & 3\,fa3 & 0 & -fa0 & -fa1 & -fa2 & 0 & fb0 & fb1 & fb2 \\
0 & 0 & 0 & -2\,fa0 & 0 & 2\,fa2 & 0 & 0 & -fa0 & -fa1 & 0 & 0 & fb0 & fb1 \\
0 & 0 & 0 & 0 & -fa0 & fa1 & 0 & 0 & 0 & -fa0 & 0 & 0 & 0 & fb0
\end{pmatrix}
$$

Generalized Sylvester matrix

Generalized Subresultant mapping S_r of $f_0(x), \ldots, f_k(x)$.

$$S_r : \left\{ \begin{array}{ccc} \prod_{i=0}^{k} \mathcal{P}_{n_i - r - 1} & \longrightarrow & \prod_{i=1}^{k} \mathcal{P}_{n_0 + n_i - r - 1} \\ \begin{pmatrix} u_0 \\ \vdots \\ u_k \end{pmatrix} & \longmapsto & \begin{pmatrix} u_1\, f_0 + u_0\, f_1 \\ \vdots \\ u_k\, f_0 + u_0\, f_k \end{pmatrix} \end{array} \right., \; n_i = \deg_x f_i(x)$$

Generalized Sylvester matrix $S_r(f_0, \ldots, f_k)$.

$$S_r(f_0, \ldots, f_k) = \begin{pmatrix} C_{n_0 - r}(f_1) & C_{n_1 - r}(f_0) & \emptyset & \cdots & \emptyset \\ C_{n_0 - r}(f_2) & \emptyset & C_{n_2 - r}(f_0) & \ddots & \vdots \\ \vdots & & \ddots & \ddots & \emptyset \\ C_{n_0 - r}(f_k) & \emptyset & \cdots & \emptyset & C_{n_k - r}(f_0) \end{pmatrix}$$

(see Rupprecht, D. (1999) and so on)

If r is the largest integer that the subresultant mapping S_r is not injective, we can compute the GCD of $f_0(x), \ldots, f_k(x)$ from the right null vector of $S_r(f_0, \ldots, f_k)$.

How to link them

$f(x, \mathbb{y}) = f_0(x) + f_1(x)\, y_1 + \cdots + f_k(x)\, y_k$

- $f(x, \mathbb{y})$ is reducible if $f_0(x), \ldots, f_k(x)$ have a non-trivial GCD.
- $f(x, \mathbb{y})$ is irreducible if they don't have any non-trivial GCD.

Coprimeness of $f_0(x), \ldots, f_k(x)$ can be tested
by a rank deficiency of their Sylvester matrix.

Irreducibility of $f(x, \mathbb{y}) = f_0(x) + \sum_{i=1}^{k} f_i(x)\, y_i$ can be tested
by a rank deficiency of its Ruppert matrix.

Relation for several polynomials

- **Postponed as a future work:**

J.P.May's differential equation becomes

$$\begin{cases} f_0\, g_i - g_0\, f_i + \lambda_i\left(f_i\, f_0' - f_0\, f_i'\right) = 0 \\ f_1\, g_i - g_1\, f_i + \lambda_i\left(f_i\, f_1' - f_1\, f_i'\right) = 0 \\ \qquad\qquad \vdots \\ f_k\, g_i - g_k\, f_i + \lambda_i\left(f_i\, f_k' - f_k\, f_i'\right) = 0 \end{cases} \quad (i = 1, \ldots, k)$$

This means that

$$\begin{cases} u_0(x) = g_0(x) - \lambda_i\, f_0' \\ u_i(x) = -g_i(x) + \lambda_i\, f_i' \end{cases} \quad (i = 1, \ldots, k)$$

$\Longrightarrow$ will be a part of proof of several polynomial version of theorem.

Conclusion

- **Sylvester and Ruppert matrices**

  have some relations for computing GCDs.

- **Their relations lead to**

  no algorithm which computes GCDs efficiently.

- **The author hopes that**

  the relations in this talk will make some progress.

Thank you ! !