Ruppert Matrix as Subresultant Mapping

Nagasaka, Kosaku

(Citation)
Lecture Notes in Computer Science,4770:316-327

(Issue Date)
2007

(Resource Type)
journal article

(Version)
Accepted Manuscript

(URL)
https://hdl.handle.net/20.500.14094/90001898

Ruppert Matrix as Subresultant mapping

Kosaku Nagasaka

Kobe University, Japan
nagasaka@main.h.kobe-u.ac.jp

Abstract. Ruppert and Sylvester matrices are very common for computing irreducible factors of bivariate polynomials and computing polynomial greatest common divisors, respectively. Since Ruppert matrix comes from Ruppert criterion for bivariate polynomial irreducibility testing and Sylvester matrix comes from the usual subresultant mapping, they are used for different purposes and their relations have not been focused yet. In this paper, we show some relations between Ruppert and Sylvester matrices as the usual subresultant mapping for computing (exact/approximate) polynomial GCDs, using Ruppert matrices.

1 Introduction

Computing irreducible factors and greatest common divisors is the most popular arithmetic for symbolic algebraic computations. In fact, there are lots of studies for exact factorization ([1],[2],[3],[4] and more), approximate factorization ([5], [6] and more), polynomial GCD ([7], [8], [9] and more) and approximate GCD ([10], [11], [12] and more). For computing GCDs, the Sylvester matrix or its variants play important roles in most of the algorithms. The structure, properties and useful lemmas related to Sylvester matrix are widely known and well published. For computing irreducible factors, there are several approaches but their basic ideas have the common idea: converting the problem to linear equations. Such linear systems form Berlekamp, Niederreiter and Ruppert matrices for example. Hence, such structured matrices are very important for symbolic computations and studying those matrices is one of interesting topics: Lee and Vanstone [13] show Berlekamp and Niederreiter subspaces and their relation, the structure of Ruppert matrix is given by Nagasaka [14] and the displacement structure of Sylvester matrix for computing approximate GCD is studied by Zhi [15].

In this paper, we show some relations between Ruppert and Sylvester matrices as the usual subresultant mapping for computing (exact/approximate) polynomial GCDs via Ruppert matrix.

1.1 Notations and Sylvester Matrix

In this paper, $P(f)$ denotes the Newton polytope of the support of polynomial f. $\mathcal{P}_k$ denotes the set of polynomials of degree k. Φ_{k_1,k_2} $(k_1 \leq k_2)$ is the natural injection from $\mathbb{C}^{k_1 \times 1}$ to $\mathbb{C}^{k_2 \times 1}$ such that $\Phi_{k_1,k_2}(\boldsymbol{a}) = {}^t(b_1 \cdots b_{k_2-k_1} a_1 \cdots a_{k_1})$ where $\boldsymbol{b} = {}^t(b_i)$ is the $(k_2 - k_1)$-dimensional zero vector and $\boldsymbol{a} = {}^t(a_i)$. For

polynomial $f(x, y_1, \ldots, y_m)$, we abbreviate it to $f(x, \boldsymbol{y})$. The range of matrix $A = (\boldsymbol{a}_1 \cdots \boldsymbol{a}_m)$ where $\boldsymbol{a}_i$s are k-dimensional column vectors, is defined as $\mathrm{range}(A) = \{A\boldsymbol{b} \mid \boldsymbol{b} \in \mathbb{C}^{k\times 1}\}$. We consider about polynomial GCDs of the following polynomials $f_0(x)$, $f_1(x)$, $\cdots$, $f_k(x)$.

$$\begin{aligned} f_0(x) &= f_{0,n_0}x^{n_0} + \cdots + f_{0,1}x + f_{0,0}, \\ f_1(x) &= f_{1,n_1}x^{n_1} + \cdots + f_{1,1}x + f_{1,0}, \\ &\vdots \\ f_k(x) &= f_{k,n_k}x^{n_k} + \cdots + f_{k,1}x + f_{k,0}. \end{aligned} \tag{1.1}$$

We assume that $n_i \geq n_{i+1}$ and $f_{i,n_i} \neq 0$.

$C_k(p)$ denotes the following convolution matrix of polynomial $p(x)$, of size $(n+k) \times k$.

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

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

Let S_r be the following subresultant mapping.

$$S_r : \begin{cases} \mathcal{P}_{n_1-r-1} \times \mathcal{P}_{n_0-r-1} \to \mathcal{P}_{n_0+n_1-r-1}, \\ (u_0, u_1) \mapsto u_1 f_0 + u_0 f_1. \end{cases} \tag{1.2}$$

where $\mathcal{P}_k$ denotes the set of univariate polynomials of degree k. This mapping can be expressed by the following Sylvester subresultant matrix $S_r(f_0, f_1)$.

$$S_r(f_0, f_1) = \begin{pmatrix} C_{n_0-r}(f_1) & C_{n_1-r}(f_0) \end{pmatrix}.$$

We note a well known fact: if r is the largest integer that S_r is not injective, we can compute the greatest common divisor of $f_0(x)$ and $f_1(x)$ from the right null vector of $S_r(f_0, f_1)$ (see the proof in Rupprecht [16] and so on). Moreover, the greatest common divisor also can be computed by QR-decomposition of $S_0(f_0, f_1)$ (see the proof in [8, 9] and so on): the last non-zero row vector of the upper triangular matrix is the coefficient vector of the polynomial GCD of f_0 and f_1. $S_0(f_0, f_1)$ also has another useful property that the dimension of the null space is the degree of the polynomial GCD.

1.2 Ruppert Matrix

Ruppert matrix is the coefficient matrix of the corresponding linear equation of the following absolute irreducibility criterion due to Ruppert [17] (Gao and

Rodrigues [18] studied the sparse polynomial version of this criterion).

$$f\frac{\partial g}{\partial y} - g\frac{\partial f}{\partial y} + h\frac{\partial f}{\partial x} - f\frac{\partial h}{\partial x} = 0, \quad g, h \in \mathbb{C}[x, y], \tag{1.3}$$

$$\begin{aligned} &\deg_x g \leq \deg_x f - 1, \ \deg_y g \leq \deg_y f, \\ &\deg_x h \leq \deg_x f, \qquad \deg_y h \leq \deg_y f - 2. \end{aligned}$$

The criterion is that $f(x, y)$ is absolutely irreducible if and only if this differential equation does not have any non-trivial solutions. The matrix is useful for computing irreducible factors [6, 1] and the irreducibility radius [19, 14, 20]. Since Ruppert matrix is the set of coefficient vectors w.r.t. unknowns of g and h, matrices by different term orders are not the same. For the Ruppert matrix of f, we use the lexicographic order of x, y and $x, y_1, \ldots, y_m$, as in Nagasaka [14, 20], and by $R(f)$ we denote the Ruppert matrix of polynomial f.

For multivariate polynomials, May [21] studied the generalized version of the Ruppert criterion, with the following differential equation and degree constraints.

$$f\frac{\partial g}{\partial y_i} - g\frac{\partial f}{\partial y_i} + h_i\frac{\partial f}{\partial x} - f\frac{\partial h_i}{\partial x} = 0, \quad g, h \in \mathbb{C}[x, y_1, \cdots, y_m], \tag{1.4}$$

$$\begin{aligned} &\deg_x g \leq \deg_x f - 2, \ \ \deg_{y_i} g \leq \deg_{y_i} f, \\ &\deg_x h_i \leq \deg_x f, \ \ \deg_{y_j} h_i \leq \begin{cases} \deg_{y_j} f & i \neq j \\ \deg_{y_j} f - 1 & i = j \end{cases} \end{aligned}$$

May [21] also studied the generalized Ruppert criterion with degree bounds via Newton polytopes as follows.

$$P(xg) \subseteq P(f) \text{ and } P(y_i h_i) \subseteq P(f). \tag{1.5}$$

The generalized two criteria have the same argument that the given polynomial $f(x, \boldsymbol{y})$ is absolutely irreducible if and only if this differential equation does not have any non-trivial solutions. For these criteria, we can also construct the coefficient matrix of the corresponding linear system, with the lexicographic order of $x, y_1, \ldots, y_m$.

2 GCD of two polynomials

In this section, we consider the subresultant mapping of two polynomials via Ruppert matrix. We define the following polynomial $f(x, y)$.

$$f(x, y) = f_0(x) + f_1(x)y. \tag{2.1}$$

It is obvious that $f(x, y)$ is reducible if and only if $f_0(x)$ and $f_1(x)$ have a non-trivial GCD. This means that we can check whether $f_0(x)$ and $f_1(x)$ have a non-trivial GCD or not via the differential equation (1.3) of the Ruppert criterion, with $f(x, y) = f_0(x) + f_1(x)y$. We note that $f_1(x) + f_0(x)y$ can be used instead of $f_0(x) + f_1(x)y$ for our purpose, since the degree constraints of Ruppert criterion are given by each variables separately.

2.1 Case 1-1: Simple Result

Substituting degrees of $f(x,y)$ for that of f in (1.3), we have

$$f\frac{\partial g}{\partial y} - g\frac{\partial f}{\partial y} = 0, \quad g \in \mathbb{C}[x,y], \quad \deg_x g \leq n_0 - 1, \ \deg_y g \leq 1. \tag{2.2}$$

Let $g(x,y)$ be the following polynomial satisfying (2.2).

$$g(x,y) = g_0(x) + g_1(x)y.$$

Substituting $g(x,y)$ for g in (2.2), we have

$$(f_0(x) + f_1(x)y)g_1(x) - (g_0(x) + g_1(x)y)f_1(x) = 0.$$

Collecting terms with respect to y, we have

$$g_1(x)f_0(x) - g_0(x)f_1(x) = 0. \tag{2.3}$$

This equations can be represented as a linear equation w.r.t. coefficients of polynomials $g(x,y)$. The coefficient matrix is the Ruppert matrix of $f(x,y)$ and its structure is given by Nagasaka [14]. Moreover, the structure of this matrix is the Sylvester matrix $S_0(f_0, -f_1)$ since the degree constraints of $u_i(x)$ and $g_i(x)$ are the same if $n_0 = n_1$. For $n_0 > n_1$, the Ruppert matrix has extra column vectors that are not included in the Sylvester matrix, hence we have $\Phi_{n_0+n_1,2n_0}(\mathrm{range}(S_0(f_0,f_1))) \subset \mathrm{range}(R(f))$. By comparing between the both sides of (2.3), degrees of $\deg(g_1f_0)$ and $\deg(g_0f_1)$ must be the same. Therefore, we have the following lemma.

Lemma 1. *For any polynomials $f_0(x)$ and $f_1(x)$, the Sylvester matrix and the Ruppert matrix of $f_0(x)$ and $f_1(x)$ have the same information for computing their GCD, with the Ruppert's original differential equation and constraints.* ◁

2.2 Case 1-2: Alternative Result

The degree bounds of the differential equation (1.3) are not the same as the following general version of the Ruppert criterion by John May [21] for bivariate polynomials , though the difference is only the roles of variables and not essential.

$$f\frac{\partial g}{\partial y} - g\frac{\partial f}{\partial y} + h\frac{\partial f}{\partial x} - f\frac{\partial h}{\partial x} = 0, \quad g,h \in \mathbb{C}[x,y], \tag{2.4}$$

$$\begin{aligned} &\deg_x g \leq \deg_x f - 2, \ \deg_y g \leq \deg_y f, \\ &\deg_x h \leq \deg_x f, \qquad \deg_y h \leq \deg_y f - 1. \end{aligned} \tag{2.5}$$

We have the following corollary (see [21] or [6]).

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 over $\mathbb{C}$) $-$ 1 ".*

Substituting degrees of $f(x,y)$ for that of f in (2.4), we have

$$f\frac{\partial g}{\partial y} - g\frac{\partial f}{\partial y} + h\frac{\partial f}{\partial x} - f\frac{\partial h}{\partial x} = 0, \quad g, h \in \mathbb{C}[x,y], \tag{2.6}$$

$$\deg_x g \le n_0 - 2,\ \deg_y g \le 1,\ \deg_x h \le n_0,\ \deg_y h \le 0.$$

Let $g(x,y)$ and $h(x,y)$ be the following polynomials satisfying (2.6).

$$g(x,y) = g_0(x) + g_1(x)y, \quad h(x,y) = h_0(x).$$

Substituting $g(x,y)$ and $h(x,y)$ for g and h, respectively, in (2.6), we have

$$\begin{array}{l}(f_0(x) + f_1(x)y)g_1(x) - (g_0(x) + g_1(x)y)f_1(x)\\ +h_0(x)(\frac{\partial f_0(x)}{\partial x} + \frac{\partial f_1(x)}{\partial x}y) - (f_0(x) + f_1(x)y)\frac{\partial h_0(x)}{\partial x} = 0.\end{array}$$

Collecting terms with respect to y, we have

$$g_1(x)f_0(x) - g_0(x)f_1(x) + h_0(x)\frac{\partial f_0(x)}{\partial x} - f_0(x)\frac{\partial h_0(x)}{\partial x} = 0, \tag{2.7}$$

$$h_0(x)\frac{\partial f_1(x)}{\partial x} - f_1(x)\frac{\partial h_0(x)}{\partial x} = 0. \tag{2.8}$$

This is not as same as the subresultant mapping in the previous subsection and is not reduces to the usual subresultant mapping (2.3).

Lemma 2. *For any polynomials $u_1(x) \in \mathcal{P}_{n_1-1}$ and $u_0(x) \in \mathcal{P}_{n_0-1}$ satisfying $\deg(u_1f_0 + u_0f_1) < n_0 + n_1 - 1$, there exist polynomials $g_0(x)$, $g_1(x)$ and $h_0(x)$ satisfying their degree constraints, the equation (2.8) and $g_1f_0 - g_0f_1 - f_0\frac{\partial h_0}{\partial x} + h_0\frac{\partial f_0}{\partial x} = u_1f_0 + u_0f_1$.* ◁

Proof. If $\deg(u_1) \le n_1 - 2 \le n_0 - 2$ and $\deg(u_0) \le n_0 - 2$, the lemma follows from (2.7) and (2.8), with $g_0(x) = -u_0(x)$, $g_1(x) = u_1(x)$ and $h_0(x) = 0$. We suppose that $\deg(u_1) = n_1 - 1$ and $\deg(u_0) = n_0 - 1$ since the leading coefficients of u_1f_0 and u_0f_1 must be canceled. We put $u_0(x) = \sum_{i=0}^{n_0-1} u_{0,i}x^i$ and $u_1(x) = \sum_{i=0}^{n_1-1} u_{1,i}x^i$, and transform $u_1f_0 + u_0f_1$ as follows.

$$\begin{array}{rl}u_1f_0 + u_0f_1 = & (u_1 - u_{1,n_0-1}x^{n_0-1})f_0 - (-u_0 + u_{0,n_0-1}x^{n_0-1})f_1\\ & +u_{1,n_0-1}x^{n_0-1}f_0 + u_{0,n_0-1}x^{n_0-1}f_1\\ = & (u_1 - u_{1,n_0-1}x^{n_0-1} + \frac{u_{0,n_0-1}}{n_0f_{0,n_0}}(f_1 - f_{1,n_0}x^{n_0})')f_0\\ & -(-u_0 + u_{0,n_0-1}x^{n_0-1} + \frac{u_{0,n_0-1}}{n_0f_{0,n_0}}(f_0 - f_{0,n_0}x^{n_0})')f_1\\ & +u_{1,n_0-1}x^{n_0-1}f_0 + u_{0,n_0-1}x^{n_0-1}f_1\\ & -\frac{u_{0,n_0-1}}{n_0f_{0,n_0}}(f_1 - f_{1,n_0}x^{n_0})'f_0 + \frac{u_{0,n_0-1}}{n_0f_{0,n_0}}(f_0 - f_{0,n_0}x^{n_0})'f_1\\ = & (u_1 - u_{1,n_0-1}x^{n_0-1} + \frac{u_{0,n_0-1}}{n_0f_{0,n_0}}(f_1 - f_{1,n_0}x^{n_0})')f_0\\ & -(-u_0 + u_{0,n_0-1}x^{n_0-1} + \frac{u_{0,n_0-1}}{n_0f_{0,n_0}}(f_0 - f_{0,n_0}x^{n_0})')f_1\\ & -\frac{u_{0,n_0-1}}{n_0f_{0,n_0}}f_1'f_0 + \frac{u_{0,n_0-1}}{n_0f_{0,n_0}}f_0'f_1 + (u_{1,n_0-1} + u_{0,n_0-1}\frac{f_{1,n_0}}{f_{0,n_0}})x^{n_0-1}f_0,\end{array}$$

where $f' = \frac{\partial f}{\partial x}$. If $n_0 = n_1$, we have $u_{1,n_0-1} + u_{0,n_0-1}\frac{f_{1,n_0}}{f_{0,n_0}} = 0$ since the leading coefficients of $u_1 f_0 + u_0 f_1$ must be canceled. For $n_0 > n_1$, we also have $u_{1,n_0-1} + u_{0,n_0-1}\frac{f_{1,n_0}}{f_{0,n_0}} = 0$ since $u_{1,n_0-1} = f_{1,n_0} = 0$. Therefore, the following $g_0(x)$, $g_1(x)$ and $h_0(x)$ prove the lemma.

$$
\begin{aligned}
g_0(x) &= -(u_0(x) - u_{0,n_0-1}x^{n_0-1}) + \tfrac{u_{0,n_0-1}}{n_0 f_{0,n_0}}(f_0 - f_{0,n_0}x^{n_0})' \\
g_1(x) &= (u_1(x) - u_{1,n_0-1}x^{n_0-1}) + \tfrac{u_{0,n_0-1}}{n_0 f_{0,n_0}}(f_1 - f_{1,n_0}x^{n_0})' \\
h_0(x) &= \tfrac{u_{0,n_0-1}}{n_0 f_{0,n_0}} f_1.
\end{aligned}
$$

□

Lemma 3. *For any polynomials $g_0(x)$, $g_1(x)$ and $h_0(x)$ satisfying their degree constraints and the equations (2.7) and (2.8), there exist polynomials $u_1(x) \in \mathcal{P}_{n_1-1}$ and $u_0(x) \in \mathcal{P}_{n_0-1}$ satisfying $u_1 f_0 + u_0 f_1 = g_1 f_0 - g_0 f_1 - f_0\frac{\partial h_0}{\partial x} + h_0\frac{\partial f_0}{\partial x}$, if $f(x,y) = f_0(x) + f_1(x)y$ is square-free over $\mathbb{C}(y)$.* ◁

Proof. Let $g_0(x)$, $g_1(x)$ and $h_0(x)$ be a solution of (2.7) and (2.8) with $f(x,y) = f_0(x) + f_1(x)y$. By the lemma 3.1 in John May [21] (or see [6]), we have

$$h_0(x) = \lambda f_1(x) \text{ with } \lambda \in \mathbb{C}.$$

If $n_1 \leq \deg(g_1) \leq n_0 - 2$, we have $\deg(g_1 f_0) \leq n_0 + n_1 - 1$ since $\max\{\deg(g_0 f_1), \deg(f_0 f_1'), \deg(f_1 f_0')\} = n_0 + n_1 - 1$. However, $\deg(g_1 f_0) \leq n_0 + n_1 - 1$ contradicts $n_1 \leq \deg(g_1)$. Hence, we have $\deg(g_1) \leq n_1 - 1$ and the following polynomials $u_0(x)$ and $u_1(x)$ prove the lemma.

$$u_0(x) = -g_0(x) + \lambda\frac{\partial f_0(x)}{\partial x}, \quad u_1(x) = g_1(x) - \lambda\frac{\partial f_1(x)}{\partial x}.$$

□

The following theorem follows from the above lemmas, directly.

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 $f(x,y) = f_0(x) + f_1(x)y$ in (2.4), if $f(x,y)$ is square-free over $\mathbb{C}(y)$.* ◁

For computing polynomial GCDs, one of well known methods is computing the QR decomposition of the Sylvester matrix of $f_0(x)$ and $f_1(x)$ as in [8], [9] and so on. In the below, we show that we can compute polynomial GCDs by the QR decomposition of the Ruppert matrix of $f(x,y) = f_0(x) + f_1(x)y$. The figure 1 illustrates the structure of the Ruppert matrix of $f(x,y) = f_0(x) + f_1(x)y$, as in Nagasaka [14]. The size of this matrix is $(4n_0) \times (3n_0 - 1)$.

Lemma 4. *The range (and the span of column vectors) of the Ruppert matrix of $f(x,y)$ includes the descending coefficient vector (its constant term is the last element) of $n_0(f_{0,n_0}f_1(x) - f_{1,n_0}f_0(x))x^{n_0-1}$.* ◁

Fig. 1. Ruppert matrix $R(f) = R(f_0(x) + f_1(x)y)$

$$R(f) = \begin{pmatrix} R_{1,1} & \mathbf{0} \\ R_{2,1} & R_{2,2} \end{pmatrix}, \quad R_{2,2} = \begin{pmatrix} -f_{0,n_0} & & 0 & f_{1,n_0} & & 0 \\ -f_{0,n_0-1} & \ddots & & f_{1,n_0-1} & \ddots & \\ \vdots & \ddots & -f_{0,n_0} & \vdots & \ddots & f_{1,n_0} \\ \vdots & \ddots & -f_{0,n_0-1} & \vdots & \ddots & f_{1,n_0-1} \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ -f_{0,1} & \ddots & \vdots & f_{1,1} & \ddots & \vdots \\ -f_{0,0} & \ddots & \vdots & f_{1,0} & \ddots & \vdots \\ & \ddots & -f_{0,1} & & \ddots & f_{1,1} \\ 0 & & -f_{0,0} & 0 & & f_{1,0} \end{pmatrix},$$

$$R_{1,1} = \begin{pmatrix} 0 & 0 & \cdots & 0 & 0 & 0 \\ f_{1,n_0-1} & -f_{1,n_0} & \ddots & \vdots & \vdots & 0 \\ 2f_{1,n_0-2} & 0 & \ddots & 0 & \vdots & \vdots \\ \vdots & f_{1,n_0-2} & \ddots & (2-n_0)\, f_{1,n_0} & 0 & \vdots \\ \vdots & \vdots & \ddots & \vdots & (1-n_0)\, f_{1,n_0} & 0 \\ n_0\, f_{1,0} & \vdots & \ddots & \vdots & \vdots & -n_0\, f_{1,n_0} \\ 0 & (n_0-1)\, f_{1,0} & \ddots & 0 & \vdots & \vdots \\ \vdots & 0 & \ddots & f_{1,1} & -f_{1,2} & \vdots \\ 0 & \vdots & \ddots & 2f_{1,0} & 0 & -2f_{1,2} \\ 0 & 0 & \cdots & 0 & f_{1,0} & -f_{1,1} \\ 0 & 0 & \cdots & 0 & 0 & 0 \end{pmatrix},$$

$$R_{2,1} = \begin{pmatrix} f_{0,n_0-1} & -f_{0,n_0} & \ddots & \vdots & \vdots & 0 \\ 2f_{0,n_0-2} & 0 & \ddots & 0 & \vdots & \vdots \\ \vdots & f_{0,n_0-2} & \ddots & (2-n_0)\, f_{0,n_0} & 0 & \vdots \\ \vdots & \vdots & \ddots & \vdots & (1-n_0)\, f_{0,n_0} & 0 \\ n_0\, f_{0,0} & \vdots & \ddots & \vdots & \vdots & -n_0\, f_{0,n_0} \\ 0 & (n_0-1)\, f_{0,0} & \ddots & 0 & \vdots & \vdots \\ \vdots & 0 & \ddots & f_{0,1} & -f_{0,2} & \vdots \\ 0 & \vdots & \ddots & 2f_{0,0} & 0 & -2f_{0,2} \\ 0 & 0 & \cdots & 0 & f_{0,0} & -f_{0,1} \end{pmatrix},$$

Proof. Put $R(f) = (\boldsymbol{r}_1, \cdots, \boldsymbol{r}_{3n_0-1})$ where $\boldsymbol{r}_i$ is $4n_0$ dimensional column vector. We note that lower $2n_0 - 1$ rows of $(\boldsymbol{r}_{n_0+2}, \cdots, \boldsymbol{r}_{3n_0-1})$ is the usual Sylvester subresultant matrix $S_1(f_1, -f_0)$. If we apply fraction-free column reductions to the first column $\boldsymbol{r}_1$ by $\boldsymbol{r}_2$, $\cdots$, $\boldsymbol{r}_{n_0+1}$, then the first column becomes

$$\bar{\boldsymbol{r}}_1 = \sum_{i=0}^{n_0} f_{1,n_0-i}\boldsymbol{r}_{i+1}.$$

Let $\hat{\boldsymbol{r}}$ be the following column vector.

$$\hat{\boldsymbol{r}} = \bar{\boldsymbol{r}}_1 + \sum_{i=0}^{n_0-2}(n_0-1-i)f_{1,n_0-1-i}\boldsymbol{r}_{n_0+2+i} + \sum_{i=0}^{n_0-2}(n_0-1-i)f_{0,n_0-1-i}\boldsymbol{r}_{2n_0+1}.$$

$\hat{\boldsymbol{r}}$ is the descending coefficient vector (its constant term is the last element) of $n_0(f_{0,n_0}f_1(x) - f_{1,n_0}f_0(x))x^{n_0-1}$. □

Theorem 2. *The polynomial GCD of $f_0(x)$ and $f_1(x)$ can be computed by applying the QR decomposition to the transpose of the last $3n_0$ rows of their Ruppert matrix $R(f) = R(f_0(x) + f_1(x)y)$. The last non-zero row vector of the triangular matrix is the coefficient vector of their polynomial GCD.* ◁

Proof. Let $\bar{R}$ be the transpose of the last $3n_0$ rows of their Ruppert matrix $R(f)$. As in the proof [8], the last non-zero row vector of the triangular matrix of the QR decomposition is the coefficient vector of the lowest degree non-constant polynomial of linear combinations of polynomials whose coefficient vectors are row vectors of $\bar{R}$. Hence, we show that the lowest degree non-constant polynomial is the polynomial GCD of $f_0(x)$ and $f_1(x)$.

The rank of the upper $(n_0+1) \times 3n_0$ submatrix is n_0 at least since its upper left $n_0 \times n_0$ submatrix is a triangular matrix and its diagonal elements are non-zero elements: $n_0 f_{1,0}, \ldots, 2f_{1,0}, f_{1,0}$. If the linear combination includes some of the first n_0 row vectors, the degree of the combination is larger than $2n_0$. Since $\bar{R}$ has row vectors whose corresponding degrees are less than or equal to $2n_0$, the lowest degree non-constant polynomial does not include the first n_0 rows.

However, as in the proof of the lemma 4, another row vector generated from the first n_0 rows, can be included in the linear combination for the lowest degree non-constant polynomial. Hence, we only have to prove that the lowest degree non-constant polynomial of linear combinations of polynomials whose coefficient vectors are row vectors of the following matrix $\hat{R}$ is the polynomial GCD of $f_0(x)$ and $f_1(x)$.

$$\hat{R} = \begin{pmatrix}
0 & \text{the coefficient vector of} & & & & n_0(f_{0,n_0}f_1(x) - f_{1,n_0}f_0(x))x^{n_0-1} & & & \\
0 & -f_{0,n_0} & -f_{0,n_0-1} & \cdots & \cdots & \cdots & -f_{0,1} & -f_{0,0} & 0 \\
\vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots \\
0 & \cdots & 0 & -f_{0,n_0} & -f_{0,n_0-1} & \cdots & \cdots & \cdots & -f_{0,1} & -f_{0,0} \\
0 & f_{1,n_0} & f_{1,n_0-1} & \cdots & \cdots & \cdots & f_{1,1} & f_{1,0} & & 0 \\
\vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \\
0 & \cdots & 0 & f_{1,n_0} & f_{1,n_0-1} & \cdots & \cdots & \cdots & f_{1,1} & f_{1,0}
\end{pmatrix}.$$

The last $2n_0 - 2$ rows form the usual Sylvester subresultant matrix $S_1(f_1, -f_0)$ whose range is the set of coefficient vectors of $u_1 f_0 + u_0 f_1$ where u_0 and u_1 are polynomials of degree $n_0 - 2$ at most, and this is enough to compute non-trivial GCDs of f_0 and f_1. Moreover, the first row of $\hat{R}$ is the $(n_1 - 1)$-th row reduced by the first row, of $S_0(f_1, -f_0)$. Therefore, the last non-zero row vector of the triangular matrix of the QR decomposition of $\hat{R}$ is that of $S_0(f_1, -f_0)$. □

We note that for practical computations of polynomial GCDs, we do not have to use the Ruppert or Sylvester matrices because the usual Sylvester subresultant matrix which is smaller, is enough for GCDs, especially for approximate GCDs.

3 GCD of several polynomials

In this section, we show brief overview of relations between Sylvester matrix and Ruppert matrix for several polynomials $f_0(x), \ldots, f_k(x)$. Basically, the relations are natural extensions of the results in the previous section.

3.1 Generalized Sylvester matrix for several polynomials

Let $\mathcal{S}_r$ be the following generalized subresultant mapping.

$$\mathcal{S}_r : \begin{cases} \prod_{i=0}^{k} \mathcal{P}_{n_i - r - 1} \to \prod_{i=1}^{k} \mathcal{P}_{n_0 - n_i - r - 1}, \\ \begin{pmatrix} u_0 \\ \vdots \\ u_k \end{pmatrix} \mapsto \begin{pmatrix} u_1 f_0 + u_0 f_1 \\ \vdots \\ u_k f_0 + u_0 f_k \end{pmatrix}. \end{cases} \tag{3.1}$$

This mapping can be expressed by the following Sylvester subresultant matrix $\mathcal{S}_r(f_0, \ldots, f_k)$.

$$\mathcal{S}_r(f_0, \ldots, f_k) = \begin{pmatrix} C_{n_0 - r}(f_1) & C_{n_1 - r}(f_0) & \mathbf{0} & \cdots & \mathbf{0} \\ C_{n_0 - r}(f_2) & \mathbf{0} & C_{n_2 - r}(f_0) & \cdots & \mathbf{0} \\ \vdots & & & \ddots & \vdots \\ C_{n_0 - r}(f_k) & \mathbf{0} & \cdots & \mathbf{0} & C_{n_k - r}(f_0) \end{pmatrix}.$$

We note a well known fact: if r is the largest integer that S_r is not injective, we can compute the greatest common divisor of $f_0(x)$, ..., $f_k(x)$ from the right null vector of $\mathcal{S}_r(f_0, \ldots, f_k)$ (see [16]).

3.2 Extension for several polynomials

Let $f(x, \boldsymbol{y})$ be the following polynomial.

$$f(x, \boldsymbol{y}) = f_0(x) + f_1(x) y_1 + \cdots + f_k(x) y_k. \tag{3.2}$$

This polynomial is irreducible if and only if the polynomials $f_0(x)$, $f_1(x)$, ..., $f_{k-1}(x)$ and $f_k(x)$ do not have any non-trivial GCD. As in the previous section, we can check whether $f_i(x)$ have a non-trivial GCD or not by the differential equation (1.4) of the generalized Ruppert criterion, with $f(x, \boldsymbol{y}) = f_0(x) + \sum_{j=1}^{k} f_j(x) y_j$. The degree constraints of (1.4) with $f(x, \boldsymbol{y})$ of (3.2), becomes

$$\deg_x g \leq n_0 - 2, \ \deg_{y_i} g \leq 1,$$
$$\deg_x h^{(i)} \leq n_0, \ \deg_{y_j} h^{(i)} \leq \begin{cases} 1 & i \neq j \\ 0 & i = j \end{cases}$$

In the previous section, we define $g(x, \boldsymbol{y})$ and $h^{(k)}(x, \boldsymbol{y})$ satisfying the following differential equation. However, the degree constraints are not by total-degrees so the number of possible terms increases exponentially.

$$f\frac{\partial g}{\partial y_i} - g\frac{\partial f}{\partial y_i} + h_i\frac{\partial f}{\partial x} - f\frac{\partial h_i}{\partial x} = 0. \tag{3.3}$$

Hence, we limit the solution polynomials $g(x, \boldsymbol{y})$ and $h^{(i)}(x, \boldsymbol{y})$ as follows.

$$g(x, \boldsymbol{y}) = g_0(x) + \sum_{j=1}^{k} g_j(x) y_j, \ \ h^{(1)}(x, \boldsymbol{y}) = h_0^{(1)}(x), \ \ \ldots, \ \ h^{(k)}(x, \boldsymbol{y}) = h_0^{(k)}(x).$$

We note that this limitation may be harmless since by the lemma 3.1 in John May [21] (or see [6]), we have

$$h_0^{(i)}(x) = \lambda_i f_i(x) \text{ with } \lambda_i \in \mathbb{C}.$$

Substituting the above $g(x, \boldsymbol{y})$ and $h^{(i)}(x, \boldsymbol{y})$ for g and h_i, respectively, in (3.3), we have

$$f(x, \boldsymbol{y}) g_i(x) - g(x, \boldsymbol{y}) f_i(x) + h_0^{(i)}(x)\frac{\partial f(x, \boldsymbol{y})}{\partial x} - f(x, \boldsymbol{y})\frac{\partial h_0^{(i)}(x)}{\partial x} = 0.$$

Collecting terms with respect to $\boldsymbol{y}$ and substituting $\lambda_i f_i(x)$, we have

$$\begin{cases} f_0 g_i - g_0 f_i + \lambda_i (f_i {f_0}' - f_0 {f_i}') = 0, \\ f_1 g_i - g_1 f_i + \lambda_i (f_i {f_1}' - f_1 {f_i}') = 0, \\ \qquad\qquad\qquad\qquad\qquad\qquad \vdots \\ f_k g_i - g_k f_i + \lambda_i (f_i {f_k}' - f_k {f_i}') = 0. \end{cases}$$

This system of equations is the system of equation (2.7) for all the combinations of $f_0, \ldots, f_k$ since the equation (2.8) with $f_0, \ldots, f_k$ is always satisfied by $h_0^{(i)}(x) = \lambda_i f_i(x)$. As in the proof of lemma 3, for the solution of the above system, there exist polynomials $u_i(x) \in \mathcal{P}_{n_i - 1}$ $(i = 0, \ldots, k)$:

$$\begin{cases} u_0(x) = g_0(x) - \lambda_0 {f_0}', \\ u_i(x) = -g_i(x) + \lambda_0 {f_i}' \ \ (i = 1, \ldots, k). \end{cases}$$

For the other lemma and theorem for two polynomials, the author thinks that the same relations are hold for several polynomials since the ranks of null spaces of Ruppert matrix and generalized Sylvester subresultant matrix are the same. However, these problems are postponed as a future work.

4 Conclusion

In this paper, we show some relations on Ruppert matrix and Sylvester matrix from the point of computing the greatest common divisors of two polynomials. Though no algorithm is present in this paper and does not compete with the finest recent algorithms for computing approximate GCDs, the author hopes that factoring polynomials and computing polynomial GCDs are the basics of symbolic computations, and revealing their relations will make some progress in the future.

References

1. Gao, S.: Factoring multivariate polynomials via partial differential equations. Math. Comp. **72** (2003) 801–822 (electronic)
2. Abu Salem, F., Gao, S., Lauder, A.G.B.: Factoring polynomials via polytopes. In: ISSAC 2004. ACM, New York (2004) 4–11
3. van Hoeij, M.: Factoring polynomials and the knapsack problem. J. Number Theory **95** (2002) 167–189
4. Chèze, G.: Absolute polynomial factorization in two variables and the knapsack problem. In: ISSAC 2004. ACM, New York (2004) 87–94
5. Sasaki, T.: Approximate multivariate polynomial factorization based on zero-sum relations. In: Proceedings of the 2001 International Symposium on Symbolic and Algebraic Computation, ISSAC 2001. (2001) 284–291
6. Gao, S., Kaltofen, E., May, J., Yang, Z., Zhi, L.: Approximate factorization of multivariate polynomials via differential equations. In: Proceedings of the 2004 International Symposium on Symbolic and Algebraic Computation, ISSAC 2004. (2004) 167–174
7. Cheng, H., Labahn, G.: On computing polynomial gcds in alternate bases. In: ISSAC '06: Proceedings of the 2006 international symposium on Symbolic and algebraic computation, New York, NY, USA, ACM Press (2006) 47–54
8. Laidacker, M.A.: Another theorem relating Sylvester's matrix and the greatest common divisor. Math. Mag. **42** (1969) 126–128
9. Corless, R.M., Watt, S.M., Zhi, L.: QR factoring to compute the GCD of univariate approximate polynomials. IEEE Trans. Signal Process. **52** (2004) 3394–3402
10. Zeng, Z., Dayton, B.H.: The approximate GCD of inexact polynomials. II. A multivariate algorithm. In: ISSAC 2004. ACM, New York (2004) 320–327
11. Kaltofen, E., Yang, Z., Zhi, L.: Approximate greatest common divisors of several polynomials with linearly constrained coefficients and singular polynomials. In: ISSAC '06: Proceedings of the 2006 international symposium on Symbolic and algebraic computation, New York, NY, USA, ACM Press (2006) 169–176
12. Pan, V.Y.: Computation of approximate polynomial GCDs and an extension. Inform. and Comput. **167** (2001) 71–85
13. Lee, T.C.Y., Vanstone, S.A.: Subspaces and polynomial factorizations over finite fields. Appl. Algebra Engrg. Comm. Comput. **6** (1995) 147–157
14. Nagasaka, K.: Towards more accurate separation bounds of empirical polynomials. SIGSAM/CCA **38** (2004) 119–129
15. Zhi, L.: Displacement structure in computing approximate GCD of univariate polynomials. In: Computer mathematics. Volume 10 of Lecture Notes Ser. Comput. World Sci. Publ., River Edge, NJ (2003) 288–298

16. Rupprecht, D.: An algorithm for computing certified approximate GCD of n univariate polynomials. J. Pure Appl. Algebra **139** (1999) 255–284 Effective methods in algebraic geometry (Saint-Malo, 1998).
17. Ruppert, W.M.: Reducibility of polynomials $f(x, y)$ modulo p. J. Number Theory **77** (1999) 62–70
18. Gao, S., Rodrigues, V.M.: Irreducibility of polynomials modulo p via newton polytopes. J. Number Theory **101** (2003) 32–47
19. Kaltofen, E., May, J.: On approximate irreducibility of polynomials in several variables. In: Proceedings of the 2003 International Symposium on Symbolic and Algebraic Computation, ISSAC 2003. (2003) 161–168
20. Nagasaka, K.: Towards more accurate separation bounds of empirical polynomials II. In: Lecture Notes in Computer Science Volume 3718, Computer Algebra in Scientific Computing, 8th International Workshop, CASC 2005. (2005) 318–329
21. May, J.P.: 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)