Subresultants Under Composition *

Hoon Hong
Research Institute for Symbolic Computation
Johannes Kepler University
A-4040 Linz, Austria
e-mail: hhong@risc.uni-linz.ac.at

Abstract

It is a well known fact that the resultants are invariant under translation. We extend this fact to arbitrary composition (where a translation is a particular composition with a linear monic polynomial), and to arbitrary subresultants (where the resultant is the 0-th subresultant).

1 Introduction

It is a well known fact that the resultants[1] are invariant under translation. For example, let $A(x) = x^2 + 2x + 1$ and $B(x) = x - 1$. Then their resultant is 4. Let us translate the two polynomials by one: $A^*(x) = A(x+1) = x^2 + 4x + 4$ and $B^*(x) = B(x+1) = x$. One can verify that their resultant remains to be 4. In general, let $A(x)$ and $B(x)$ be two polynomials and R be their resultant. Let $A^*(x) = A(x+c)$ and $B^*(x) = B(x+c)$ and let R^* be their resultant. Then $R = R^*$.

Note that a translation (by c) is a particular composition, that is, $A^* = A \circ C$ where $\circ$ is a composition and $C = x + c$. In this notation, the invariance under translation can be written as

$$\mathrm{res}(A \circ C, B \circ C) = \mathrm{res}(A, B)$$

where C is $x + c$ for some c and res stands for the resultant.

One naturally ponders what happens when we allow an arbitrary polynomial for C (not just $x+c$). We show that if C is a monic polynomial of degree ℓ then

$$\mathrm{res}(A \circ C, B \circ C) = \mathrm{res}(A, B)^\ell.$$

This is not difficult to prove, but somewhat surprising. The resultant of $A \circ C$ and $B \circ C$ does not depend on the coefficients of C but only on its degree!

We recall that the resultant is the 0-th principal subresultant coefficient (psc_0). Thus, one now ponders what happens to a k-th one under composition. In this paper, we show that if C is a monic polynomial of degree ℓ then

$$\mathrm{psc}_k(A \circ C, B \circ C) = \begin{cases} \mathrm{psc}_\mu(A, B)^\ell & \text{if } k = \ell\mu \\ 0 & \text{otherwise.} \end{cases}$$

Emboldened by this elegant relation and recalling that the psc_k is the (formal) leading coefficient of the k-th subresultant sres_k, one now asks what happens to the subresultants under composition,

*This research was done in the framework of the European project ACCLAIM.

[1] For those who forget the definition of resultants, it can be found in Section 2.

We show that if C is a monic polynomial of degree ℓ then

$$\mathrm{sres}_k(A \circ C, B \circ C) = \begin{cases} \mathrm{psc}_\mu(A,B)^{\ell-1} & \mathrm{sres}_\mu(A,B) \circ C & \text{if } k = \ell\mu \\ \mathrm{psc}_\mu(A,B)^{\ell-1}\ \sigma_\mu & \mathrm{sres}_{\mu-1}(A,B) \circ C & \text{if } k = \ell\mu - 1 \\ 0 & & \text{otherwise} \end{cases}$$

where σ_μ is a sign ($\pm$) whose precise expression will be given in the next section. Those who are familiar with the theory of polynomial remainder sequence (prs) might guess that this has something to do with the gap structure of prs. It is true and their relationship will be made explicit in the proof.

So far we assumed that C is monic. Finally we ask what will happen if we allow an arbitrary leading coefficient c for C? We show that

$$\mathrm{sres}_k(A \circ C, B \circ C) = \begin{cases} c^{u_\mu}\ \mathrm{psc}_\mu(A,B)^{\ell-1} & \mathrm{sres}_\mu(A,B) \circ C & \text{if } k = \ell\mu \\ c^{v_\mu}\ \mathrm{psc}_\mu(A,B)^{\ell-1}\ \sigma_\mu & \mathrm{sres}_{\mu-1}(A,B) \circ C & \text{if } k = \ell\mu - 1 \\ 0 & & \text{otherwise} \end{cases}$$

where u_μ and v_μ are certain constants whose precise expression will be given in the next section. Note this relation subsumes all the previous relations in that the previous relations can be derived immediately by specializing this last relation. Thus, it will be sufficient to prove this last one, obtaining all other relations as corollaries.

The structure of the paper is as follows. In Section 2, we recall the definitions of resultants, principal subresultant coefficients, and subresultants. Then we give a precise statement of the main theorem. In Section 3, we give a proof of the main theorem.

2 Main Result

The main goal of this section is to give a precise statement of the relations mentioned in the introduction. For this, we briefly recall some basic notions such as resultants, principal subresultant coefficients, subresultants, and composition. For details, see [2, 1, 4, 5]. For those who are familiar with them can skip the following definitions.

Throughout this paper, let F stand for a field. Let $A = \sum_{i=0}^{m} a_i x^i$ and $B = \sum_{i=0}^{n} b_i x^i$ be two non-zero polynomials over F of degree m and n.

Definition 1 (Sylvester Matrices) The *Sylvester matrix* of A and B, written as $M_{A,B}$, is the $(m+n)$ by $(m+n)$ matrix

$$\begin{bmatrix} a_m & a_{m-1} & \cdots & a_0 & & & \\ & a_m & a_{m-1} & \cdots & a_0 & & \\ & & \cdots & \cdots & \cdots & \cdots & \\ & & & a_m & a_{m-1} & \cdots & a_0 \\ b_n & b_{n-1} & \cdots & b_0 & & & \\ & b_n & b_{n-1} & \cdots & b_0 & & \\ & & \cdots & \cdots & \cdots & \cdots & \\ & & & b_n & b_{n-1} & \cdots & b_0 \end{bmatrix}$$

where it consists of n rows of the shifted coefficients of A and m rows of the shifted coefficients of B. The blanks are zeros. □

Definition 2 (Resultants) The *resultant* of A and B, written as $\mathrm{res}(A,B)$, is the determinant of the Sylvester matrix of A and B. (When $m = n = 0$, the Sylvester matrix is the 0 by 0 matrix. We assume that its determinant is 1.) □

Definition 3 (Principal Subresultants Coefficients) Let M_k be the submatrix of $M_{A,B}$ consisting of the first $n-k$ rows of the A coefficients, the first $m-k$ rows of the B coefficients, and the first $m+n-2k$ columns. The k-th *principal subresultant coefficient* of A and B, written as $\mathrm{psc}_k(A,B)$, is the determinant of M_k. Obviously, it is defined only for $0 \leq k \leq \min(m,n)$. □

Thus, the resultant is the 0-th principal subresultant coefficient. The name "principal subresultant coefficient" is motivated by the following.

Definition 4 (Subresultants) Let $M_k^{(i)}$ be the submatrix of $M_{A,B}$ consisting of the first $n-k$ rows of the A coefficients, the first $m-k$ rows of the B coefficients, and the first $m+n-2k-1$ columns and the $m+n-k-i$-th column. The k-th *subresultant* of A and B, written as $\mathrm{sres}_k(A,B)$, is the polynomial over F

$$\sum_{i=0}^{k} |M_k^{(i)}| x^i.$$

Again it is defined only for $0 \leq k \leq \min(m,n)$. For the case $m=n=k$, we assume that it is B/b_n. □

Thus, the k-th principal subresultant coefficient is $|M_k^{(k)}|$, the coefficient for the term x^k in the k-th subresultant. It is not called the "leading" coefficient because it could be zero.

From now on, let C be a polynomial over F with degree $n \geq 1$ and leading coefficient c.

Definition 5 (Composition) The composition of A and C, written as $A \circ C$ is the polynomial over F obtained by replacing the indeterminate x in A with C. □

Note that we did *not* define this as a "function" composition:

$$\forall x \in F \quad (A \circ C)(x) = A(C(x)).$$

The reason is that this "definition" does not guarantee the uniqueness when F is a finite field. Now we are ready to state the main theorem of this paper.

Theorem 1 (Subresultants under Composition)

$$\mathrm{sres}_k(A \circ C, B \circ C) = \begin{cases} c^{u_\mu}\,\mathrm{psc}_\mu(A,B)^{\ell-1} & \mathrm{sres}_\mu(A,B) \circ C & \text{if } k = \ell\mu \\ c^{v_\mu}\,\mathrm{psc}_\mu(A,B)^{\ell-1}\sigma_\mu & \mathrm{sres}_{\mu-1}(A,B) \circ C & \text{if } k = \ell\mu - 1 \\ 0 & & \text{otherwise} \end{cases}$$

where

$$\begin{aligned} u_\mu &= c^{\ell(mn-\mu^2)-\mu} \\ v_\mu &= c^{\ell(mn-\mu^2)+\mu} \\ \sigma_\mu &= (-1)^{(m-\mu)(\ell-1)}. \end{aligned}$$ □

As mentioned earlier, all other relations stated in the introduction are easy special cases of this theorem. Thus, we will prove only this main theorem in the next section.[2]

[2]However, it should be noted that one might find simpler proofs for the special cases. For instance, one can find a few line proof for the resultant under composition (shown in the introduction) by utilizing the fact that $\mathrm{res}(A, B_1B_2) = \mathrm{res}(A,B_1)\mathrm{res}(A,B_2)$. For details, see [3].

3 Proof

The main goal of this section is to give a proof of the main theorem stated in the previous section. The proof will be divided into several lemmas which are interesting on their own.

Recall that F is a field and A, B and C are polynomials over F of degrees m, n and ℓ respectively where $m, n \geq 0$ and $\ell \geq 1$. Assume that the degree of the zero polynomial is $-\infty$. We begin with a well-known elementary, but important fact.

Lemma 1 (Uniqueness of Quotient/Remainder) There exists *unique* polynomials $Q, R \in F[x]$ such that $A = QB + R$ and $\deg(R) < \deg(B)$. □

It is also an elementary fact that that the composition commutes with addition, subtraction, and multiplication. What about division (that is, quotient and remainder)? Do they also commute with composition? The following lemma answers positively, making an essential use of their uniqueness property.

Lemma 2 (Commutativity of Quotient/Remainder with Composition) Let

$$A = QB + R$$

where $\deg(R) < \deg(B)$. Let $A^* = A \circ C$ and $B^* = B \circ C$ and

$$A^* = Q^* B^* + R^*$$

where $\deg(R^*) < \deg(B^*)$. Then, $Q^* = Q \circ C$ and $R^* = R \circ C$. □

Proof. From the hypothesis of the lemma, we have $A = QB + R$. Since the composition commutes with multiplication and addition, we have $A \circ C = (Q \circ C)(B \circ C) + (R \circ C)$. Since $A^* = A \circ C$ and $B^* = B \circ C$, we have

$$A^* = (Q \circ C)B^* + (R \circ C).$$

Note that

$$\deg(R \circ C) = \deg(R)\deg(C) < \deg(B)\deg(C) = \deg(B^*).$$

Thus, we have $\deg(R \circ C) < \deg(B^*)$. Here we have made an essential use of the assumption that $\deg(C) \geq 1$. If $\deg(C) = 0$, the above inequality will not hold!

Since the quotient and the remainder are unique (Lemma 1), we conclude that $Q^* = Q \circ C$ and $R^* = R \circ C$. □

Next, repeatedly applying the above finding, we show that the composition also commutes with the (natural) polynomial quotient/remainder sequence computation.

Definition 6 (Natural Polynomial Remainder Sequence) The sequences

$$Q_1, Q_2, \ldots, Q_{r-1} \quad \text{and} \quad A_1, A_2, \ldots, A_r$$

are called respectively the *natural polynomial quotient* and *remainder sequences* of A and B iff $A_1 = A$, $A_2 = B$ and

$$A_i = Q_i A_{i+1} + A_{i+2}$$

where $\deg(A_{i+1}) > \deg(A_{i+2})$ for $i = 1, \ldots, r-1$ and $A_{r+1} = 0$. □

Lemma 3 (Commutativity of Polynomial Sequence with Composition) Let the sequences

$$Q_1, Q_2, \ldots, Q_{r-1} \quad \text{and} \quad A_1, A_2, \ldots, A_r$$

be the polynomial quotient and the remainder sequences of A and B. Let the sequences

$$Q_1^*, Q_2^*, \ldots, Q_{r^*-1}^* \quad \text{and} \quad A_1^*, A_2^*, \ldots, A_{r^*}^*$$

be the polynomial quotient and the remainder sequences of $A^* = A \circ C$ and $B^* = B \circ C$. Then, we have $r = r^*$ and

$$A_i^* = A_i \circ C \quad \text{and} \quad Q_i^* = Q_i \circ C$$

for every i. □

Proof. Immediately follows by repeatedly (inductively) applying the commutativity of the quotient and remaindering with the composition (Lemma 2). □

From now on, let $A_1, \ldots, A_r$ be the natural polynomial remainder sequence of A and B. Let $n_1, \ldots, n_r$ be the sequence of their degrees and let $a_1, \ldots, a_r$ be the sequence of their leading coefficients. Let S_k stand for the k-th subresultant of A and B.

Now we recall the fundamental theorem of polynomial remainder sequence proved by Collins [4]. The original theorem of Collins was more general in that it was for an arbitrary polynomial remainder sequence (not just the natural one). But we only need it for the natural one, thus we give a simplified version of it (by setting $e_i = f_i = 1$ in the notation of [4]).

Lemma 4 (Fundamental theorem of Polynomial Remainder Sequence) We have, for every $0 \le k \le \min(n_1, n_2)$,

$$S_k = \begin{cases} \left\{\prod_{i=1}^{j-2} (-1)^{(n_i - n_j)(n_{i+1} - n_j)} a_{i+1}^{n_i - n_{i+2}}\right\} a_j^{n_{j-1} - n_j - 1} A_j & \text{if } k = n_j \quad \text{for } 2 \le j \le r \\ \left\{\prod_{i=1}^{j-1} (-1)^{(n_i - n_j + 1)(n_{i+1} - n_j + 1)} a_{i+1}^{n_i - n_{i+2}}\right\} a_j^{-n_j + n_{j+1} + 1} A_{j+1} & \text{if } k = n_j - 1 \quad \text{for } 2 \le j \le r-1 \\ 0 & \text{otherwise. } \square \end{cases}$$

Here the range for the index j is slightly wider than that of [4], but it does not cause incorrectness because we assumed that when $n_1 = n_2$ the n_2-th subresultant is A_2/a_2 (Definition 4).

By using the fundamental theorem of polynomial remainder sequence, we derive expressions for the leading coefficients of the subresultants. From now on let s_k stand for the leading coefficient of the k-th subresultant S_k.

Lemma 5 (Leading Subresultant Coefficients) We have the followings:
(a) For $2 \le j \le r$, we have

$$s_{n_j} = \left\{\prod_{i=1}^{j-2} (-1)^{(n_i - n_j)(n_{i+1} - n_j)} a_{i+1}^{n_i - n_{i+2}}\right\} a_j^{n_{j-1} - n_j}.$$

(b) For $2 \le j \le r-1$, we have

$$s_{n_j - 1} = (-1)^{j - 1 + n_1 - n_j}\ s_{n_j}\ a_j a_{j+1}. \ \square$$

Proof. The proof for (a) is trivial. We only need to recall that a_j is the leading coefficient of A_j. Thus, from now on, let us prove (b). By making elementary rewritings, we obtain

$$s_{n_j - 1} \quad = \quad \left\{\prod_{i=1}^{j-1} (-1)^{(n_i - n_j + 1)(n_{i+1} - n_j + 1)} a_{i+1}^{n_i - n_{i+2}}\right\} a_j^{-n_j + n_{j+1} + 1} a_{j+1}$$

$$
\begin{aligned}
&= \left\{\prod_{i=1}^{j-1}(-1)^{(n_i-n_j+1)(n_{i+1}-n_j+1)}\right\}\left\{\prod_{i=1}^{j-1}a_{i+1}^{n_i-n_{i+2}}\right\}a_j^{-n_j+n_{j+1}+1}a_{j+1}\\
&= \left\{\prod_{i=1}^{j-1}(-1)^{(n_i-n_j+1)(n_{i+1}-n_j+1)}\right\}\left\{\prod_{i=1}^{j-2}a_{i+1}^{n_i-n_{i+2}}\right\}a_j^{n_{j-1}-n_{j+1}}a_j^{-n_j+n_{j+1}+1}a_{j+1}\\
&= \left\{\prod_{i=1}^{j-1}(-1)^{(n_i-n_j+1)(n_{i+1}-n_j+1)}\right\}\left\{\prod_{i=1}^{j-2}a_{i+1}^{n_i-n_{i+2}}\right\}a_j^{n_{j-1}-n_j}a_ja_{j+1}\\
&= \rho_j s_{n_j}a_ja_{j+1}
\end{aligned}
$$

where

$$\rho_j = \frac{\prod_{i=1}^{j-1}(-1)^{(n_i-n_j+1)(n_{i+1}-n_j+1)}}{\prod_{i=1}^{j-2}(-1)^{(n_i-n_j)(n_{i+1}-n_j)}}.$$

Note that $\rho_j = (-1)^{\omega_j}$ where

$$\omega_j = \left\{\sum_{i=1}^{j-1}(n_i-n_j+1)(n_{i+1}-n_j+1)\right\} - \left\{\sum_{i=1}^{j-2}(n_i-n_j)(n_{i+1}-n_j)\right\}.$$

Next, let us repeatedly simplify the expression for ω_j (modulo 2 since we are only interested in its parity).

$$
\begin{aligned}
\omega_j &= \left\{\sum_{i=1}^{j-2}(n_i-n_j+1)(n_{i+1}-n_j+1)-(n_i-n_j)(n_{i+1}-n_j)\right\}+(n_{j-1}-n_j+1)\\
&= \left\{\sum_{i=1}^{j-2}(n_i-n_j+n_{i+1}-n_j+1)\right\}+(n_{j-1}-n_j+1)\\
&= \left\{\sum_{i=1}^{j-2}(n_i-n_{i+1}+1)\right\}+(n_{j-1}-n_j+1)\\
&= \sum_{i=1}^{j-1}(n_i-n_{i+1}+1)\\
&= j-1+\sum_{i=1}^{j-1}(n_i-n_{i+1})\\
&= j-1+(n_1-n_2+n_2-\cdots-n_{j-1}+n_{j-1}-n_j)\\
&= j-1+n_1-n_j.
\end{aligned}
$$

Putting them together, we finally have

$$s_{n_j-1} = (-1)^{n_1-n_j+j-1}s_{n_j}a_ja_{j+1}$$

which proves (b). □

From now on, let $A^* = A \circ C$ and $B^* = B \circ C$ and let $A_1^*, \ldots, A_{r^*}^*$ be the natural polynomial remainder sequence of A^* and B^*. Let also $n_1^*, \ldots, n_{r^*}^*$ be their degree sequence and let $a_1^*, \ldots, a_{r^*}^*$ be their leading coefficient sequence. From Lemma 3, we know that $r^* = r$, thus from now on, we will use only r.

Further let S_k^* stand for the k-th subresultant of A^* and B^* and let s_k^* be its leading coefficient. Let c be the leading coefficient of C and ℓ be its degree.

Lemma 6 (Subresultant Coefficients under Composition) We have the following:
(a) For $2 \le j \le r$, we have

$$s^*_{n^*_j} = c^{\ell(n_1 n_2 - n_j^2)}\, s^\ell_{n_j}$$

(b) For $2 \le j \le r-1$, we have

$$s^*_{n^*_j - 1} = (-1)^{(n_1 - n_j)(\ell-1)}\, c^{\ell(n_1 n_2 - n_j^2) + n_j + n_{j+1}}\, s^{\ell-1}_{n_j} s_{n_j - 1}. \ \square$$

Proof. Let us first prove (a). By applying Lemma 5(a) on the natural polynomial remainder sequence of A^* and B^*, we obtain

$$s^*_{n^*_j} = \left\{ \prod_{i=1}^{j-2} (-1)^{(n^*_i - n^*_j)(n^*_{i+1} - n^*_j)} {a^*_{i+1}}^{n^*_i - n^*_{i+2}} \right\} {a^*_j}^{n^*_{j-1} - n^*_j}.$$

From Lemma 3, we know that $A^*_i = A_i \circ C$. Thus $n^*_i = n_i \ell$ and $a^*_i = a_i c^{n_i}$. Putting these into the above expression and repeatedly simplifying, we obtain

$$\begin{aligned}
s^*_{n^*_j} &= \left\{ \prod_{i=1}^{j-2} (-1)^{(n_i - n_j)(n_{i+1} - n_j)\ell^2} {a_{i+1}}^{(n_i - n_{i+2})\ell} \right\} {a_j}^{(n_{j-1} - n_j)\ell} \\
&\quad \left\{ \prod_{i=1}^{j-2} c^{n_{i+1}(n_i - n_{i+2})\ell} \right\} c^{n_j(n_{j-1} - n_j)\ell} \\
&= s^\ell_{n_j} \left\{ \prod_{i=1}^{j-2} c^{n_{i+1}(n_i - n_{i+2})\ell} \right\} c^{n_j(n_{j-1} - n_j)\ell} \\
&= s^\ell_{n_j} c^{\left\{\sum_{i=1}^{j-2} n_{i+1}(n_i - n_{i+2})\ell\right\} + n_j(n_{j-1} - n_j)\ell} \\
&= s^\ell_{n_j} c^{\ell\left\{\sum_{i=1}^{j-2} n_i n_{i+1} - n_{i+1} n_{i+2}\right\} + n_j(n_{j-1} - n_j)\ell} \\
&= s^\ell_{n_j} c^{\ell(n_1 n_2 - n_{j-1} n_j) + n_j(n_{j-1} - n_j)\ell} \\
&= s^\ell_{n_j} c^{\ell(n_1 n_2 - n_j^2)}
\end{aligned}$$

which proves (a).

Now let us prove (b). By applying Lemma 5(b) on the natural polynomial remainder sequence of A^* and B^*, we obtain

$$s^*_{n^*_j - 1} = (-1)^{j-1+n^*_1 - n^*_j} s^*_{n^*_j} a^*_j a^*_{j+1}.$$

Again repeatedly rewriting, using various facts known so far, we obtain

$$\begin{aligned}
s^*_{n^*_j - 1} &= (-1)^{j-1+(n_1 - n_j)\ell} s^*_{n^*_j} c^{n_j} c^{n_{j+1}} a_j a_{j+1} \quad \text{(Lemma 3)} \\
&= (-1)^{j-1+(n_1 - n_j)\ell} s^*_{n^*_j} c^{n_j} c^{n_{j+1}} \frac{s_{n_j - 1}}{(-1)^{j-1+n_1 - n_j} s_{n_j}} \quad \text{(Lemma 5(b))} \\
&= (-1)^{j-1+(n_1 - n_j)\ell} s^\ell_{n_j} c^{\ell(n_1 n_2 - n_j^2)} c^{n_j} c^{n_{j+1}} \frac{s_{n_j - 1}}{(-1)^{j-1+n_1 - n_j} s_{n_j}} \quad \text{(Lemma 6(a))} \\
&= (-1)^{(n_1 - n_j)(\ell-1)} s^{\ell-1}_{n_j} c^{\ell(n_1 n_2 - n_j^2) + n_j + n_{j+1}} s_{n_j - 1}
\end{aligned}$$

which proves (b). $\square$

Lemma 7 (Subresultant PRS under Composition) We have, for every $0 \leq k \leq \min(n_1^*, n_2^*)$,

$$S_k^* = \begin{cases} c^{u_{n_j}}\ s_{n_j}^{\ell-1} & S_{n_j} \circ C & \text{if } k = n_j^* & \text{for } 2 \leq j \leq r \\ c^{v_{n_j}}\ s_{n_j}^{\ell-1}\ \sigma_{n_j} & S_{n_j-1} \circ C & \text{if } k = n_j^* - 1 & \text{for } 2 \leq j \leq r-1 \\ 0 & & \text{otherwise} & \end{cases}$$

where

$$\begin{aligned} u_\mu &= c^{\ell(n_1 n_2 - \mu^2) - \mu} \\ v_\mu &= c^{\ell(n_1 n_2 - \mu^2) + \mu} \\ \sigma_\mu &= (-1)^{(n_1 n_2 - \mu)(\ell - 1)}. \ \square \end{aligned}$$

Proof. By applying the fundamental theorem of the polynomial remainder sequence (Lemma 4) on A^* and B^*, we know, for every $0 \leq k \leq \min(n_1^*, n_2^*)$,

$$S_k^* \sim \begin{cases} A_j^* & \text{if } k = n_j^* & \text{for } 2 \leq j \leq r \\ A_{j+1}^* & \text{if } k = n_j^* - 1 & \text{for } 2 \leq j \leq r-1 \\ 0 & \text{otherwise.} & \end{cases} \tag{1}$$

From the commutativity of composition with polynomial remainder sequence (Lemma 3), we know that

$$A_i^* = A_i \circ C. \tag{2}$$

Thus, putting (1) and (2) together, we see for every $0 \leq k \leq \min(n_1^*, n_2^*)$,

$$S_k^* \sim \begin{cases} A_j \circ C & \text{if } k = n_j^* & \text{for } 2 \leq j \leq r \\ A_{j+1} \circ C & \text{if } k = n_j^* - 1 & \text{for } 2 \leq j \leq r-1 \\ 0 & \text{otherwise.} & \end{cases} \tag{3}$$

By applying the fundamental theorem of the polynomial remainder sequence (Lemma 4) on A and B, we know, for every $0 \leq k \leq \min(n_1, n_2)$,

$$S_k \sim \begin{cases} A_j & \text{if } k = n_j & \text{for } 2 \leq j \leq r \\ A_{j+1} & \text{if } k = n_j - 1 & \text{for } 2 \leq j \leq r-1 \\ 0 & \text{otherwise.} & \end{cases} \tag{4}$$

By composing (4) with C, we see for every $0 \leq k \leq \min(n_1, n_2)$,

$$S_k \circ C \sim \begin{cases} A_j \circ C & \text{if } k = n_j & \text{for } 2 \leq j \leq r \\ A_{j+1} \circ C & \text{if } k = n_j - 1 & \text{for } 2 \leq j \leq r-1 \\ 0 & \text{otherwise.} & \end{cases} \tag{5}$$

Putting together (3) and (5), we see for every $0 \leq k \leq \min(n_1^*, n_2^*)$,

$$S_k^* = \begin{cases} U_j\ S_{n_j} \circ C & \text{if } k = n_j^* & \text{for } 2 \leq j \leq r \\ V_j\ S_{n_j-1} \circ C & \text{if } k = n_j^* - 1 & \text{for } 2 \leq j \leq r-1 \\ 0 & \text{otherwise.} & \end{cases} \tag{6}$$

for some similarity constants U_j and V_j. Next we determine U_j and V_j by dividing the leading coefficients and by using Lemma 6.

$$\begin{aligned} U_j &= \frac{s_{n_j^*}^*}{s_{n_j} c^{n_j}} \\ &= \frac{c^{\ell(n_1 n_2 - n_j^2)}\ s_{n_j}^\ell}{s_{n_j} c^{n_j}} \end{aligned}$$

$$
\begin{aligned}
&= c^{\ell(n_1 n_2 - n_j^2) - n_j}\ s_{n_j}^{\ell-1} \\
&= c^{u_{n_j}}\ s_{n_j}^{\ell-1}
\end{aligned}
$$

$$
\begin{aligned}
V_j &= \frac{s^*_{n_j^*-1}}{s_{n_j-1} c^{n_{j+1}}} \\
&= \frac{(-1)^{(n_1-n_j)(\ell-1)}\ c^{\ell(n_1 n_2 - n_j^2)+n_j+n_{j+1}}\ s_{n_j}^{\ell-1} s_{n_j-1}}{s_{n_j-1} c^{n_{j+1}}} \\
&= (-1)^{(n_1-n_j)(\ell-1)}\ c^{\ell(n_1 n_2 - n_j^2)+n_j}\ s_{n_j}^{\ell-1} \\
&= \sigma_{n_j}\ c^{v_{n_j}}\ s_{n_j}^{\ell-1}
\end{aligned}
$$

which proves the lemma. □

Proof of the Main Theorem

Finally we prove the main theorem of this paper (Theorem 1).

Case 1: $k = \ell n_j$ for some $2 \le j \le r$.

By the Lemma 7, we have $S_k^* = c^{u_{n_j}}\ \ s_{n_j}^{\ell-1}\ \ S_{n_j} \circ C$. Since the degree of S_{n_j} is n_j (by the fundamental theorem of polynomial remainder sequence), its leading coefficient s_{n_j} is also the principal one. Thus, we have

$$S_k^* = c^{u_{n_j}}\ \ \mathrm{psc}_{n_j}(A,B)^{\ell-1}\ \ S_{n_j} \circ C$$

which coincides with the claim of the theorem.

Case 2: $k = \ell n_j - 1$ for some $2 \le j \le r-1$.

By the Lemma 7, we have $S_k^* = c^{v_{n_j}}\ \ s_{n_j}^{\ell-1}\ \ \sigma_{n_j}\ \ S_{n_j-1} \circ C$. Since the degree of S_{n_j} is n_j (again by the fundamental theorem of polynomial remainder sequence), its leading coefficient s_{n_j} is also the principal one. Thus, we have

$$S_k^* = c^{v_{n_j}}\ \ \mathrm{psc}_{n_j}(A,B)^{\ell-1}\ \ \sigma_{n_j}\ \ S_{n_j-1} \circ C$$

which coincides with the claim of the theorem.

Case 3: Otherwise.

By the Lemma 7, we have $S^* = 0$. We need to check whether the theorem claims the same.

Case 3a: $\ell > 1$.

Case 3a1: $k = \ell\mu$ or $k = \ell\mu - 1$ for some μ.

There is no j such that $\mu = n_j$, hence, the degree of S_μ must be less than μ (by the fundamental theorem of polynomial sequence). Thus, $\mathrm{psc}_\mu(A,B) = 0$. Since $\ell - 1 > 0$, the theorem also claims that $S_k^* = 0$.

Case 3a2: Otherwise.

Since there is no μ such that $k = \ell\mu$ or $k = \ell\mu - 1$, the theorem also claims that $S_k^* = 0$.

Case 3b: Otherwise.

Since there is no j such that $k = n_j$ or $k = n_j - 1$, we have $S_k = 0$. Hence, the theorem also claims that $S_k^* = 0$.

Thus, the main theorem of this paper (Theorem 1) has been proved. □

References

[1] W. S. Brown and J. F. Traub. On Euclid's algorithm and the theory of subresultants. *Journal ACM*, 18(4):505–514, October 1971.

[2] G. E. Collins. Subresultants and reduced polynomial remainder sequences. *Journal ACM*, 14:128–142, 1967.

[3] H. Hong and J. Schicho. A new proof for the implicitization of curves parameterized by generalized trigonometric polynoimals. Technical report, Research Institute for Symbolic Computation, Johannes Kepler University A-4040 Linz, Austria, 1995.

[4] R. G. K. Loos. Generalized polynomial remainder sequences. In B. Buchberger, G. E. Collins, and R. G. K. Loos, editors, *Computer Algebra, Symbolic and Algebraic Computation*, pages 115–137. Springer-Verlag, Wien-New York, 1982.

[5] B. Mishra. *Algorithmic Algebra*. Springer-Verlag, New York, 1993.