On Computing the Elimination Ideal Using Resultants with Applications to Gröbner Bases

Matteo Gallet, Hamid Rahkooy, Zafeirakis Zafeirakopoulos

Abstract

We are after a generator of the elimination ideal of an ideal generated by two polynomials in two variables. Such a generator is unique (up to multiplication by units) and can be computed via Gröbner basis. We are interested in finding the generator of the elimination ideal using the resultant of the generators of the ideal. All the factors of the generators are factors of the resultant but the multiplicities might be different. Geometrically we are looking at two algebraic curves. Factors of the resultant give us projections of all the intersection points with their multiplicities. We are investigating the difference between the multiplicities of the factors of the Gröbner basis and the resultant. In the case of general ideals we can express the difference between the variety of the elimination ideal and the variety of the set of the resultants of pairs of the generators. Also we show an attempt to use resultants in Gröbner basis computations.

1 Introduction

The aim of the work presented in this paper is to study the elimination ideal by the use of resultants. This is part of the elimination problem, which is an old and central topic in polynomial algebra.

Historically the motivation comes from the solution of polynomial systems and the desire to reduce the solution of a system in \( n \) variables to the solution of a system in less variables. In this context, many different tools appeared and in this paper we investigate some of the connections between them. The two objects we will focus on are the first elimination ideal and the resultant.

The problem has been considered among others by Sylvester, Bezout, Dixon, Macaulay and van der Waerden [14]. W. Gröbner wrote an article on this topic in 1949 [9]. A review of the topic has been given in Emiris and Mourrain [6]. Gelfand, Kapranov and Zelevinski in [10] give a modern view and review of resultants.

From an algebraic point of view, the elimination problem is the problem of computing the first elimination ideal. Geometrically we are considering the relation between the varieties of \( I \) and \( I_1 \), i.e., the solutions of the system and the solutions of the elimination ideal.

Gröbner bases will play a central role in our efforts to tackle the elimination problem. They were introduced by Buchberger in his PhD thesis [11]. Also
he gave an algorithm to compute a Gröbner basis. Gröbner bases have many important properties, the one we will use most extensively is the elimination property [2]. The elimination property says that we can compute a Gröbner basis for the elimination ideal algorithmically using Buchberger’s algorithm [2]. Nevertheless, this way of computing a basis of the elimination ideal has two drawbacks. Firstly, one computes a Gröbner basis of the ideal first and then discards most of the polynomials in the basis, which computationally is an overkill. We note that the computation is in \( n \) rather than \( n - 1 \) variables and Gröbner basis computation is doubly exponential in the number of variables [12]. Secondly, it provides very little intuition about what the elimination ideal represents. Our goal is to explicitly compute a basis for \( I_1 \), the first elimination ideal of a given ideal \( I \).

We focus on the case of ideals given by two generators in two variables. Geometrically this means two plane algebraic curves. The reason is that in the case of bivariate ideals, the elimination ideal is principal and this is crucial for a large part of our investigation. We consider ideals given by two generators, so that we only have to deal with one resultant (the resultant of these two polynomials). Section 2 deals with the problem of finding the factors of the generator of the elimination ideal. We relate the variety of the resultant with the projection of the variety of the ideal and we give a sufficient condition in term of the vanishing of the resultant for the projection of the variety of the ideal to coincide with the variety of the elimination ideal.

In Section 2.3 we examine the relation between the multiplicity at an intersection point of two affine plane curves, namely the multiplicity of a certain factor of the resultant of two polynomials, and the multiplicity of the corresponding factor in the elimination ideal generator. We provide examples in which the behaviour of these two multiplicities exhibit some unexpected (for us) phenomena. We propose a conjecture about a sufficient condition for the difference between these two numbers to be strictly positive.

Our motivation to consider the elimination problem was Gröbner basis computation. Although there are incremental algorithms for Gröbner basis computation, e.g., F5 [7], the induction is on the number of polynomials in the basis. Our goal is an incremental algorithm for Gröbner basis computation by use of resultants, performing induction on the number of variables. A sketch of such an algorithm appeared in [13]. A short description of the method and its benefits is given in Section 3.

2 Elimination

Let \( \mathbb{K} \) denote an algebraically closed field (we usually think of \( \mathbb{K} \) as being \( \mathbb{C} \)). In what follows we require the polynomial ring \( \mathbb{K}[x_1, x_2, \ldots, x_n] \) to be equipped with an elimination order, and we will denote by \( \text{lm}(f) \) the leading monomial of the polynomial \( f \). In particular we fix \( y \prec x \) or \( x_n \prec x_{n-1} \prec \ldots \prec x_1 \), depending on the number and naming of the variables.

Given an ideal \( I \subseteq \mathbb{K}[x_1, x_2, \ldots, x_n] \), we denote by \( I_i \) the \( i \)-th elimination
ideal, i.e., \( I_i = I \cap \mathbb{K}[x_{i+1}, x_{i+2}, \ldots, x_n] \). The celebrated Elimination Property of Gröbner bases asserts that if \( G \) is a Gröbner basis for an ideal \( I \) with respect to the lexicographic term order \( x_1 < x_2 < \ldots < x_n \), then \( G \cap \mathbb{K}[x_{i+1}, x_{i+2}, \ldots, x_n] \) is a Gröbner basis for \( I_i \) with respect to the same order.

For the most part of what follows we assume that our polynomials are bivariate. Since the univariate polynomial ring is a principal ideal domain and due to the Elimination Property mentioned above, we have that for \( I \subseteq \mathbb{K}[x, y] \), there is a unique (up to units) monic polynomial in \( \mathbb{K}[y] \), denoted by \( g \), such that \( I_1 = (g) \).

The object we will try to connect are resultants and Gröbner bases for elimination ideals. Let \( R \) be a commutative ring and \( f_1, f_2 \in R[x] \) be of degree \( d_1, d_2 \) respectively and denote by \( r_{ij} \) the coefficient of \( x^{i} \) in \( f_i \). We define the resultant of \( f_1 \) and \( f_2 \) to be

\[
\text{res}_x (f_1, f_2) = \det (\text{Syl}(f_1, f_2)),
\]

where \( \text{Syl}(f_1, f_2) \) is the Sylvester matrix.

We set some notation, which will be useful in the following:

- Given \( m \) polynomials \( f_1, \ldots, f_m \), we denote by \( R := \{(r_{ij} := \text{res}_x (f_i, f_j) | 1 \leq i < j \leq m)\} \) the ideal generated by the pairwise resultants of the \( m \) polynomials and by \( R := \gcd (r_{ij} \text{ for } 1 \leq i < j \leq m) \) the greatest common divisor of the pairwise resultants of the \( m \) polynomials.

- By \( S_{12} \) we denote the S-polynomial of \( f_1 \) and \( f_2 \), i.e.

\[
S_{12} = \frac{\text{lcm}(\text{lt}(f_1), \text{lt}(f_2))}{\text{lt}(f_1)} f_1 - \frac{\text{lcm}(\text{lt}(f_1), \text{lt}(f_2))}{\text{lt}(f_2)} f_2
\]

- If \( f_1, \ldots, f_m \in \mathbb{K}[x_1, x_2, \ldots, x_n] \), for each \( 1 \leq i \leq m \), we write \( f_i \) in the form

\[
f_i = h_i(x_2, \ldots, x_n)x_1^{N_i} + \text{ terms of } x_1\text{-degree less than } N_i.
\]

- If \( I \) is an ideal in \( \mathbb{K}[x_1, x_2, \ldots, x_n] \), then its associated variety is denoted by \( \mathcal{V}(I) \). If \( S \) is a variety, then \( \mathcal{I}(S) \) is its vanishing ideal.

2.1 Two Polynomials

We start the investigation of elimination ideals providing a lemma about S-polynomials and a proposition about the elimination ideal of an ideal generated by polynomials whose resultant is zero.

**Lemma 1.** Let \( f_1, f_2 \in \mathbb{K}[x_1, x_2, \ldots, x_n] \) and suppose that \( h \in \mathbb{K}[x_1, x_2, \ldots, x_n] \) with \( \text{deg}_x(h) > 0 \) is a common factor of them, so \( f_1 = hf_1' \) and \( f_2 = hf_2' \) for some \( f_1', f_2' \) in \( \mathbb{K}[x_1, x_2, \ldots, x_n] \). Let \( \ell_1 = \text{lm}(f_1), \ell_2 = \text{lm}(f_2), \ell_1' = \text{lm}(f_1'), \ell_2' = \text{lm}(f_2') \) and \( \ell_0 = \text{lm}(h) \), denote by \( S_{12} \) the S-polynomial of \( f_1 \) and \( f_2 \) and by \( S'_{12} \) the S-polynomial of \( f_1' \) and \( f_2' \). Then

\[
S_{12} = hS'_{12}.
\]
Proof. Let $\ell = \text{lcm}(\ell_1, \ell_2)$ and $\ell' = \text{lcm}(\ell'_1, \ell'_2)$. Then

\[
S_{12} = \frac{\ell}{\ell_1} f_1 - \frac{\ell}{\ell_2} f_2 \\
= \frac{\ell}{\ell_1} h f'_1 - \frac{\ell}{\ell_2} h f'_2 \\
= h \left( \frac{\ell}{\ell_1} f'_1 - \frac{\ell}{\ell_2} f'_2 \right)
\]

Since $\text{lcm}(\ell_1, \ell_2) = \ell_h \text{lcm}(\ell'_1, \ell'_2)$, we have that $\ell = \ell' \ell_h$. Therefore $\frac{\ell}{\ell_1} = \frac{\ell'}{\ell_h}$ and

\[
h \left( \frac{\ell}{\ell_1} f'_1 - \frac{\ell}{\ell_2} f'_2 \right) = h \left( \frac{\ell'}{\ell_h} f'_1 - \frac{\ell'}{\ell_h} f'_2 \right) = h S'_{12}.
\]

\[\Box\]

Theorem 1. Let $I = \langle f_1, f_2 \rangle \in \mathbb{K}[x_1, x_2, \ldots, x_n]$ and $\mathcal{R} = \text{res}_{x_1}(f_1, f_2)$. Then

\[
\mathcal{R} \equiv 0 \iff I_1 = \langle 0 \rangle.
\]

Proof. ($\Leftarrow$) Assume that $I_1 = \langle 0 \rangle$. Since $\mathcal{R} \in I_1$ we have $\mathcal{R} \equiv 0$.

($\Rightarrow$) Assume that $\mathcal{R} \equiv 0$. Then either one of $f_i$ is zero (for which the theorem is trivial) or $f_1$ and $f_2$ have a common factor $h$ with $\deg_2(h) > 0$. Let $S$ be the normal form of $S_{12}$ (after reduction with respect to $f_1$ and $f_2$). If $S = 0$, then $\{f_1, f_2\}$ is a Gröbner basis for the ideal $I$. Since $f_1, f_2 \in \mathbb{K}[x_1, x_2, \ldots, x_n] \setminus \mathbb{K}[x_2, x_3, \ldots, x_n]$, none of them is in $I_1$, and by the Elimination Property of Gröbner bases we have $I_1 = \langle 0 \rangle$. Now assume $S \neq 0$. Let $S'_{12}, f'_1, f'_2$ and $h$ be as in Lemma 1 and $S'$ be the reduced form of $S'_{12}$ with respect to $f'_1$ and $f'_2$. From Lemma 1 and the fact that reducing $S_{12}$ by $f_1$ and $f_2$ is equivalent to reducing $S'_{12}$ by $f'_1$ and $f'_2$, we have that $S = h S'$. Therefore in the process of the Gröbner basis computation by Buchberger’s algorithm, all of the new polynomials will have $h$ as a factor, and since $h \in \mathbb{K}[x_1, x_2, \ldots, x_n] \setminus \mathbb{K}[x_2, x_3, \ldots, x_n]$, all the polynomials in the Gröbner basis will belong to $\mathbb{K}[x_1, x_2, \ldots, x_n] \setminus \mathbb{K}[x_2, x_3, \ldots, x_n]$. By the Elimination Property of Gröbner bases we have $I_1 = \langle 0 \rangle$.

At first, we connect the variety of the resultant with the projection of the variety of the ideal $I$. In the projective space, see [4] and [5], we know that the variety of the resultant describes roots at infinity and affine roots of the polynomial system we started with.

We provide the reader with the proof in affine case. Indeed the following is an affine description of the roots of the resultant.

Theorem 2. Let $I = \langle f_1, f_2 \rangle \in \mathbb{K}[x_1, x_2, \ldots, x_n]$ and $\mathcal{R} = \text{res}_{x_1}(f_1, f_2)$. Then

\[
\mathcal{V}(\mathcal{R}) = \mathcal{V}(h_1, h_2) \cup \pi(\mathcal{V}(I))
\]

Proof. We prove the following three statements:
1. \( \mathcal{V}(h_1, h_2) \subseteq \mathcal{V}(R) \)

It is easy to see from the Laplace expansion of the Sylvester matrix, that the greatest common divisor of \( h_1 \) and \( h_2 \) divides \( R \). Thus \( \mathcal{V}(h_1, h_2) \subseteq \mathcal{V}(R) \).

2. \( \pi(\mathcal{V}(I)) \subseteq \mathcal{V}(R) \)

If \( f_1, f_2 \in \mathbb{K}[x_2, \ldots, x_n][x_1] \) have positive degree in \( x_1 \), then \( \text{res}_{x_1}(f_1, f_2) \in I_1 \) (\cite{4}, P. 162, Proposition 1). Thus \( \mathcal{V}(I_1) \subseteq \mathcal{V}(R) \). From theorem 2, page 124 in \cite{4} we have that

\[
\mathcal{V}(I_1) = \pi(\mathcal{V}(I)) \cup (\mathcal{V}(h_1, h_2) \cap \mathcal{V}(I_1))
\]

Which proves that \( \pi(\mathcal{V}(I)) \subseteq \mathcal{V}(I_1) \).

3. \( \mathcal{V}(R) \setminus \mathcal{V}(h_1, h_2) \subseteq \pi(\mathcal{V}(I)) \)

Let \( c \not\in \mathcal{V}(h_1, h_2) \). Then we have two cases:

- \( h_1(c) \neq 0 \) and \( h_2(c) \neq 0 \). We have that \( R(c) = \text{res}_{x_1}(f_1(x_1, c), f_2(x_1, c)) \). Thus

\[
R(c) = 0 \Rightarrow \text{res}_{x_1}(f_1(x_1, c), f_2(x_1, c)) = 0
\]

- Either \( h_1(c) = 0 \), or \( h_2(c) = 0 \). Without loss of generality, assume that \( h_1(c) = 0 \), \( h_2(c) = 0 \). Also assume that \( d_2 \) is the degree of \( f_2 \) and \( m < d_2 \) is the degree of \( f_2(x_1, c) \). From proposition 3, page 164 in \cite{4}, we have that

\[
\text{res}_{x_1}(f_1, f_2)(c) = h_1(c)^{d_2-m} \text{res}_{x_1}(f_1(x_1, c), f_2(x_1, c))
\]

Thus

\[
R(c) = h_1(c)^{d_2-m} \text{res}_{x}(f_1(x, c), f_2(x, c)).
\]

and since \( h_1(c) \neq 0 \), we have that

\[
R(c) = 0 \Rightarrow \text{res}_{x}(f_1(x, c), f_2(x, c)) = 0.
\]

So in both cases we have that \( R(c) = 0 \Rightarrow \text{res}_{x}(f_1(x, c), f_2(x, c)) = 0 \). On the other hand we have that

\[
c \in \pi(\mathcal{V}(f_1, f_2)) \iff \exists c_1 \in \mathbb{K} : (c_1, c) \in \mathcal{V}(f_1, f_2)
\]

\[
\iff \exists c_1 \in \mathcal{V}(f_1(x, c), f_2(x, c))
\]

\[
\iff \text{res}_{x}(f_1(x, c), f_2(x, c)) = 0
\]

Thus \( c \in \pi(\mathcal{V}(I)) \) and \( \mathcal{V}(R) \setminus \mathcal{V}(h_1, h_2) \subseteq \pi(\mathcal{V}(I)) \).

The theorem follows immediately from the three statements. \( \square \)

**Corollary 1.** \( \mathcal{V}(I_1) \subseteq \mathcal{V}(R) \)
Proof. We have $V(I_1) = (V(h_1, h_2) \cap V(I_1)) \cup \pi(V(I))$. Therefore from Theorem 2 we have $V(I_1) \subseteq V(R)$.

Now we focus for a moment on the bivariate case, proving that the variety of the elimination ideal is the projection of the variety of $I$, if $R$ is not identically zero.

Theorem 3. If $f_1, f_2 \in K[x, y]$ and $R$ is not identically zero, then

$$V(I_1) = \pi(V(I))$$

Proof. Assume that $R$ is not identically 0. Since $R$ vanishes at $\pi(V(I))$ and $R$ is a non-zero univariate polynomial, we have that $\pi(V(I))$ is finite. By the closure property (see §2 in [1]), we have that $V(I_1)$ is the Zariski closure of $\pi(V(I))$. Since finite sets are Zariski closed, we have that $V(I_1) = \pi(V(I))$.

Coming back to the general setting, if we take $f_1, f_2 \in K[x_1, x_2, \ldots, x_n]$, we can write them in the form

$$f_k = t_k + h_k x_1^{d_k} + \sum_{i=1}^{d_k-1} h_{ki} x_1^i$$

where $d_k$ is the degree of $f_k$ with respect to $x_1$ for $k = 1, 2$, $t_k \in K[x_2, x_3, \ldots, x_n]$ are the trailing coefficients and $h_k \in K[x_2, x_3, \ldots, x_n]$ are the leading coefficients of the two polynomials. If we expand the Sylvester matrix along its columns/rows we have

$$gcd(\text{entries in each column/row}) | R$$

But for columns it suffices to consider only first and last columns, because entries of at least one of these two columns appear in all other columns. Also for the rows it suffices to consider only first and last rows, as all other rows are shifts of these two rows. Thus we have the following divisibility relations:

Lemma 2. 

$$gcd(h_1, h_2) | R,$$

$$gcd(t_1, t_2) | R$$

and

$$gcd(h_k, t_k, h_{k1}, \ldots, h_{k(d_k-1)}) | R$$

for $k = 1, 2$.

Note 1. Theorem 2 does not imply the statement of Lemma 2 about leading coefficients because it doesn’t say anything about the multiplicities of the factors of the gcd of the leading coefficients.
2.2 More Than Two Polynomials

We consider the case of $I = \langle f_1, \ldots, f_m \rangle$, where $m > 2$ and $f_i \in \mathbb{K}[x_1, x_2, \ldots, x_n]$.
Recall the definition of the ideal
\[ R := \langle \{ r_{ij} := \text{res}_{x_1} (f_i, f_j) \mid 1 \leq i < j \leq m \} \rangle, \]
the ideal generated by the pairwise resultants of the $m$ polynomials. The following theorem describes the roots of $R$.

**Theorem 4.** Let $V_{ij} = \pi (V(f_i, f_j)), V(h_i, h_j)$ for $1 \leq i < j \leq m$ and $C$ be the Cartesian product $C = \times_{1 \leq i < j \leq m} V_{ij}$. Then
\[ V(R) = \bigcup_{c \in C} \bigcap_{i=1}^{m} c_i \]

**Proof.** By definition
\[ V(R) = \bigcap V(r_{ij}) \]
By Proposition 2 we have that $V(r_{ij}) = \pi (V(f_i, f_j)) \cup V(h_i, h_j)$. Then
\[ V(R) = \bigcap (\pi (V(f_i, f_j)) \cup V(h_i, h_j)) \]
\[ = \bigcup_{c \in C} \bigcap_{i=1}^{m} c_i. \]

**Corollary 2.**
With the above notation we have
\begin{itemize}
  \item $V(h_1, \ldots, h_m) \subseteq V(R)$
  \item $\pi (V(I)) \subseteq V(R)$
\end{itemize}
**Proof.** For the first part, since $V(h_i, h_j) \subseteq V(r_{ij})$ for all $1 \leq i < j \leq m$, we conclude that $\bigcap V(h_i, h_j) \subseteq V(R)$ and therefore $V(h_1, \ldots, h_m) \subseteq V(R)$.
For the second part we have $\pi (V(I)) \subseteq \pi (V(f_i, f_j))$ for all $1 \leq i < j \leq m$ and thus $\pi (V(I)) \subseteq V(r_{ij})$ for all $1 \leq i < j \leq m$. Therefore $\pi (V(I)) \subseteq V(R)$.

**Note 2.** Not necessarily $\bigcap \pi (V(f_i, f_j)) \subseteq \pi (V(I))$.

Corollary 2 states that all the factors of gcd $(h_1, \ldots, h_m)$ are factors of $R$ as well. It doesn’t say anything about their multiplicity. However we have a divisibility condition.
Lemma 3.
\[ \gcd(h_1, \ldots, h_m) | \mathcal{R} \]

Proof. For \(1 \leq i < j \leq m\) we have that \(\gcd(h_i, h_j) \mid \text{res}_x(f_i, f_j)\). Thus
\[ \gcd(\gcd(h_i, h_j)) \mid \gcd(r_{ij}) \]
which means that \(\gcd(h_1, \ldots, h_m) \mid \mathcal{R}\).

Note 3. If we set \(f_i = f_1\) in \(R\) and consider the ideal \(R' := \langle \{\text{res}_x(f_1, f_j) | 2 \leq j \leq m\} \rangle\) then all the theorems and corollaries of this section about \(R\) will be correct for \(R'\). Now the question is what are the advantages and disadvantages of working with \(R\) or \(R'\). Since \(R' \subseteq R\) then \(\mathcal{V}(R) \subseteq \mathcal{V}(R')\), which means that \(\mathcal{V}(R)\) is closer to \(\mathcal{V}(I_1)\) than \(\mathcal{V}(R')\). On the other hand for \(R'\) we have a basis with much less generators than for \(R\) (\(m\) vs. \(\binom{m}{2}\)) and therefore working with \(R'\) may lead us to less or easier computations.

The following lemma connects the generator of the elimination ideal to the resultant, in the case of bivariate ideals.

Lemma 4. Let \(f_1, f_2, \ldots, f_m \in \mathbb{K}[x, y]\) and \(g\) be the unique monic generator of \(I_1\). Then \(R = \langle \mathcal{R} \rangle\) and \(g | \mathcal{R}\).

Proof. \(R \subseteq \mathbb{K}[y]\) and \(\mathbb{K}[y]\) is a principal ideal domain, thus \(R = \langle \mathcal{R} \rangle\). Since \(\mathcal{R} \in I_1\), we have \(g | \mathcal{R}\).

Lemma 4 says that although \(\mathcal{R}\) itself does not necessarily generate the elimination ideal, the product of some of its factors does. In [11] Lazard gave a structure theorem for the minimal lexicographic Gröbner basis of a bivariate ideal which reveals some of the factors of the elements. Also he has shown that the product of some of those factors divides the resultant, however it does not tell us about the extra factors that we are looking for without Gröbner basis computation.

2.3 Multiplicities

In this section we focus on bivariate ideals. From Lemma 4 we know that the factors of \(g\) are factors of \(\mathcal{R}\). The next natural question is to identify their multiplicities. Let \(I = \langle f_1, f_2 \rangle \subseteq \mathbb{K}[x, y]\) and \(I_1 = \langle g \rangle \subseteq \mathbb{K}[y]\) be its first elimination ideal. We start by stating an obvious upper bound.

Lemma 5. If \(c \in \mathbb{C}\) is a root of \(g\) with multiplicity \(\mu\) then \(c\) is a root of \(\mathcal{R}\) with multiplicity \(\nu\) and \(\mu \leq \nu\), since \(g | \mathcal{R}\) due to Lemma 4.

The rest of this section investigates the problems faced when trying to establish a lower bound. We will stick with the notation \(\mu\) and \(\nu\) for multiplicities of factors of \(g\) and \(\mathcal{R}\) respectively.
2.3.1 $\nu = 1$

Let $f \in \mathbb{K}[y]$ be an irreducible factor of $\mathcal{R}$ with multiplicity $\nu = 1$. Combining Theorem 2 and Theorem 3 we have that roots of the resultant are either roots of $h_1$ and $h_2$ or roots of $I_1$. Moreover, from Theorem ?? and since roots of $\text{gcd}(h_1, h_2)$ correspond to roots at infinity if we homogenize, we know that if $f$ corresponds to both a root of $I_1$ and of $\text{gcd}(h_1, h_2)$ then the degree of $f$ in $\mathcal{R}$ would be greater than 1. Thus

$$f \not| \text{gcd}(h_1, h_2) \Rightarrow f|g$$

and we get the following

**Proposition 1.** Let $I = \langle f_1, f_2 \rangle \subseteq \mathbb{K}[x, y]$ and $I_1 = \langle g \rangle \subseteq \mathbb{K}[y]$ be its first elimination ideal. If $\mathcal{R}$ is square free, then

$$g = \frac{\mathcal{R}}{\text{gcd}(h_1, h_2)}$$

2.3.2 $\nu > 1$

Let us now assume that $\mathcal{R}$ contains factors with multiplicity greater than 1.

We propose some examples, which show the fact that in one side we consider the intersection multiplicity at a point $P$ of the two curves in the affine plane defined by $f_1$ and $f_2$, namely the multiplicity $\nu$ of the factor corresponding to $P$ in $\mathcal{R}$, and on the other side we consider the multiplicity $\mu$ of the factor corresponding to the projection of $P$ along the $x$-axis in $g$, then there are situations in which $\mu$ can be strictly smaller than $\nu$, and we propose a possible sufficient condition for this phenomenon to happen.

$$f_1 = x^3 + 3x^2y + 3xy^2 + 4xy + y^3$$

$$f_2 = x - y$$

$$h_1 = 1$$

$$h_2 = 1$$

$$g = \frac{1}{2} \cdot (2y + 1) \cdot y^2$$

$$\mathcal{R} = (-4) \cdot (2y + 1) \cdot y^2$$
One might be tempted to think that the multiplicity drop is related to the fact that $h_2 = y - 1$. The following example shows that the situation is more complicated.

One of the configuration where the difference in the multiplicities of a factor in the resultant and the generator of the elimination ideal is positive is described in the following conjecture.

**Conjecture 1.** Assume that no two affine roots of the system given by $f_1$ and $f_2$ have the same $y$-coordinate. If the two curves defined by $f_1$ and $f_2$ admit a common tangent at an intersection point $P$ which is parallel to the $x$-axis, then multiplicity of the factor corresponding to (the projection of) $P$ in $g$ is strictly smaller than the multiplicity of the factor corresponding to $P$ in $R$.

In order to illustrate the conjecture in one example we provide the following.

**Example 1.**
\[ f_1 = -(y + 1)(x - y - 1) \]
\[ f_2 = x^2 + y^2 - 1 \]
\[ h_1 = -(y + 1) \]
\[ h_2 = 1 \]
\[ g = y(y + 1)^2 \]
\[ \mathcal{R} = 2y(y + 1)^3 \]

The factor \( y \) in \( g \) is preserved with the same multiplicity as in \( \mathcal{R} \), but the factor \( (y + 1) \) drops by 1. One can notice that we are in the situation covered by the Conjecture, since \( (y + 1) \) and the circle have a common tangent parallel to the \( x \)-axis at their intersection.

3 Future Directions

In this section we present some ideas and open problems for future directions of this work. These include problems and/or new ideas on investigating the relation between resultants and Gröbner basis computation and also the elimination and expansion problems.

3.1 Resultants of Gröbner basis members

Can we find a (necessary) condition for a set \( G \) to be a (reduced) Gröbner basis by looking at the properties/forms of the resultants of the members of \( G \)?

We try to approach this problem by computing the resultant of \( S_{12} \) and \( f_2 \). In the following we set the notation and do the computations in several steps. Let \( f_1 = \sum_{i=0}^{d_1} a_i x^i, f_2 = \sum_{i=0}^{d_2} b_i x^i \), in which \( a_i, b_j \in \mathbb{K}[y] \). Then \( S_{12} = m_1 f_1 - m_2 f_2 \), where \( m_1 = c_1 y^{k_1}, m_2 = c_2 y^{k_2} x^{d_1 - d_2} \) such that \( c_i \in \mathbb{K} \). During the following computations we use several properties of the resultants which can be found in [3].

**Step 1.** \( R(f_2, S_{12}) \).

Let \( d_{12} := \deg(S_{12}) \) and \( R(f_1, f_2) := \text{res}_x(f_1, f_2) \). Then

\[
R(f_2, S_{12}) = R(f_2, m_1 f_1 - m_2 f_2)
\]

\[
= b^{(d_1 - d_2) - d_1}_{d_2} R(f_2, m_1 f_1)
\]

\[
= b^{d_2}_{d_2} R(f_2, m_1) R(f_2, f_1)
\]

\[
= b^{d_2}_{d_2} m_1^{d_2} R(f_2, f_1)
\]

\[
= b^{d_2}_{d_2} c_1^{d_2} y^{k_2} x^{d_1 - d_2} R(f_2, f_1).
\]

**Step 2.** \( R(f_2, S_{12} - h f_2) \).
Let $S_1 - h f_2$ be a step in reducing the S-polynomial and $l := \deg(h)$, then

$$ R(f_2, S_1 - h f_2) = R(f_2, -h f_2 + S_1) $$

$$ = b_{d_2}^{l - d_2} R(f_2, S_1) $$

$$ = b_{d_2}^{l - d_2} b_{d_2}^{c_1 y^k d_2} R(f_2, f_1) $$

$$ = b_{d_2}^{l - 2d_2 c_1 y^k d_2} R(f_2, f_1). $$

**Step 3.** $R(f_2, S_1 - k f_1)$

Let $S_1 - k f_1$ be a step in reducing the S-polynomial. Then

$$ R(f_2, S_1 - k f_1) = R(f_2, m_1 f_1 - m_2 f_2 - k f_1) $$

$$ = R(f_2, -m_2 f_2 + (m_1 - k) f_1) $$

$$ = b_{d_2}^{(d_1 - d_2) - d_2} R(f_2, (m_1 - k) f_1) $$

$$ = b_{d_2}^{d_1 - 2d_2} R(f_2, m_1 - k) R(f_2, f_1). $$

Let $k := c_k y^x x^v$. Performing Gaussian elimination on the rows of $Syl(f_2, m_1 - k)$ that contain coefficients of $m_1 - k$ using the rows corresponding to the coefficients of $f_2$, we obtain a triangularized matrix and the resultant will be equal to:

$$ R(f_2, m_1 - k) = b_{d_2}^* \prod (c_1 y^{k_1} - p(b_i)), $$

where $p$ is a univariate polynomial and $b_{d_2}^*$ is a power of $b_{d_2}$. Therefore we have:

$$ R(f_2, S_1 - k f_1) = b_{d_2}^{l - d_2} b_{d_2}^* \prod (c_1 y^{k_1} - p(b_i)) R(f_2, f_1). $$

**Step 4.** $R(f_2, S_1 - h f_2 - k f_1)$

$$ R(f_2, S_1 - h f_2 - k f_1) = R(f_2, m_1 f_1 - m_2 f_2 - h f_2 - k f_1) $$

$$ = R(f_2, -m_2 f_2 + (m_1 - k) f_1) $$

$$ = b_{d_2}^{l - s - d_1} R(f_2, (m_1 - k) f_1) $$

$$ = b_{d_2}^{l - s - d_1} R(f_2, m_1 - k) b_{d_2}^{t - s - d_1}, $$

$$ = b_{d_2}^{l - s - d_1} \prod (c_1 y^{k_1} - p(b_i)) b_{d_2}^{t - s - d_1}, $$

where $t = \deg(-m_2 - h) = \deg(m_2 + h) \leq \max\{\deg(m_2), \deg(h)\}$ and $s = \deg(m_1 - k)$ and therefore $\deg((m_1 - k) f_1) = s + d_1$ and $b^*$ and $p$ are as above.

Finally, we know that the normal form of $S_1$ can be written as $S_1 - \sum_{i=1}^{i} h_i f_i$, where $h_i$ are the cofactors. Then the above computations can be adapted for computing $R(f_2, S_1 - \sum_{i=1}^{i} h_i f_i)$ in terms of degrees of $h_i$ and $f_i$ and also coefficients of $f_i$.

**Note.** If \{f_1, f_2\} is a Gröbner basis, then $S_1$ can be reduced to zero with respect to \{f_1, f_2\}. From the above steps in the special case that all of the reduction steps were done only by $f_2$, $R(S_1, f_2)$ can be written in terms of
R(f_2, f_1) and some coefficients in \( K \) and some monomials in \( y \). But since reductions are only done using \( f_2 \) we can conclude that there exists a polynomial \( h \) such that \( S_1^2 = hf_2 \). Therefore \( f_2|S_1^2 \) and then \( R(S_1^2, f_2) = 0 \). So \( \{f_1, f_2\} \) being a Gröbner basis means that \( R(f_2, f_1) = 0 \), which means that \( f_1 \) and \( f_2 \) have a common factor that contains \( x \) with positive degree.

### 3.2 Expansion Problem

Our motivation to study the elimination problem was originally to give an incremental algorithm for lexicographic Gröbner basis computation, based on induction on the number of variables. The algorithm that was first suggested in [13] is as follows.

Let \( I \) be the ideal in \( \mathbb{K}[x_1, x_2, \ldots, x_n] \) generated by \( F_0 = \{f_1, \ldots, f_m\} \), \( I_i \) the \( i \)-th elimination ideal of \( I \) and \( G_i \) its reduced Gröbner basis. Given \( F_0 \), assume that we can compute \( F_i \) iteratively using resultants. Then, having \( F_{n-1} \) compute \( G_n \) by a GCD algorithm for the case we arrive to univariate non zero resultants. Now, having \( F_{n-1} \) and \( G_n \) we are interested in finding an algorithm that computes \( G_{n-1} \). We can iterate such an algorithm until we have \( G_0 \).

So we are concerned with the following problem:

**The Expansion Problem.** Given \( F_{i-1} \), a generating set for \( I_{i-1} \) and \( G_i \), the reduced Gröbner basis of \( I_i \), find \( G_{i-1} \), the reduced Gröbner basis of \( I_{i-1} \).

First, based on the Elimination Property of Gröbner basis and also the uniqueness of the reduced Gröbner basis, we have the following observation:

If \( G_0 \) and \( G_1 \) are the reduced Gröbner bases of \( I \) and \( I_1 \) with respect to the lexicographic order \( (x_1 > \ldots > x_n) \), then \( G_1 \subseteq G_0 \).

We suggest the following modification of Buchberger’s algorithm for the expansion problem:

- **Reduce** \( F_{i-1} \) by \( G_i \):
  1. consider \( F_{i-1} \subset K[x_{i+1}, \ldots, x_n][x_i] \).
  2. reduce coefficients of polynomials in \( F_{i-1} \) by \( G_i \).

- **Compute** \( G_{i-1} \) in the following way:
  1. Compute \( \{NF(Spol(f, g))|f, g \in F_{i-1} \setminus (F_{i-1} \cap K[x_i, \ldots, x_n])\} \)
  2. Compute \( \{NF(Spol(f, g))|f \in F_{i-1} \setminus (F_{i-1} \cap K[x_i, \ldots, x_n]), g \in G_i\} \)
  3. Run Buchberger’s algorithm on the union of the sets above and autoreduce

Removing the condition for the Gröbner basis to be reduced, the following more general question arises naturally:

Given \( G_1 \), a Gröbner basis which is not necessarily reduced, how to **construct** \( G_0 \), a Gröbner basis of \( I \) such that \( G_1 \subseteq G_0 \)? Note that the existence of such \( G_0 \) is obvious.
In the following there are some problems related to the elimination and expansion problems.

1. Investigate possibilities of generating $I_1$ by random combinations of the resultants with coefficients from the polynomial ring.

2. Investigate the degenerate cases of Theorem $4$. Suppose that all the resultants are zero but there’s no common factor for all of the polynomials. Considering degrees of the polynomials, can we say how many of these cases can happen?

3. Let $f_1, \ldots, f_m \in K[x_1, x_2, \ldots, x_n]$ be generic polynomials and $r_{ij}$ as above. Does there exist $e_{ij} \in K[x_2, x_3, \ldots, x_n]$ such that $I_1 = \langle \frac{r_{ij}}{e_{ij}} \mid 1 \leq i < j \leq m \rangle$? the well-known concept of the extraneous factor in Resultants?

4. Investigate possible connections between this work and the work of M. Green on partial elimination ideals [8].

4 Conclusions

In this paper we study elimination ideals as a connection between Gröbner bases and resultants. For the case of ideals generated by two polynomials in two variables, which is both a starting point for general ideals and interesting in its own right (plane curves), we prove that if the resultant of the generators is zero then the elimination ideal is the zero ideal and vice versa. In the case of non-zero resultant, we identify the variety of the resultant in terms of the projection of the variety of the ideal and the variety of the coefficients of the generators. Actually we give an affine version for this well known result. Knowing the variety of the resultant gave us the ability to compare it with the variety of the elimination ideal and therefore to compare their factors and see that the resultant has more factors than the Gröbner basis generator. Moreover, in some cases the generator of the elimination ideal and the resultant present the same factors, but with different multiplicities.

The next step was to explore the difference between these multiplicities. A simple case, when the resultant is square free, is dealt completely expressing the generator of the elimination ideal as a fraction of the resultant and an explicit factor. If the resultant is not square free, we give examples in order to show that the situation may be complicated and counter-intuitive.

For ideals generated by any number of polynomials in any number of variables, we were able to identify the difference between the variety of the ideal generated by the resultants of the pairs of the polynomials in the basis and the variety of the elimination ideal. And indeed the difference is considerable.

A question that naturally arose from our work is whether the resultant of Gröbner basis members have a special structure or some strong property. Towards that end, if $S_{12}$ is the S-polynomial of $f_1$ and $f_2$, we show that the resultant of $S_{12}$ and $f_2$ is the resultant of $f_1$ and $f_2$ multiplied by a monomial.
Our motivation for dealing with the elimination problem stems from an attempt to devise an incremental algorithm for Gröbner basis computation. A second problem related to this attempt is the expansion problem. For the expansion problem we give a modification of Buchberger's algorithm that takes advantage of having part of the Gröbner basis based on the elimination property of the Gröbner basis and uniqueness of the reduced Gröbner basis.

Concluding, in this paper we deal with the base cases of the connection between Gröbner bases of elimination ideals and resultants. Our results are preliminary but indicate the complexity of the general case, as well as solve some of the special cases.

Acknowledgments

The authors would like to express their gratitude to Prof. B. Buchberger, who helped with identifying and formulating the expansion problem as an independent problem. Also he helped with the clarification of ideas and by being critical about the formulations of definitions and theorems, assertions, algorithms etc. Dr. M. Kauers provided us with helpful hints during discussions. The authors highly appreciate the valuable comments from Prof. H. Hong and Dr. E. Tsigaridas during personal communications with them. The first author would like to thank the second and third author for introducing him to the topic and generously sharing their ideas and results with him.

All the authors were supported by the strategic program "Innovatives OÖ 2010 plus" of the Upper Austrian Government". The second and third authors were also supported by the Austrian Science Fund (FWF) grant W1214-N15, projects DK1 and DK6. Part of the research of the second author was carried out during a stay at the mathematics department of UC Berkeley supported by a Marshall Plan Scholarship. The third author is partially supported by Austrian Science Fund grant P22748-N18.

References

[1] B. Buchberger. Ein Algorithmus zum Auffinden der Basiselemente des Restklassenringes nach einem nulldimensionalen Polynomsystem. PhD thesis, 1965.

[2] B. Buchberger. Ein Algorithmisches Kriterium für die Lösbarekeit eines Algebraischen Gleichungssystems. Aequationes mathematicae, 4(3):374–383, 1970.

[3] B. Buchberger, G.E. Collins, and R. Loos, editors. Computer Algebra - Symbolic and Algebraic Computation, volume Supplement Nr. 4 (1st ed.) of Computing (Archiv for Informatics and Numerical Computation). Springer Verlag Wien, 1982. (2nd edition: Springer-Verlag Wien-New York, 1982, 1983; Reprinted: World Publishing Corporation, Beijing, 1988; Russian
translation: translated by V.P. Gerdt, D.Yu.Grigoryev, V.A. Rostovtsev, S.Yu. Slavyanov, Mir Publishing Company, Moscow, 1986).

[4] D. Cox, J. Little, and D. O’Shea. *Ideals, Varieties, and Algorithms : An Introduction to Computational Algebraic Geometry and Commutative Algebra*. Springer, 2005.

[5] D. Eisenbud. *Commutative algebra with a view toward algebraic geometry*, volume 150 of *Graduate Texts in Mathematics*. Springer-Verlag, 1995.

[6] I. Emiris and B. Mourrain. Matrices in elimination theory. *Journal of Symbolic Computation*, 28(1-2):3–44, 1999.

[7] J. C. Faugère. A new efficient algorithm for computing Gröbner bases without reduction to zero (F5). In *Proceedings of the 2002 international symposium on Symbolic and algebraic computation*, ISSAC ’02, pages 75–83, New York, NY, USA, 2002. ACM.

[8] D. J. Green. *Gröbner Bases and the Computation of Group Cohomology*. Springer-Verlag, 2003.

[9] W. Gröbner. Über die eliminationstheorie. *Monatschafte für Mathematik*, 5:71–78, 1950.

[10] M. M. Kapranov I. M. Gelfand and A. V. Zelevinski. *Discriminants, resultants, and Multidimensional Determinants*. Birkhäuser, 1994.

[11] D. Lazard. Ideal bases and primary decomposition: Case of two variables. *Journal of Symbolic Computation*, 1(3):261 – 270, 1985.

[12] E. W. Mayr and A. R. Meyer. The complexity of the finite containment problem for petri nets. *Journal of ACM*, 28(3):561–576, July 1981.

[13] H. Rahkooy and Z. Zafeirakopoulos. Using resultants for inductive gröbner bases computation. *ACM Communications in Computer Algebra*, 45(1), 2011.

[14] B. L. van der Waerden. *Algebra*, volume 1. Springer, New York, 7th edition, 1991. Based in part on lectures by E. Artin and E. Noether.