On Computing Elimination Ideals Using Resultants with Applications to Gröbner Bases

Hamid Rahkooy, Zafeirakis Zafeirakopoulos

REPORT ON VISITING UC BERKELEY UNDER MARSHAL PLAN SCHOLARSHIP

Advisor at JKU:	*Host at UC Berkeley:*
Bruno buchberger	Bernd Sturmfels

Contents

Abstract

In this report we investigate possible ways of generating the elimination ideal using the set of Sylvester resultants of pairs of all polynomials in a given basis for the ideal. We characterize the variety of this ideal and its difference with the variety of the elimination ideal. In the case of an ideal generated by two polynomials in two variables, we show that the factors and/or the multiplicities of the resultant and the generator of the elimination ideal can be different. Finding an alternative way (using resultants) for computing the elimination ideals, we suggest an incremental algorithm for Gröbner bases computation that performs induction on the number of variables.

1 Introduction

1.1 Motivation and Literature Review

Gröbner bases theory has been discovered, extended and popularized by Buchberger in his PhD thesis in 1965 and subsequent papers and books [3, 4, 6, 5]. Buchberger's algorithm is the main tool in this theory. This theory has become the subject or a part of lots of books in mathematics [1, 9, 17, 2, 8, 21], as well as other branches of science and engineering [23, 13].

Buchberger discovered two criteria which help decreasing the number of unnecessary computations [3, 4]. There are modifications making the algorithm faster in special cases [20]. Faster algorithms and techniques have been found, e.g. Faugére's F4 that uses linear algebra [11] and his F5, the first of the so called signature-based algorithms, which avoids computing a lot of polynomials that would be reduced to zero [12].

In spite of the attempts to make computations more efficient, Mayr and Meier have given an explicit example for which the complexity of the Gröbner basis computation is doubly exponential in terms of the number of variables and other parameters [19].

As the complexity depends on the number of variables, computations on ideals with less variables might be drastically faster. This motivates us to think of an incremental approach which is based on the induction on the number of variables in the ideal. Among inductive approaches on computations in ideals, one can name Hermann's seminal work on ideal membership [15]. However we are unaware of any such inductive approach to the Gröbner basis computation.

This discussion lead us to think of the part of a Gröbner basis that does not contain one of the variables. Such a subset of the ideal is called the elimination ideal and it has been shown by Buchberger that it can be computed by a special kind of Gröbner basis, the lexicographic Gröbner basis, due to the elimination property of the Gröbner bases [4]. Wang's book on elimination methods gives a thorough review of the topic [25]. Having the elimination ideal of an ideal I, i.e., a (Gröbner) basis for the elimination ideal, then we ask how difficult it is to compute a Gröbner basis for the ideal I, containing the Gröbner basis of the elimination ideal. In the following we state the main problems more accurate.

- **Elimination problem** How to find a basis for the elimination ideal, not necessarily a Gröbner basis?
- **Expansion Problem.** Given a generating set for the ideal and a (the reduced) Gröbner basis for the elimination ideal , find a (the reduced) Gröbner basis of the ideal.

Based on those problems we propose an algorithm for computing Gröbner basis with indution on the number of variables. A sketch of such an algorithm appeared in [22].

Algorithm. Given a basis for the ideal, iteratively use resultants to find a basis for the elimination ideals. Then compute the Gröbner basis for the elimination ideals and taking advantage of having it, compute the Gröbner basis of the ideal by a modified version of the Buchberger's algorithm.

$$\begin{tikzcd}
K[x_1,\dots,x_n] \trianglerighteq I = \langle f_1,\dots,f_m\rangle \arrow[d, "\text{Resultants}"'] & G_0 \subseteq K[x_1,\dots,x_n] \\
K[x_2,\dots,x_n] \trianglerighteq I_1 = \langle F_1\rangle \arrow[d, "\text{Resultants}"'] \arrow[ur] & \vdots \arrow[u, "\text{modified B. Alg.}"'] \\
\vdots \arrow[d, "\text{Resultants}"'] \arrow[ur] & G_{n-2} \subseteq K[x_{n-1},x_n] \arrow[u, "\text{modified B. Alg.}"'] \\
K[x_n] \trianglerighteq I_{n-1} = \langle F_{n-1}\rangle \arrow[r, "\text{GB=GCD}"'] \arrow[ur] & GCD(F_{n-1}) =: G_{n-1} \subseteq K[x_n] \arrow[u, "\text{modified B. Alg.}"']
\end{tikzcd}$$

In this report we mainly focus on studying the elimination ideals by means of the resultants, which is an old and central topic in polynomial algebra. Historically the motivation comes from the solution of polynomial systems via triangularization, the desire to reduce the solution of a system in n variables to the solution of systems in less variables. In this context, many different tools have appeared and in this report we investigate some of the connections between them. The two objects we will focus on are the first elimination ideal and the resultant (for definitions see Section 2).

Resultants has been considered among others by Sylvester, Bezout, Dixon, Macaulay and van der Waerden [24]. W. Gröbner wrote an article on this topic in 1949 [14]. A review of the topic has been given by Emiris and Mourrain in [10]. Gelfand, Kapranov and Zelevinski in [16] 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*.

Based on the elimination property of Gröbner basis and the fact that we can algorithmically compute Gröbner bases one can compute a Gröbner basis for the elimination ideal. 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 discard many 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. Secondly, it provides very little intuition about what the elimination ideal represents. Our goal is to explicitly compute a basis for the elimination ideal of a given ideal.

1.2 Results and Structure

In section 2 we provide the reader with the main definitions and notations that will be used in this report. Then we attack the elimination problem in section 3. The idea is to try to make the ideal generated by a set of resultants as big as (and as close to as) the elimination ideal, possibly by dividing out of the resultants suitable factors. Some general lemmata and propositions are given at the beginning of section 3. Then we start by simplifying the problem into the case of ideals generated by two polynomials in two variables in subsection 3.2 We investigate the degenerate case in which the resultant of the generators is zero and the generic case of non-zero resultant separately. In this way we give a rough description of the form of the Gröbner basis in the degenerate case.

In the generic case we focus on the identifying the varieties of the resultant and the elimination ideal in terms of the projection of the variety of the ideal and the variety of the coefficients of the generators, which leads to an affine proof for the variety of resultants. Knowing the variety of the resultant we are able to compare its factors with the factors of the generator of the elimination ideal. Subsection 3.3 is devoted to understanding the case of ideals generated by any number of polynomials in any number of variables. An identification of the difference between the variety of the ideal generated by the resultants and the variety of the elimination ideal is given.

Section 4 is about what the difference in the multiplicities of the resultant and the generator of the the elimination ideal can be, even if they have the same factors. Our set of examples and counterexamples show that it is hard to identify the multiplicity of the factors in general.

One might think that radicality or zero dimensionality can improve the situation so that the multiplicities or factors can be the same. However in section 5 we show that this is not the case by giving several counterexamples.

Next we shortly try to attack the expansion problem by modifying Buchberger's algorithm in section 6. We take advantage of having part of the Gröbner basis, the part that has been computed by solving the elimination problem, and also of the uniqueness of the reduced Gröbner basis.

At the end we classify four main directions for future work in section 7. These include ideas on the elimination and expansion problems, trying to understand the interactions of those problems with other methods in polynomial algebra and also some precise ideas on what the resultants of the members of Gröbner basis might be or what the Gröbner basis of a set of resultants might look like. Searching the complexity of the problems is a natural question that is a future direction in this work.

2 Preliminaries

In this section we provide the necessary definitions, fix notation and present some theorems from the literature that we will use in what follows. All terminology that is not explicitly defined here (elimination order, reduction. etc.) is contained in standard commutative algebra textbooks.

Let $\mathbb{K}$ denote an algebraically closed field (we usually think of $\mathbb{K}$ as being $\mathbb{C}$). A term order $\prec$ is an order on monomials in $\mathbb{K}[x_1, x_2, \ldots, x_n]$ in which 1 is the smallest monomial and it's compatible with monomial multiplication. An example of such a term order is the lexicographic order (which is an elimination order) with $y \prec x$ or $x_n \prec x_{n-1} \prec \ldots \prec x_1$. Let $f_1, \ldots, f_m \in \mathbb{K}[x_1, x_2, \ldots, x_n]$ and for each $1 \leq i \leq m$, write f_i in the form

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

Let $I = \langle f_1, \ldots, f_m \rangle \trianglelefteq \mathbb{K}[x_1, x_2, \ldots, x_n]$ be the ideal generated by $f_1, \ldots, f_m$. A Gröbner basis G for an ideal I with respect to a term order $\prec$ is a basis G such that $\mathrm{lm}_\prec(G) = \mathrm{lm}_\prec(I)$, where $\mathrm{lm}_\prec(G)$ and $\mathrm{lm}_\prec(I)$ are the ideals generated by the leading monomials of g and I respectively.

The above definition of Gröbner basis is not constructive. However there's a well-known algorithm by Buchberger which computes a Gröbner basis by reducing the S-polynomials of each pair of polynomials appearing in the basis by the polynomials of the basis. S-polynomials are defined below and we will resort to them in order to prove Proposition 1.

Definition 1 (S-polynomial)**.** *Given $f_1, f_2 \in \mathbb{K}[x_1, x_2, \dots, x_n]$, we define S_{12}, the S-polynomial of f_1 and f_2, as:*

$$S_{12} = \frac{\operatorname{lcm}(\operatorname{lt}(f_1), \operatorname{lt}(f_2))}{\operatorname{lt}(f_1)} f_1 - \frac{\operatorname{lcm}(\operatorname{lt}(f_1), \operatorname{lt}(f_2))}{\operatorname{lt}(f_2)} f_2,$$

where lt *stand for the leading term (including the leading coefficient).*

The main object of our study is the elimination ideal.

Definition 2 (Elimination ideal [8])**.** *Given an ideal $I \trianglelefteq \mathbb{K}[x_1, x_2, \dots, x_n]$, we denote by I_i the i-th elimination ideal, i.e., $I_i = I \cap \mathbb{K}[x_{i+1}, x_{i+2}, \dots, x_n]$.*

Lemma 3. *Let $I \trianglelefteq \mathbb{K}[x, y]$. Then there is a unique monic polynomial in $\mathbb{K}[y]$, denoted by g, such that $I \cap \mathbb{K}[y] = \langle g \rangle$.*

Proof. Since $\mathbb{K}[y]$ is a principal ideal domain, the ideal $I \cap \mathbb{K}[y]$ is generated by a polynomial $g \in \mathbb{K}[y]$ that is unique up to multiplication by units. □

Theorem 4 (Elimination property)**.** *let G be a Gröbner basis for an ideal I with respect to the lexicographic term order ($x_1 > \ldots > x_n$). Then $G \cap \mathbb{K}[x_{i+1}, x_{i+2}, \dots, x_n]$ is a Gröbner basis for I_i with respect to the lexicographic term order.*

The following theorems deal with the relation between the varieties of I and I_1.

Theorem 5 (Extension theorem [8, 24])**.** *Let $I = \langle f_1, \dots, f_m \rangle \trianglelefteq \mathbb{K}[x_1, x_2, \dots, x_n]$ and for $1 \leq i \leq m$ let h_i be as defined before. Assume that $(c_2, \dots, c_n) \in \mathcal{V}(I_1)$. Then*

$$(c_2, \dots, c_n) \notin \mathcal{V}(h_1, \dots, h_m) \Rightarrow \textit{ there exists } c_1 \textit{ such that } (c_1, \dots, c_n) \in \mathcal{V}(I).$$

In exploring the connection of resultants to the elimination ideal, studying projections of varieties is essential.

Definition 6 (Projection operator)**.** *Let the operator $\pi\,(:)\,\mathbb{K}^n \to \mathbb{K}^{n-1}$ be defined as*

$$\pi((c_1, c_2, \dots, c_n)) = (c_2, c_3, \dots, c_n).$$

By abuse of notation, for $S \subseteq \mathbb{K}^n$ we denote by $\pi(S)$ the set $\{\pi(c) : c \in S\}$ extending the definition element-wise.

Theorem 7 ([8, 24])**.** *Let I, I_1 and h_i for $1 < i < m$ be defined as above. Then*

$$\mathcal{V}(I_1) = \pi(\mathcal{V}(I)) \cup (\mathcal{V}(h_1, \dots, h_m) \cap \mathcal{V}(I_1))$$

Note 8. Not Necessarily $V(h_1, \dots, h_m) \subseteq V(I_1)$. For an example refer to [8].

Theorem 9 (The closure property, §2 in [8])**.** *Let I, I_1 and π be as before. Then*

- *$\mathcal{V}(I_1)$ is the smallest affine variety containing $\pi(\mathcal{V}(I))$, i.e., it is the Zariski closure of $\pi(\mathcal{V}(I))$.*
- *If $\mathcal{V}(I) \neq \emptyset$, then there is an affine variety $W \subsetneq \mathcal{V}(I_1)$ such that $\mathcal{V}(I_1) \setminus W \subset \pi(\mathcal{V}(I))$.*

The object we will try to connect to elimination ideals is the resultant. Resultants give us a geometric view on the elimination problem.

Definition 10 (Sylvester Matrix). *Let R be a commutative ring and $f_1, f_2 \in R[x]$ be of degree d_1, d_2 respectively. The Sylvester matrix $\operatorname{Syl}(f_1, f_2)$ is defined to be the matrix of size $(d_1 + d_2) \times (d_1 + d_2)$ with the following entries: if $1 \leq i \leq d_2$ and $1 \leq j \leq d_1 + d_2$, the entry in the i-th row and j-th column is the $(d_1 + d_2 - j)$-th coefficient of $x^{d_2 - i} f_1$. If $d_2 + 1 \leq i \leq d_1 + d_2$ and $1 \leq j \leq d_1 + d_2$, the entry in the i-th row and j-th column is the $(d_1 + d_2 - j)$-th coefficient of $x^{d_1 - (i - d_2)} f_2$.*

$$\left(\begin{array}{cccccc}
f_{1,d_1} & \cdots & \cdots & f_{1,0} & & \\
 & \ddots & & & \ddots & \\
 & & f_{1,d_1} & \cdots & \cdots & f_{1,0} \\
f_{2,d_2} & \cdots & f_{2,0} & & & \\
 & \ddots & & \ddots & & \\
 & & \ddots & & \ddots & \\
 & & & f_{2,d_2} & \cdots & f_{2,0}
\end{array}\right)
\begin{array}{l}
\left.\vphantom{\begin{array}{c}1\\1\\1\end{array}}\right\} d_2 \\
\left.\vphantom{\begin{array}{c}1\\1\\1\\1\end{array}}\right\} d_1
\end{array}$$

Definition 11 (Resultant). *Let R be a commutative ring. For $f_1, f_2 \in R[x]$, we define the resultant of f_1, f_2 as*

$$\operatorname{res}_x (f_1, f_2) = \det (\operatorname{Syl}(f_1, f_2)) .$$

Resultants have the following two important properties.

Theorem 12 (§6 in [8]). *Let $f_1, f_2 \in \mathbb{K}[x_2, \ldots, x_n][x_1]$ have positive degree in x_1. Then*

- $\operatorname{res}_{x_1} (f_1, f_2) \in I_1$.
- $\operatorname{res}_{x_1} (f_1, f_2) = 0$ *if and only if f_1 and f_2 have a common factor, which has positive degree in x_1, in $\mathbb{K}[x_1, x_2, \ldots, x_n]$.*

When the resultant is not zero we will use the following lemma in order to identify roots of the resultant. This will show us how and when resultants project roots of the system and how this can give us information about the roots of the elimination ideal, roots of the system and multiplicities of the roots of the system.

Lemma 13 (§6 in [8]). *Let $f_1, f_2 \in \mathbb{K}[x_1, x_2, \ldots, x_n]$ have (total) degree N_1 and N_2 respectively, and let $c = (c_2, \ldots, c_n) \in \mathbb{K}^{n-1}$ satisfy the following conditions:*

- *$f_1(x_1, c) \in \mathbb{K}[x_1]$ has degree N_1,*
- *$f_2(x_1, c) \in \mathbb{K}[x_1]$ has degree $p \leq N_2$.*

Then the polynomial $\operatorname{res}_{x_1} (f_1, f_2) \in \mathbb{K}[x_2, x_3, \ldots, x_n]$ *satisfies*

$$\operatorname{res}_{x_1} (f_1, f_2) (c) = h_1(c)^{N_2 - p} \operatorname{res}_{x_1} (f_1(x_1, c), f_2(x_1, c))$$

For the rest of the paper we fix the following notation (except otherwise is explicitly stated):

- $f_1, f_2, \ldots, f_m \in \mathbb{K}[x_1, x_2, \ldots, x_n]$,

- $I = \langle f_1, f_2, \ldots, f_m \rangle$,
- $I_i = I \cap \mathbb{K}[x_{i+1}, x_{i+2}, \ldots, x_n]$,
- Given that I_1 is principal, g is the unique monic generator of I_1,
- $R := \langle \{r_{ij} := \operatorname{res}_x (f_i, f_j) \, | 1 \leq i < j \leq m\} \rangle$
- $\mathcal{R} = \gcd(r_{ij})$ for $1 \leq i < j \leq m$.
- S_{12} is the S-polynomial of f_1 and f_2.
- $h_i \in \mathbb{K}[x_2, x_3, \ldots, x_n]$ is the leading coefficient of f_i, when considered as an element of $\mathbb{K}[x_2, x_3, \ldots, x][x_1]$.
- By $\mathcal{V}(I)$ we denote the variety of the ideal I and if $f_i \in \mathbb{K}[x_1, x_2, \ldots, x_n]$ for $1 < i < m$ we have $\mathcal{V}(f_1, f_2, \ldots, f_m) = \mathcal{V}(\langle f_1, f_2, \ldots, f_m \rangle)$.
- $\mathcal{I}(S)$ is the vanishing ideal of a variety S.

3 Elimination

3.1 General Lemmata

Proposition 1. *Let $f_1, f_2 \in \mathbb{K}[x_1, x_2, \ldots, x_n]$ and assume $h \in \mathbb{K}[x_1, x_2, \ldots, x_n]$ with $\deg_{x_1}(h) > 0$ is their common factor. Then there exist f_1' and f_2' in $\mathbb{K}[x_1, x_2, \ldots, x_n]$ such that $f_1 = h{f_1}'$ and $f_2 = h{f_2}'$. Let $\ell_1 = lm(f_1)$, $\ell_2 = lm(f_2)$, $\ell_1' = lm(f_1')$, $\ell_2' = lm(f_2')$ and $\ell_h = lm(h)$ be the leading monomials of f_1, f_2, f_1', f_2' and h respectively. 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 $\ell = \operatorname{lcm}(\ell_1, \ell_2)$ and $\ell' = \operatorname{lcm}(\ell_1', \ell_2')$. Then

$$\begin{aligned} S_{12} &= \frac{\ell}{\ell_1} f_1 - \frac{\ell}{\ell_2} f_2 \\ &= \frac{\ell}{\ell_1} h f_1' - \frac{\ell}{\ell_2} h f_2' \\ &= h(\frac{\ell}{\ell_1} f_1' - \frac{\ell}{\ell_2} f_2') \end{aligned}$$

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

$$\begin{aligned} h(\frac{\ell}{\ell_1} f_1' - \frac{\ell}{\ell_2} f_2') &= h\left(\frac{\ell'}{{\ell_1}'} f_1' - \frac{\ell'}{{\ell_2}'} f_2'\right) \\ &= hS_{12}'. \end{aligned}$$

□

Proposition 2. *Let $f_1, f_2 \in \mathbb{K}[x_1, x_2, \ldots, x_n]$ with $\deg_{x_1}(f_1) > 0$ and $\deg_{x_1}(f_2) > 0$ such that $\gcd(f_1, f_2) = h \in \mathbb{K}[x_1, x_2, \ldots, x_n]$ with $\deg_{x_1}(h) > 0$ and $I = \langle f_1, f_2 \rangle$. Then $I_1 = \langle 0 \rangle$.*

Proof. Let S be the reduced reduced by f_1 and f_2 form of S_{12}. 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 et $S \neq 0$. Let S'_{12},f'_1,f'_2 and h be as in Proposition 1, and S' be the reduced form of S'_{12} with respect to f'_1 and f'_2. From Proposition 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 $S = hS'$. 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 $I_1 = \langle 0 \rangle$. □

3.2 Two Polynomials

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

Theorem 14.

$$\mathcal{R} \equiv 0 \Leftrightarrow I_1 = \langle 0 \rangle .$$

Proof. ($\Rightarrow$) Assume that $\mathcal{R} \equiv 0$. Then f_1 and f_2 have a common factor h with $\deg_{x_1}(h) > 0$. Then from Proposition 2 we have that $I_1 = \langle 0 \rangle$.

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

At first, we connect the variety of the resultant with the projection of the variety of the ideal I. In the projective space, see [8] and [9], we know that the variety of the resultant describes roots at infinity and affine roots. We provide the reader with the proof in affine case. Indeed the following is an affine description of the roots of the resultant.

Theorem 15.

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

Proof. We need to prove the following three claims:

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

Claim 1. 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 $\mathcal{R}$. Thus $\mathcal{V}(h_1, h_2) \subseteq \mathcal{V}(\mathcal{R})$.
Claim 2. By Theorem 12 we have that $\mathcal{R}$ is in I_1, we have that $\mathcal{V}(I_1) \subseteq \mathcal{V}(\mathcal{R})$. From Theorem 7 we have that $\pi(\mathcal{V}(I)) \subseteq \mathcal{V}(I_1)$, which proves Claim 2.
Claim 3. Let $c \notin \mathcal{V}(h_1, h_2)$. Then we have two cases:

- $h_1(c) \neq 0$ and $h_2(c) \neq 0$. We have that $\mathcal{R}(c) = \operatorname{res}_x(f_1(x, c), f_2(x, c))$. If $\mathcal{R}(c) = 0$ then $\operatorname{res}_x(f_1(x, c), f_2(x, c)) = 0$.

- Either $h_1(c) \neq 0, h_2(c) = 0$ or $h_1(c) = 0, h_2(c) \neq 0$. Without loss of generality, assume that $h_1(c) \neq 0, h_2(c) = 0$. Also assume that d_2 is degree of f_2 and $m < d_2$ is degree of $f_2(x, c)$. From lemma 13 we have that

  $$\mathcal{R}(c) = h_1(c)^{d_2 - m} \operatorname{res}_x(f_1(x, c), f_2(x, c)) .$$

  Since $h_1(c) \neq 0$, if $\mathcal{R}(c) = 0$ then $\operatorname{res}_x(f_1(x, c), f_2(x, c)) = 0$.

So in both of the above cases we have that $\operatorname{res}_x(f_1(x,c), f_2(x,c)) = 0$. Also we have that

$$\begin{aligned} c \in \pi(\mathcal{V}(f_1, f_2)) &\Leftrightarrow \exists c_1 \in \mathbb{K} : (c_1, c) \in \mathcal{V}(f_1, f_2) \\ &\Leftrightarrow \exists c_1 \in \mathcal{V}(f_1(x,c), f_2(x,c)) \\ &\Leftrightarrow \operatorname{res}_x(f_1(x,c), f_2(x,c)) = 0 \end{aligned}$$

Thus $c \in \pi(\mathcal{V}(I))$ and this finishes the proof of Claim 3. □

Corollary 16. $\mathcal{V}(I_1) \subseteq \mathcal{V}(\mathcal{R})$

Proof. We have $\mathcal{V}(I_1) = (\mathcal{V}(h_1, h_2) \cap \mathcal{V}(I_1)) \cup \pi(\mathcal{V}(I))$. Therefore from Theorem 15 we have $\mathcal{V}(I_1) \subseteq \mathcal{V}(\mathcal{R})$. □

The elimination ideal of a bivariate ideal is univariate, thus principal. We denote the unique (up to units) generator of I_1 by g. We prove that the variety of the elimination ideal is the projection of the variety of I, if $\mathcal{R}$ is not identically zero.

Theorem 17. *If $f_1, f_2 \in \mathbb{K}[x,y]$ and $\mathcal{R}$ is not identically zero, then*

$$\mathcal{V}(I_1) = \pi(\mathcal{V}(I))$$

Proof. Assume that $\mathcal{R}$ is not identically 0. Since $\mathcal{R}$ vanishes at $\pi(\mathcal{V}(I))$ and $\mathcal{R}$ is a non-zero univariate polynomial, we have that $\pi(\mathcal{V}(I))$ is finite. By Theorem 9, we have that $\mathcal{V}(I_1)$ is the Zariski closure of $\pi(\mathcal{V}(I))$. Since finite sets are Zariski closed, we have that $\mathcal{V}(I_1) = \pi(\mathcal{V}(I))$. □

Let $f_1, f_2 \in \mathbb{K}[x_1, x_2, \ldots, x_n]$ be the polynomials

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

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

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

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 18.

$$\gcd(h_1, h_2) \,|\mathcal{R},$$

$$\gcd(t_1, t_2) \,|\mathcal{R}$$

and

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

for $k = 1, 2$.

Note 19. Theorem 15 does not imply the statement of lemma 18 about leading coefficients because it doesn't say anything about the multiplicities of the factors of the gcd of the leading coefficients.

3.3 More Than Two Polynomials

We consider the case of $I = \langle f_1, \ldots, f_m \rangle$, where $m > 2$ and $f_i \in \mathbb{K}[x_1, x_2, \ldots, x_n]$

The following theorem describes the roots of R.

Theorem 20. *Let $V_{ij} = \{\pi (\mathcal{V}(f_i, f_j)), \mathcal{V}(h_i, h_j)\}$ for $1 \leq i < j \leq m$ and C be the Cartesian product $C = \otimes_{1 \leq i < j \leq m} V_{ij}$. Then*

$$\mathcal{V}(R) = \bigcup_{c \in C} \bigcap_{i=1}^{\binom{m}{2}} c_i$$

Proof. By definition

$$\mathcal{V}(R) \quad = \quad \bigcap \mathcal{V}(r_{ij})$$

By Proposition 15 we have that $\mathcal{V}(r_{ij}) = \pi(\mathcal{V}(f_i, f_j)) \cup \mathcal{V}(h_i, h_j)$. Then

$$\begin{aligned} \mathcal{V}(R) &= \bigcap (\pi(\mathcal{V}(f_i, f_j)) \cup \mathcal{V}(h_i, h_j)) \\ &= \bigcup_{c \in C} \bigcap_{i=1}^{\binom{m}{2}} c_i. \end{aligned}$$

□

Corollary 21.

With the above notation we have

- $\mathcal{V}(h_1, \ldots, h_m) \subseteq \mathcal{V}(R)$
- $\pi(\mathcal{V}(I)) \subseteq \mathcal{V}(R)$

Proof. For the first part, since $\mathcal{V}(h_i, h_j) \subseteq \mathcal{V}(r_{ij})$ for all $1 \leq i < j \leq m$, we conclude that $\bigcap \mathcal{V}(h_i, h_j) \subseteq \mathcal{V}(R)$ and therefore $\mathcal{V}(h_1, \ldots, h_m) \subseteq \mathcal{V}(R)$.

For the second part we have $\pi(\mathcal{V}(I)) \subseteq \pi(\mathcal{V}(f_i, f_j))$ for all $1 \leq i < j \leq m$ and thus $\pi(\mathcal{V}(I)) \subseteq V(r_{ij})$ for all $1 \leq i < j \leq m$. Therefore $\pi(\mathcal{V}(I)) \subseteq V(R)$.

□

Note 22. Not necessarily $\bigcap \pi(\mathcal{V}(f_i, f_j)) \subseteq \pi(\mathcal{V}(I))$.

Corollary 21 states that all the factors of $\gcd(h_1, \ldots, h_m)$ are factors of $\mathcal{R}$ as well. It doesn't say anything about their multiplicity. However we have a divisibility condition.

Lemma 23.

$$\gcd(h_1, \ldots, h_m) | \mathcal{R}$$

Proof. For $1 \leq i < j \leq m$ we have that $\gcd(h_i, h_j) \,|\, \mathrm{res}_x(f_i, f_j)$. Thus

$$\gcd(\gcd(h_i, h_j)) \,|\, \gcd(r_{ij})$$

which means that $\gcd(h_1, \ldots, h_m) | \mathcal{R}$. □

Note 24. If we set $f_i = f_1$ in R and consider the ideal $R' := \langle \{res_x(f_1, f_j) | 2 \leq j \leq m\} \rangle$ 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.

Lemma 25. *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. $R \trianglelefteq \mathbb{K}[y]$ and $\mathbb{K}[y]$ is a PID, thus $R = \langle \mathcal{R} \rangle$. Since $\mathcal{R} \in I_1$, we have $g | \mathcal{R}$. □

Lemma 25 says that although $\mathcal{R}$ itself does not necessarily generate the elimination ideal, the product of some of its factors does. In [18] 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.

4 Multiplicities

Since we know the factors of g and $\mathcal{R}$, the next natural question is to identify their multiplicities. Let $I = \langle f_1, f_2 \rangle \trianglelefteq \mathbb{K}[x, y]$ and $I_1 = \langle g \rangle \trianglelefteq \mathbb{K}[y]$ be its first elimination ideal. We start by stating an obvious upper bound.

Lemma 26. *If $c \in \mathbb{C}$ is a root of g with multiplicity μ then c is a root of $\mathcal{R}$ with multiplicity ν and $\mu \leq \nu$.*

Proof. For all $p \in \mathbb{K}[y]$ and $\mu \in \mathbb{N}^*$ such that $p^\mu | g$ we have $p^\mu | \mathcal{R}$ since $g | \mathcal{R}$ due to Lemma 25. □

The rest of this section investigates the problems faced when trying to establish a lower bound. We will stick with the notation μ and ν for multiplicities of roots of g and $\mathcal{R}$ respectively. In case of different roots one should think of μ and ν as vectors and when comparing them to a number, by abuse of notation, we pick the coordinate for which the largest difference between the respective μ and ν values happen.

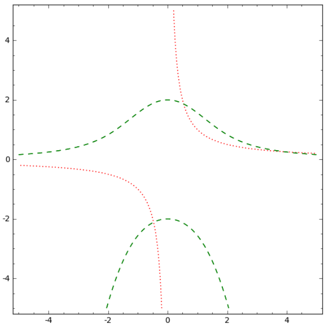
4.1 $\nu = 1$

We first examine possible cases when all roots of $\mathcal{R}$ have multiplicity 1. We proceed according to μ in order to see that even in that case the situation is not clear.

4.1.1 $\mu = 0$

In the following example, one of the factors of $\mathcal{R}$ appears in g, while the other one does not.

Example 27. Let $f_1 = xy - 1, f_2 = x^2y + y^2 - 4 \in \mathbb{C}[x, y]$. Then $\mathcal{R} = y(y^3 - 4y + 1)$ and $I_1 = \langle y^3 - 4y + 1 \rangle$. It is obvious that $c = 0$ is a root of $\mathcal{R}$ with multiplicity 1, but it is a root of g with multiplicity 0.



f_1	$xy-1$
f_2	x^2y+y^2-4
h_1	y
h_2	y
g	y^3-4y+1
$\mathcal{R}$	$y(y^3-4y+1)$

We observe though that this ideal is radical, y is the common factor of h_1 and h_2 and that $g = \frac{\mathcal{R}}{\gcd h_1, h_2}$. However this is not the case for all of the radical ideals. An example of such an ideal is 4.2.1. Neither is the case under the stronger assumption that g is square-free, e.g. 27. We are not aware of an example in which I is radical and $\mathcal{R}$ and g are square-free but $g \neq \frac{\mathcal{R}}{h}$.

Trying to find a counterexample for the above case, we were lead to the following general question.

Question 28. Given $\mathcal{R}, g$ (and maybe h) in $\mathbb{K}[y]$, find $f_1, f_2 \in \mathbb{K}[x,y]$ such that $\mathcal{R} = \operatorname{res}_{x_1}(f_1, f_2)$ and g is the unique generator of the elimination ideal of the ideal generated by f_1 and f_2.

One way to attack this problem is explained in the following very special case. Let $\mathcal{R} = (y-1)(y-2)(y-3), h = gcd(h_1, h_2) = (y-2)(y-3)$.
Ansatz. Let $f_1 = (y-2)(y-3)x^2 + cx + d$ and $f_2 = (y-2)(y-3)x + a$, where $c \in \mathbb{K}[y], a, d \in \mathbb{K}$. Then

$$\begin{aligned}\mathcal{R} &= det \begin{pmatrix} (y-2)(y-3) & c & d \\ (y-2)(y-3) & a & 0 \\ 0 & (y-2)(y-3) & a \end{pmatrix} \\ &= (y-2)(y-3)a^2 - (y-2)(y-3)(ac - d(y-2)(y-3)) \\ &= (y-2)(y-3)(a^2 - ac - d(y-2)(y-3))\end{aligned}$$

However we know that $\mathcal{R} = (y-1)(y-2)(y-3)$. By coefficient comparison we have that

$$\begin{aligned} y-1 &= a^2 - ac - d(y-2)(y-3) \\ &= -dy^2 + 5dy - ac + a^2 - 6d \end{aligned}$$

Setting $d = 0$, the following answer can be achieved:

$$\begin{aligned} f_1 &= (y-2)(y-3)x^2 - ixy \\ f_2 &= (y-2)(y-3)x + i. \end{aligned}$$

There are obviously other answers. The ideal generated by f_1 and f_2 is radical. $\mathcal{R}$ and g are square free and $g = \frac{\mathcal{R}}{h}$.

The following is a slightly different ideal which is radical, $\mathcal{R}$ and g are square free and it does satisfy $g = \frac{\mathcal{R}}{h}$.

Example 29. Let $f_1 = (y-2)(y-3)x^2 - 2xy, f_2 = (y-2)(y-3)x+2$. Then $\mathcal{R} = 4(y-2)(y-3)(y+1), G = \{x-1, y+1\}$, where G is the reduced Gröbner basis.

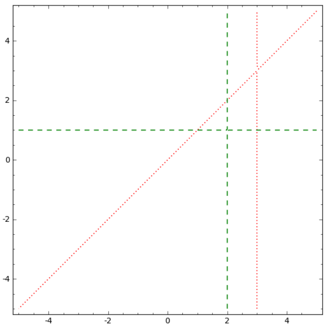
4.1.2 $\mu = 1$

If we consider $f_1 = x$, $f_2 = y$, then obviously $g = \mathcal{R} = y$. Then all factors of $\mathcal{R}$ appear in g. In that case, computing the Gröbner basis is equivalent to computing $\mathcal{R}$.

4.2 $\nu > 1$

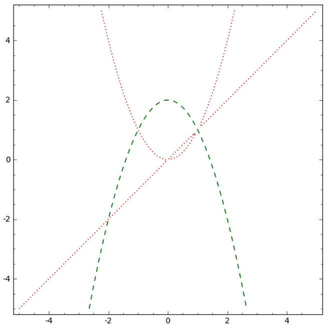
Let us now assume that $\mathcal{R}$ contains factors with multiplicity greater than 1.

4.2.1 $\mu < \nu$



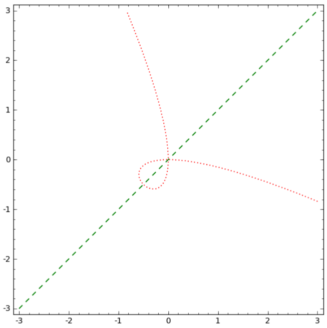
f_1	$(x-y)(x-3)$
f_2	$(y-1)(x-2)$
h_1	1
h_2	$y-1$
g	$(y-2)(y-1)$
$\mathcal{R}$	$(y-2)(y-1)^2$

One is 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.



f_1	$-(x^2+y-2)$
f_2	$(x-y)(y-x^2)$
h_1	1
h_2	1
g	$(y+2)(y-1)^2$
$\mathcal{R}$	$-4(y+2)(y-1)^3$

4.2.2 $\mu = \nu$

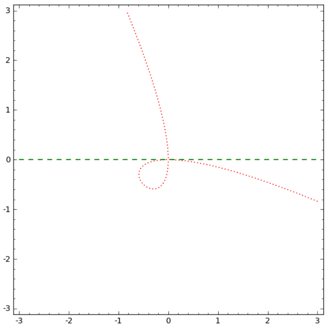


f_1	$x^3 + 3x^2y + 3xy^2 + 4xy + y^3$
f_2	$x - y$
h_1	1
h_2	1
g	$\frac{1}{2} \cdot (2y + 1) \cdot y^2$
$\mathcal{R}$	$(-4) \cdot (2y + 1) \cdot y^2$

4.3 Towards a conjecture

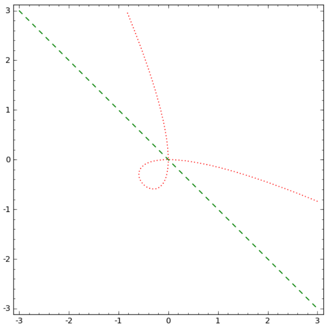
Now we present a series of four examples that illustrate that the multiplicities of the factors of g are not directly connected to the multiplicity of roots that correspond to that factor. In these four examples we take the algebraic curve $x^3+3x^2y+3xy^2+4xy+y^3$ and a line.that is rotated by 90 degrees in each successive example.

Example 30.



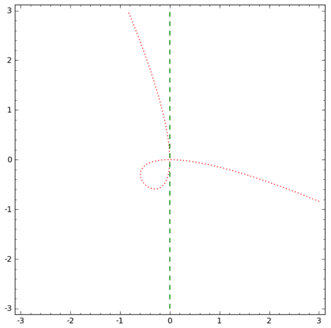
f_1	$x^3 + 3x^2y + 3xy^2 + 4xy + y^3$
f_2	y
h_1	1
h_2	y
g	y
$\mathcal{R}$	y^3

Example 31.



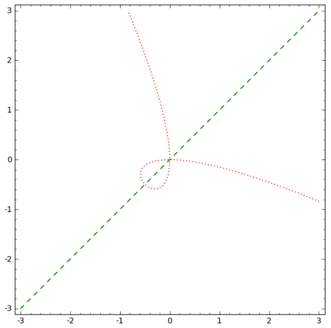
f_1	$x^3 + 3x^2y + 3xy^2 + 4xy + y^3$
f_2	$x + y$
h_1	1
h_2	1
g	y^2
$\mathcal{R}$	$4y^2$

Example 32.



f_1	$x^3+3x^2y+3xy^2+4xy+y^3$
f_2	x
h_1	1
h_2	1
g	y^3
$\mathcal{R}$	$-y^3$

Example 33.



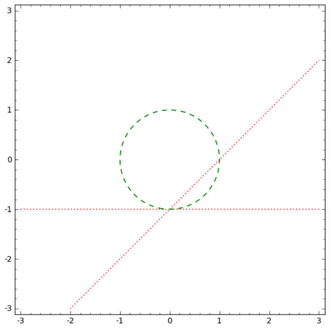
f_1	$x^3+3x^2y+3xy^2+4xy+y^3$
f_2	$x-y$
h_1	1
h_2	1
g	$\frac{1}{2}(2y+1)y^2$
$\mathcal{R}$	$-4(2y+1)y^2$

We note that in Example 31 and Example 33, the intersection point has multiplicity 2, while in Example 30 and Example 32, the intersection point has multiplicity 3. Observe that in the case $f_2 = x$ the multiplicity is preserved in the corresponding factor of g, while in the case $f_2 = y$ it is reduced to 1. These examples support evidence for the following conjecture.

Conjecture 34. Assume for simplicity that no two affine roots have the same y-coordinate. Then the multiplicity of a factor of g is equal to the multiplicity of the affine root this factor represents, as long as no common tangent direction of the two curves at this root is parallel to the y-axis.

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

Example 35.



f_1	$-1(y+1)(x-y-1)$
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 is preserved with the correct multiplicity, but the factor $(y+1)$ drops by 1. We claim that this is due to the fact that the triple root is only counted twice, once for the intersection of $(x-y-1)$ with the circle and once for the intersection of $(y+1)$ with the circle, instead of being counted as double in the latter case. This happens because $(y+1)$ and the circle have a common tangent parallel to the y-axis at their intersection.

5 Counterexamples

One might think that for the special cases of zero dimensional and/or radical ideals R is a basis for the elimination ideal. However this is not the case. In this section we give counterexamples for cases with strong assumptions.

5.1 I being radical or zero-dimensional does not imply that $\mathcal{V}(\mathcal{R}) = \mathcal{V}(g)$

Discussing multiplicities in subsection 4.1 we already gave an example that radical ideals are not necessarily generated by the resultant. We give another example here.

Counter-example 36. Let $f_1 = (y^2-y)x^2 + x$ and $f_2 = (y^2-y)x + y$. Then $G = \{x, y\}$ and therefore the ideal is both radical and zero dimensional. However

$$g = y \neq y^2(y-1)^2 = \mathcal{R}.$$

and thus $\mathcal{V}(\mathcal{R}) \neq \mathcal{V}(g)$.

5.2 Not necessarily $R = g^{k_1} \operatorname{gcd}(h_1, h_2)^{k_2} \operatorname{gcd}(t_1, t_2)^{k_3}$.

Let h denote $\operatorname{gcd}(h_1, h_2)$ and t denote $\operatorname{gcd}(t_1, t_2)$. From theorem 15 and its following corollary we can conclude that every factor of $\mathcal{R}$ is either a factor of g or a factor of h. Or equivalently $\mathcal{V}(\mathcal{R}) = \mathcal{V}(hg)$. From lemma 18 we have even the stronger result that $h|\mathcal{R}$ and $t|\mathcal{R}$.

However we cannot conclude that there exist natural numbers k_1, k_2 and k_3 such that $\mathcal{R}^{k_1} = g^{k_1} h^{k_2} t^{k_3}$. The following is a counterexample.

Counter-example 37. Let $f_1 = y(\frac{-1}{666}x^2 + \frac{29}{4}x + y^2)$ and $f_2 = x(y+1)$. Then

$$\mathcal{R} = y^3(y+1)^2, g = y^3(y+1)$$

$h = 1$ and $t = 1$. But the extra factor is $e = (y+1)$.

Note 38. The fact that the Resultant of f_1 and f_2 with respect to x does not vanish identically means that there are finitely many projections of roots of the system $\{f_1, f_2\}$ in the y axis. This is enough for our argument in the proof of Theorem 17. Assuming that also the projection of the roots on the x-axis are finitely many does not give us more freedom. Zero dimensionality implies that for each variable, the resultant with respect to that variable does not vanish identically. But since we eliminate variables in a particular order (given by the fixed term order) it is not necessarily a natural condition.

6 Expansion

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 [22] 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 $G_1 \subseteq G_0$.

Now we suggest the following modification of Buchberger's algorithm for the expansion problem:

- Reduce F_{i-1} by G_i:
  1. consider $F_{i-1} \subset K[x_{i+1}, \cdots, x_n][x_i]$.
  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

Although our proposed method is based on induction on the number of variables, we are investigating possibilities of adapting other incremental algorithms which add the polynomials of the basis one by one during the computations. More precisely we are interested in having a signature-based algorithm, e.g., F5, which take advantage of having that part of the Gröbner basis that has one less variable.

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.

7 Future Directions and Questions

In this section we propose some ideas and open problems for future directions of this work. These include problems or new ideas on investigating the relation between resultants and Gröbner basis computation, the elimination and expansion problems, complexity and experimental problems and interactions of the elimination and expansion problems with other computer algebra methods.

7.1 Resultant of Gröbner basis members, Gröbner basis of Resultants

From the proof of Theorem 2, we already know the following in the case of two polynomials in two variables.

Note 39. A common factor of the elements of the basis will be a common factor of the elements of a Gröbner basis. Therefore, before the computation of a Gröbner basis we can check whether there is such a factor or not and this might reduce computations.

This motivates us to ask what more information the resultants could gives us about Gröbner bases or vice versa. The following problems are in this direction.

Question 40.

1. 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?

2. Does a Gröbner basis of resultants have a nice form?

We try to make these questions more precise.

Question a. Let $1 < \ell_n < \ell_{n-1} < \ldots < \ell_1 < k$ be an integer sequence and $g_1, \ldots, g_k$ be a reduced Gröbner basis for I such that

- $g_k \in \mathbb{K}[x_n]$
- $g_{\ell_1}, \ldots, g_{k-1} \in \mathbb{K}[x_{n-1}, x_n,]$
- $\vdots$
- $g_{\ell_n}, \ldots, g_{\ell_{n-1}-1} \in \mathbb{K}[x_2, x_3, \ldots, x_n]$
- $g_1, \ldots, g_{\ell_n - 1} \in \mathbb{K}[x_1, x_2, \ldots, x_n]$.

Then

$$\begin{aligned} r_{ij} = res_{x_1}(f_i, f_j) &= res_{x_1}\left(\sum_{s=1}^{k} a_{i_s} g_s, \sum_{t=1}^{k} b_{j_t} g_t\right) \\ &= \sum_{s=1}^{k} res_{x_1}\left(a_{i_s} g_s, \sum_{t=1}^{k} b_{j_t} g_t\right) \\ &= \sum_{s=1}^{k}\sum_{t=1}^{k} res_{x_1}\left(a_{i_s} g_s, b_{j_t} g_t\right) \\ &\vdots \\ &= A(x_2, \ldots, x_n) res_{x_1}\left(g_s, g_t\right), \end{aligned}$$

where $A(x_2, \ldots, x_n) \in \mathbb{K}[x_2, x_3, \ldots, x_n]$. So knowing the resultants of the Gröbner basis members, we can find what the resultants of generators are. For the resultants of the generators we have

$$res_{x_1}(g_s, g_t) = \begin{cases} 1 & s, t \geq \ell_n \\ g_s^{deg_{x_1}(g_s)} & s \leq \ell_n, t > \ell_n \\ ? & s, t < \ell_n \end{cases}$$

Therefore if we can find a relation for the form of the resultants of members of a reduced Gröbner basis, then we might be able to figure out a form for the resultant of a Gröbner basis. Investigations on special cases like two bivariate polynomials might be helpful.

Question b. Let r_{ij} and r_{kl} be in R. Since none of them contain x_1, their s-polynomial also won't contain x_1. What else can be said about (reduced) Gröbner basis of R? What if R is a basis for I_1?

Also the following question is of interest as it imposes conditions similar to zero dimensionality.

Question 41.

1. What is the relation between $\operatorname{res}_{x_1}(f_1, f_2)$ and $\operatorname{res}_{x_1}(f_1', f_2)$, where f_1' is the reduced form of f_1 with f_2?
2. What is the relation between $\operatorname{res}_{x_1}(f_1, f_2)$ and $\operatorname{res}_{x_1}(g_i, g_j)$, where $G = \{g_1, \ldots, g_k\}$ is a(the) reduced Gröbner basis of $\langle f_1, f_2 \rangle$?

7.2 Elimination and Expansion Problems

1. If I_1 is a principal ideal, then is there any relation between its generator and the resultants of a basis for I? How can we check whether I_1 is a principal ideal without computing a Gröbner basis?
2. Find an invariant of a Gröbner basis algorithm that stops when I_1 is computed.
3. Investigate possibilities of generating I_1 *generically* by random combinations of the resultants with coefficients from the polynomial ring.
4. Explore other inductive approaches (on the number of variables) to Gröbner basis computation as possible alternative solutions to the expansion problem.
5. Investigate the degenerate cases of Theorem 20:
   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?
6. For m univariate polynomials, the resultant system is a set of polynomials in coefficients of these polynomials such that they are zero if and only if the original polynomials have a common root, see [24].

   > If we consider $f_1, \ldots, f_m$ as univariate polynomials in x with coefficients in $\mathbb{K}[y]$, are the members of the resultant system of $f_1, \ldots, f_m$ in the elimination ideal?
   >
   > If so, can we use these polynomials in order to find the generator of I_1?

7. Let $f_1, \ldots, f_m \in \mathbb{K}[x_1, x_2, \ldots, x_n]$ and r_{ij} as above. Then does there exist $e_{ij} \in \mathbb{K}[x_2, x_3, \ldots, x_n]$ such that generically $I_1 = \left\langle \frac{r_{ij}}{e_{ij}} | 1 \leq i < j \leq m \right\rangle$?
8. What if we consider $\langle \operatorname{res}_{x_1}(f, g) \,|\, f, g \in I \rangle$ instead of R?

9. Is there any relation between denominator in question 7 and the well-known concept of the extraneous factor in Resultants?

10. Is there any relation between this work and the work of M. Green on *partial elimination ideals* [13]?

7.3 Complexity, Computational Aspects, Experiments

1. Explore the complexity of the elimination steps in the proposed Gröbner basis algorithm:

   - Doubly exponentially many polynomials: $(O(m^{2^n}))$.
   - Exponential growth of the degree: $O(2^n d^2)$, (d is the maximum degree of the elements with respect to x_1).

2. Analyze the complexity of the expansion steps.

3. If resultants give us the elimination ideal, are they faster than Gröbner basis? Make experiments on this.

4. Make systematic experiments on the expansion problem and the algorithm.

7.4 Interaction with Other Methods

1. Can we use *Cylindrical Algebraic Decomposition*?

   - CAD uses resultants and discriminants in order to find the projections of the real variety [7]. Can we find the projections of the complex variety in a similar way?
   - Does adding discriminants to the set of resultants help with the multiplicity problem?

2. Can we use multivariate resultants instead of a set of Sylvester resultants?

3. Is there any intersection between computing the elimination ideal using R and *Triangular Decomposition*?

8 Conclusions

Trying to devise an incremental algorithm for Gröbner basis computation, we came across two main problems, the well-known elimination problem and the expansion problem. This report mainly aimed at answering the first problem, finding a basis for the elimination ideal of a given ideal. We used a set of resultants to generate an ideal quite close to the elimination ideal.

For the case of ideals generated by two polynomials in two variables we divide the problem into the degenerate case where the resultant of the generators is zero and the generic case of non-zero resultant. In the degenerate case we proved that the elimination ideal is the zero ideal. This gave us an indication on the form of the Gröbner basis as well. For the generic case 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 proof 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 extra factors or in some cases the same factors with different multiplicity. Then we explored the difference of the multiplicities via examples. Mostly we gave counterexamples for the natural but not correct expectation that imposing the extra conditions of radicality or zero dimensionality may give us a chance to avoid extra factors in the resultant.

We also tried to understand the more general case of 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.

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. However we are interested in figuring out a signature based algorithm to answer the problem more efficiently. Also as future directions of this work, we are intending to attack the elimination and expansion problems with other methods, consider interaction of this work with other known methods in polynomial algebra and try to figure out tighter relations between Gröbner bases and resultants. Understanding the complexity of the problems is a natural future direction.

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 a proof for the zero dimensional case for the extension of roots of the elimination ideal. The authors highly appreciate the valuable comments from Prof. H. Hong, M. Gallet, and Dr. E. Tsigaridas during personal communications with them.

The research was supported by the strategic program "Innovatives OÖ 2010 plus" by the Upper Austrian Government and partially supported by the Austrian Science Fund (FWF): W1214-N15, project DK1. The second author was partially supported by Austrian Science Fund (FWF) grants P20347-N18 and P22748-N18. Also part of this research is done when the first author was visiting mathematics department of UC Berkeley under Marshall Plan Scholarship.

References

[1] W. Adams and P. Loustaunau. *An Introduction to Gröbner Bases*. American Mathematical Society, 1994.

[2] T. Becker, H. Kredel, and V. Weispfenning. *Gröbner Bases: A Computational Approach to Commutative Algebra*. Springer-Verlag, 1993.

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

[4] B. Buchberger. Ein algorithmisches kriterium für die lösbarkeit eines algebraischen gleichungssystems. *Aequationes mathematicae*, 4(3):374–383, 1970.

[5] B. Buchberger. Gröbner Bases and Systems Theory. *Multidimensional Systems and Signal Processing, Special Issue on "Applications of Groebner Bases in Multidimensional Systems and Signal Processing"*, 12(3/4):223–253, October 2001.

[6] B. Buchberger and F. Winkler. *Gröbner Bases and Applications*, volume 251 of *London Mathematical Society Lecture Notes Series*. Cambridge University Press, 1998.

[7] B. F. Caviness and J.R. Johnson, editors. *Quantifier Elimination and Cylindrical Algebraic Decomposition*. Texts and monographs in symbolic computation. Springer-Verlag, 1998.

[8] D. Cox, J. Little, and D. O'Shea. *Ideals, Varieties, and Algorithms : An Introduction to Computational Algebraic Geometry and Commutative Algebra*. Springer, 7 2005.

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

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

[11] J. C. Faugère. A new efficient algorithm for computing Gröbner basis (f4). *Journal of Pure and Applied Algebra*, 139(1-3):61–88, 1999.

[12] 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.

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

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

[15] G. Hermann. The question of finitely many steps in polynomial ideal theory. *SIGSAM Bulletin*, 32(3):8–30, September 1998.

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

[17] M. Kreuzer and L. Robbiano. *Computational Commutative Algebra 1*. Springer, 2000.

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

[19] 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.

[20] H. M. Möller and B. Buchberger. The construction of multivariate polynomials with preassigned zeros. In *EUROCAM*, pages 24–31, 1982.

[21] F. Mora. *Solving Polynomial Equation Systems II : Macaulay's Paradigm and Gröbner Technology*. Cambridge University Press, 2005.

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

[23] M. Sala, T. Mora, L. Perret, S. Sakata, and C. Traverso, editors. *Gröbner Bases, Coding, and Cryptography*. Springer, 2009.

[24] 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.

[25] D. Wang. *Elimination Methods*. Texts and Monographs in Symbolic Computation. Springer-Verlag, 2001.