Using Resultants for Inductive Gröbner Bases Computation

Hamid Rahkooy, Zafeirakis Zafeirakopoulos
Research Institute for Symbolic Computation (RISC)
Doctoral Program Computational Mathematics (DK)
Johannes Kepler University, Austria
{rahkooy,zafeirakopoulos}@risc.jku.at

1 Outline

In his PhD thesis, B. Buchberger introduced the concept of Gröbner basis and gave an algorithm to compute it [1]. Later on a number of inductive algorithms for computing Gröbner bases appeared, which employ induction on the number of polynomials in the given basis of the ideal. For the slightly different but related problem of ideal membership, G. Hermann [3] proceeds by induction on the number of variables. In this work we are aiming to give an inductive approach to Gröbner bases computation of a radical ideal with induction over the variables. To this end we employ resultants, which is an important tool in elimination theory [2].

Throughout this text we will use the following notation and conventions. $\mathbb{K}$ is an algebraically closed field of characteristic 0. We fix the lexicographic term order $>$ with $x_1 > x_2 > \ldots > x_n$. I is a radical ideal of the polynomial ring $\mathbb{K}[x_1, x_2, \ldots, x_n]$, generated by $F = \{f_1, f_2, \ldots, f_s\}$. By I_i we denote the i-th elimination ideal of I, $I \cap \mathbb{K}[x_{i+1}, \ldots, x_n]$. $Res(F)$ denotes the set of the resultants of pairs of polynomials in F, $\{res_{x_1}(f_i, f_j) | 1 \leq i < j \leq s\}$. *Spol* and *NF* will stand for s-polynomial and normal form.

The main idea is to compute the reduced Gröbner basis in two phases. In the first phase we recursively project the given ideal I into its elimination ideals $I_1, I_2, \ldots, I_k$ until we cannot project anymore. The following proposition gives us a method to do the projection.

Proposition 1. *Assume that* $\forall f \in F, \deg_{x_1}(f) > 0$. *Then* $\sqrt{\langle Res(F) \rangle} = I_1$.

In the second phase we inductively compute the reduced Gröbner basis starting from the last elimination ideal until we reach the reduced Gröbner basis of the given ideal, using the following observation.

Observation 1. *If* G_i *denotes the reduced Gröbner basis of* I_i *for* $1 \leq i \leq n$, *then* $G_i \subseteq G_{i-1}$.

2 Method

1. Project F into the sets $F_1, F_2, \ldots F_k$, where F_i is a generating set of I_i in the following way:
   (a) $T := F, i = 1$
   (b) While $T \nsubseteq \mathbb{K}$ do
      i. $T' := \{f \in T | \deg_{x_i}(f) = 0\}$
      ii. Compute $Res' := Res(T \backslash T')$
      iii. $T := \sqrt{\langle T' \cup Res' \rangle}$
      iv. $F_i := T$, $i = i + 1$
   (c) $k = i - 1$

2. Compute G_k in the following way:
   (a) If F_k contains only univariate polynomials then $G_k = gcd(F_k)$
   (b) Otherwise run Buchberger's algorithm on F_k to obtain G_k
3. Reduce F_{i-1} by G_i in the following way(denoted by $red(F_{i-1}, G_i)$):
   (a) consider $F_{i-1} \subset \mathbb{K}[x_{i+1}, \cdots, x_n][x_i]$.
   (b) take polynomials in F_{i-1}, reduce their coefficients by G_i and replace them in F_{i-1}.
4. Compute G_{i-1} in the following way:
   (a) Compute $\{NF(Spol(f,g)) | f, g \in F_{i-1} \setminus (F_{i-1} \cap \mathbb{K}[x_i, \ldots, x_n])\}$
   (b) Compute $\{NF(Spol(f,g)) | f \in F_{i-1} \setminus (F_{i-1} \cap \mathbb{K}[x_i, \ldots, x_n]), g \in G_i\}$
   (c) Run Buchberger's algorithm on the union of the sets above and autoreduce

Example Let $F = \{x_1^2 + x_2^2 - x_3^2 - 1, x_1 - x_2, -x_2^2 + x_3^2\} \subset \mathbb{K}[x_1, x_2, x_3]$. Then

Down			**Up**	
F	$\{x_1^2 + x_2^2 - x_3^2 - 1, x_1 - x_2, -x_2^2 + x_3^2\}$		G	$\{x_2^2 - 1, x_3^2 - 1, x_1 - x_2\}$
T'	$\{-x_2^2 + x_3^2\}$		Run Step 4 on G_1 and $red(F, G_1)$	
Res'	$Res(\{x_1^2 + x_2^2 - x_3^2 - 1, x_1 - x_2\}) = \{2x_2^2 - x_3^2 - 1\}$		$red(F, G_1)$	$\{x_1^2 - 1, x_1 - 1\}$
F_1	$\{-x_2^2 + x_3^2, 2x_2^2 - x_3^2 - 1\}$		G_1	$\{x_2^2 - 1, x_3^2 - 1\}$
T'	$\{\}$		Run Step 4 on G_2 and $red(F_1, G_2)$	
Res'	$Res(\{-x_2^2 + x_3^2, 2x_2^2 - x_3^2 - 1\}) = \{x_3^4 - 2x_3^2 + 1\}$		$red(F_1, G_2)$	$\{-x_2^2 + 1, 2x_2^2 - 2\}$
F_2	$\{x_3^2 - 1\}$	$\longrightarrow$	G_2	$\{x_3^2 - 1\}$

3 Future Directions

The following are the main open problems that we are concerned with:

- Under what assumptions is $\langle Res(F) \rangle$ a radical ideal? We assume that I is a radical ideal. How can this restriction be lifted?
- In the first phase, could we benefit by employing different ways of resultant computation?
- In the second phase we employ Buchberger's Algorithm. Is there any way, exploiting the already computed G_i to detect G_{i-1} without computing the normal form of S-polynomials?
- What is the complexity of the steps? Is the method efficient in practice?

References

[1] B. Buchberger, Ein Algorithmus zum Auffinden der Basiselemente des Restklassenringes nach einem nulldimensionalen Polynomideal, University of Innsbruck, 1965.

[2] I. M. Gelfand, M. M. Kapranov, A. V. Zelevinsky, Discriminants, Resultants and Multidimensional Determinants, Birkhäuser, 1994.

[3] G. Hermann, Die Frage der endlich vielen Schritte in der Theorie der Polynomideale, *Math. Ann.*, 95:736-788, 1926.