Gröbner Bases and Resultants

Marko Roczen

Abstract

This is an example relating Gröbner bases to resultants, as well as a proof of a classical elimination theorem. Partially, the presentation will be following Sturmfels [S] and Cox, Little, O'Shea [CLO], where the reader may find further material.

This short talk was given in the Summer School on Gröbner Bases, University of Constantza, September 14 - 20, 1999.

0. Introduction

The following remarks are made to give evidence of how resultants can be a useful tool solving polynomial equations in cases where Gröbner bases may fail. We will be solving an exercise from Sturmfels' paper (loc. cit.) using the computer algebra system Singular (see [GPS]) and present resultant techniques to prove Hilbert's Nullstellensatz.

Elimination theory may be considered the origin of algebraic geometry, its history can be traced back to Newton (for very special equations) and to Euler and Bezout (the "elimination theorem" in dimensions 1 and 2). The classical method using resultants has been for a long period the major tool to compute zeroes of a set of polynomials.

The alternative of using Gröbner bases became fashionable since we begun using computers; although the method was known to Gordan by the end of the 19^{th} century, already.

Surprisingly, calculations with Gröbner bases may reach their limitations quite soon. There are theoretical indications that this is not due to the poor quality of our computers, but rather to complexity questions which recently have been studied by M. Giusti and others.

For some remarks on the history and the present of elimination theory, see Eisenbud [E] as well as Sturmfels for an alternative opinion in favour of resultants ("In my opinion the old-fashioned approach is well, alive and surprisingly effective.", cf. [S], p. 27).

1. Failure of computer algebra

k denotes an algebraically closed field. Consider the ring of polynomials $k[X_, \ldots, X_n]$ over k and choose the lexicographic ordering for monomials.

As we have seen already (in the preceding talks, cf. also [R], 5.), for any ideal I and any Gröbner basis G of I with respect to our given ordering, the intersection $I_r := I \cap k[X_{r+1}, \ldots, X_n]$ (the "r-th elimination ideal of I") has $G \cap k[X_{r+1}, \ldots, X_n]$ as Gröbner basis.

Now consider the following polynomials in the indeterminate X (over some field) with coefficients u_i, v_j:

$$f = u_2X^2 + u_1X + u_0$$
$$g = v_2X^2 + v_1X + v_0$$

Suppose $u_2v_2 \neq 0$. As we know from elementary algebra, these polynomials have a common zero in k iff their resultant $r := res(f, g, X)$ vanishes. There should be no need to specify the indeterminate X, but now replace the coefficients with indeterminates, i.e. consider as base ring $A := k(u_0, \ldots, v_2)[X]$. r is an integer polynomial in $u_0, \ldots, v_2$. Thus, if we give the lexicographic ordering of letters to monomials in $k[u_0, \ldots, v_2, X]$, we obtain $r \in J_1$, the first elimination ideal of $I = (f, g)$. The polynomial r gives us the same set of zeroes as J_1, and the computation of a (reduced) Gröbner basis for J easily gives us r as the element not containing any monomial divisible by X.

In Singular, this may be done using the commands

```
ring r=0,(X,u0,u1,u2,v0,v1,v2),lp;
option(redSB);
poly f=u2*X^2+u1*X+u0;
poly g=v2*X^2+v1*X+v0;
ideal i=f,g;
std(i);
```

to obtain a Gröbner basis of the ideal generated by f and g. To get generators of the first elimination ideal, we only have to check which of the elements do not depend on X. This is apparently only the first. Now, to compute the resultant (as it can be obtained from the familiar determinant formula), we use Singular again:

```
resultant(f,g,X);
```

Apparently, this is the same as the first element of the above computed Gröbner basis. There is no problem to do this for polynomials of higher degree, but already, if I took them both of degree 4, my machine was running short of memory. On the other hand, using the `resultant` command, you are done within moments.

Let me mention a nice example which illustrates why it is hopeless to compute Gröbner bases in general (see Cox [C], 5.).

For any graph Γ with N vertices numbered by the integers $\leq N$, the problem of giving a 3-colouring for Γ can be formulated as follows: Let $1, \omega, \omega^2$ be the 3 colours, where ω is a primitive 3-rd unit root. In $\mathbb{C}[X_0, \ldots, X_N]$ we have a system of equations

$$\begin{array}{ll} X_i^3 - 1 = 0 & 0 \leq i \leq N \\ X_i^2 + X_i X_j + X_j^2 = 0 & \text{for edges } (i,j) \text{ of } \Gamma. \end{array}$$

Solutions correspond to the regular 3-colourings of the graph, because the second equation guarantees different colours for any neighbouring vertex of i. From the beginning on we know that there is a finite (possibly empty) set of solutions. But the problem of colouring a graph with 3 colours is known to be NP-complete. Thus, computation of Gröbner bases is at least as difficult as finding the 3-colouring.

Let's continue with an application of resultants in the proof of the elimination theorem.

2. Resultants and Hilbert's Nullstellensatz

We use the notations from 1. The elimination ideal I_1 of I defines a closed subset $V(I_1)$ of k^{n-1} which is referred to as set of partial zeroes of I (with respect to $X_1, \ldots, X_n$). The projection map $\pi_1 : k^n \longrightarrow k^{n-1}$ maps $V(I)$ into $V(I_1)$, but not necessarily onto that set. The question considered here is how to lift a partial zero to an element of $V(I)$.

Extension theorem:

Let $I = (f_1, \ldots, f_s)$ and $f_i = g_i(X_2, \ldots, X_n) X_1^{N_i} + \ldots$ (terms of degree $< N_i$ in X_1, $N_i \geq 0$ and g_i not the zero polynomial. Then for any $(a_2, \ldots, a_n) \in V(I_1)$, there exists $a_1 \in k$ such that $(a_1, \ldots, a_n) \in V(I)$.

Thus, $\pi_1(V(I)) \cup (V(g_1, \ldots, g_s) \cap V(I_1)) = V(I_1)$ (and the "Nullstellensatz" below even shows, that $V(I_1)$ is the Zariski-closure of $\pi_1(V(I))$).

The case $s = 2$ of the above theorem is essentially what we have seen above for the case of two quadratic polynomials in one variable.

Proof of the theorem:
Let $U_2, \ldots U_s$ be new indeterminates. The generalised resultants of $(f_1, \ldots, f_s)$ with respect to X_1 are defined to be the coefficients $r_\alpha(X_2, \ldots, X_n) \in k[X_2, \ldots, X_n]$ in the expression

$$(*) \quad res(f_1, U_2f_2 + \ldots + U_sf_s, X_1) = \sum_{\alpha \in I\!N^n} r_\alpha(X_2, \ldots, X_n)U^\alpha.$$

For a given $c = (c_2, \ldots, c_n) \in V(I_1)$, we have to find $c_1 \in k$ sucht that $c = (c_1, \ldots, c_n) \in V(I)$, provided $c \notin V(g_1, \ldots, g_s)$. Assume $g_1(c) \neq 0$, and (replacing f_2 by some $f_2 + X_1^N f_1$) also $g_2(c) \neq 0$, such that f_2 has the largest degree in X_1 among the $f_2, \ldots, f_s$.
Now the classical resultant of two polynomials is a linear combination of the polynomials where the coefficients are integer polynomials in the coefficients of the original ones,

$$res(f_1, U_2f_2 + \ldots + U_sf_s, X_1) = Af_1 + B(U_2f_2 + \ldots + U_sf_s),$$

and $A, B \in k[U_2, \ldots, U_s, X_1, \ldots, X_n]$. We obtain $A = \sum_{\alpha \in I\!N^n} A_\alpha U^\alpha$ and $B = \sum_{\alpha \in I\!N^n} B_\alpha U^\alpha$, where $A_\alpha, B_\alpha \in k[X_1, \ldots, X_n]$. Substituting into $(*)$ and comparing coefficients with respect to U gives us h_α as a sum of multiples of $f_1, \ldots, f_s$, thus $h_\alpha \in I_1$. $c \in V(I_1)$ implies $h_\alpha(c) = 0$ for all α, thus

$$(**) \quad res(f_1(X_1, c), U_2f_2(X_1, c) + \ldots + U_sf_s(X_1, c), X_1) = h(c, U_2, \ldots, U_s) = 0$$

as a polynomial in U. Therefore, there is a common factor of a positive degree in X_1 for the polynomials $f_1(X_1, c)$ and $U_2f_2(X_1, c) + \ldots + U_sf_s(X_1, c)$; this factor does not depend on U, thus it divides all $f_i(X_1, c)$, giving us a common zero since k is algebraically closed. □

As a corollary, we obtain the following celebrated theorem.

5.5. Nullstellensatz: *Let k be algebraically closed and $I \subseteq k[X_1, \ldots, X_n]$ be an ideal. Then the set $V(I)$ of zeroes of I is empty iff $I = (1)$.*

Proof: Suppose $n > 1$, $I = (f_1, \ldots, f_s)$, $V(I) = \emptyset$ and $I \neq 0, (1)$. Without loss of generality, $f_1 = X_1^N + (terms\ of\ degree\ < N\ in\ X_1)$. Thus by the above Extension theorem, the projection $\pi_1 : k^n \to k^{n-1}$ maps $V(I)$ onto $V(I_1)$, i.e. $V(I_1) = \emptyset$. By induction, we may suppose $I_1 = (1)$, thus $1 \in I_1 \subseteq I$. □

For a detailed account on resultants, cf. [GKZ] and the included references.

References

[BWe] Becker, T., Weispfenning, V., Gröbner Bases, Springer Berlin Heidelberg New York (1995)

[BW] Buchberger, B., Winkler, F. (ed's), Gröbnerbases and Applications, London Mathematical Society Lecture Note Series 251, Cambridge University Press (1998)

[C] Cox, D., Introduction to Gröbner Bases, Proceedings of Symposia in Applied Mathematics, Vol. 53 (1998), 1-24

[CLO] Cox, D., Little, J., O'Shea, D., Ideals, Varieties and Algorithms, Springer Berlin Heidelberg New York (1992)

[E] Eisenbud, D., Commutative Algebra with a View towards Algebraic Geometry, Springer New York (1995)

[GKZ] Gel'fand, I.M., Kapranov, M., Zelevinsky, A., Discriminants, Resultants and Multidimensional Determinants, Birkhäuser (1994)

[GPS] Greuel, G.-M., Pfister, G., Schönemann, H., Singular, a System for Computation in Algebraic Geometry and Singularity Theory, available from http://www.mathematik.uni-kl.de/ftp/pub/Math/Singular

[R] Roczen, First Steps with Gröbner Bases, An. St. Univ. Ovidius Constanta (Seminars), 33-48 (1998)

[S] Sturmfels, B., Introduction to Resultants, Proceedings of Symposia in Applied Mathematics, Vol. 53 (1998), 25-39

[V] Vasconcelos, W. V., Computational methods of commutative algebra and algebraic geometry, with chapters by D. Eisenbud, D. R. Grayson, J. Herzog and M. Stillman, Springer Berlin (1998)