GRÖBNER BASES, A PERSONAL EXPERIENCE AND AN APPLICATION

RAHIM ZAARE-NAHANDI
UNIVERSITY OF TEHRAN

PRESENTED AT THE WORKSHOP ON COMPUTATIONAL COMMUTATIVE ALGEBRA
2-7 JULY 2011, IPM, TEHRAN

1. A personal experience

Throughout more than the first half of the 20th century, while the mission was towards a solid foundation for algebraic geometry, the mentality of the leading experts in the subject was against constructive methods.

We all have heard the story of "elimination of elimination theory". D. Eisenbud [1, p. 306] points out that, A. Weil in his influential book [11, p. 31], says " The device that follows ..., it may be hoped finally eliminates from algebraic geometry the last traces of Elimination Theory...". This statement is actually due to C. Chevalley from his Princeton lectures [11, p. 31, The footnote]. It is therefore not surprising that, in the preface of the fourth edition of his book Algebra, B. L. van der Wearden, influenced by other masters like A. Weil, and C. Chevalley, writes "By omitting some material I have tried to keep the size of the book within reasonable bound. Thus, the chapter "Elimination Theory" has been omitted. The theorem on the existence of resultant system for homogeneous equations, which was formerly proved by means of elimination theory, now appears in Section 121 as a Corollary to Hilbert's Nullstellensatz."

In 1971, on a panel discussion at the 2nd Annual Iranian Mathematics Conference in Tehran, with J. Dieudonne and some prominent mathematical figures, J. McCarty, a computer scientist, was addressing the future mathematics to be affordable by computers. Dieudonne was harshly against the idea. At the time, I was a master student and, influenced by my professors who were mostly educated in France, I had a great admiration for Dieudonne. But clearly, MacCarty was referring to constructive methods in mathematics and the future was in his favor.

As far as I could remember, the first time I attended a talk on Gröbner bases, was in Italy, in 1988-89. I was at University of Bologna for my sabbatical year, working with Paolo Salmon. Together with Paolo, we went to the University of Ferrara for a talk by Teo Mora.

A coupe of days ago, I asked Teo if he remembers the title of his talk. He replied "An introduction to Gröbner bases" or, "Noncommutative Grb̈ner bases".

I am not really sure. What I could remember is that the talk was not so elementary.

At that time, my view towards the so called “Computer Algebra” was naively negative. When my ex supervisor Joel Roberts visited me at University of Bologna (in 1989), I complained of a set back by some strong Italian commutative algebraists in turning to computer algebra. As it was his habit, he did not comment right away. The day after, he offered me a tutorial to start working with the computer algebra system “Macaulay”!

During my sabbatical, I visited University of Genova and participated at some activities on computer algebra and related topics. I was working on a problem which had computational nature. In Genova, I met Aron Simis who showed me how to run CoCoA to compute an elimination ideal. This opened an exciting avenue for me to check some examples which supported my expected results. However, as I will explain at the end, after some years, to handle our problem in the general case, we were urged to compute some Gröbner bases.

When I returned home, I already was a fan of computer algebra. But I could just run CoCoA for some operations and I didn’t even know the definition of Gröbner basis. I remember giving a talk at University of Tabriz in 1989 introducing computer algebra. But when I checked my old notes for the talk, I found out that my definition of Gröbner basis was incorrect. Embarrassingly, it was the definition of a “Primbasis”, a concept I took from Gröbner’s book “Moderne Algebraicshe Geometrie” [2] as I felt if it is Gröbner basis, it should be given in his book!!!

However, I learned the subject and some of its applications when I attended a couple of workshops on this spirit at ICTP, Trieste, where several leading experts lectured (September 92 and May 94). These activities were truly valuable for me.

As far as I remember, J. P. Serre had put the following statement on the top of the introduction for the first edition of his book “Algebre Locale.Multiplicites”: “Parturient montes, nascetur ridiculus mus” (Mountains are in labor only to give birth to a ridiculous mouse, from Horace’s Ars Poetica). He was referring to an enormous amount of work in algebraic geometry to reach to a seemingly small result. This statement disappeared in the later editions [8]! On the contrary, it seems that, the idea of Gröbner bases was simple although clever, but the outcome, could be surprisingly effective and fruitful.

In our country, researchers and students started to work on computational aspects of commutative algebra rather slowly. Maybe, this was due to the fact that our commutative algebraists were mostly influenced by the British school. By 2005, we had quite a few graduate students who worked on the subject either abroad or inside the country. In July 2005, the CIMPA School on Gröbner Bases and Applications was held at the Institute for Advanced Studies in Basic Sciences, Zanjan, Iran. In this school some prominent experts of the subject lectured. Since then the trend has been considerably accelerated. It has been some years that we offer graduate courses on computational commutative algebra at mathematics departments of most of our major universities.

It needs mentioning that, in the last 10 years or so, research work on Combinatorial Commutative Algebra has also started to grow. Nowadays, with a rich tradition in combinatorics, this subject is extremely popular, and we have some strong researchers, mostly young, in this discipline.

For the rest of my time, I try to offer a small contribution on Gröbner bases.

2. An application

Let k be a field, b and q integers. Let

$$R = k[z_i, u_{ij} : 0 \leq i \leq b, 1 \leq j \leq q-1]$$

and

$$B = k[t, u_{ij} : 0 \leq i \leq b, 1 \leq j \leq q-1]$$

be polynomial rings. Consider the homomorphism $\varphi : R \longrightarrow B$, where

$$\varphi(u_{ij}) = u_{ij},$$
$$\varphi(z_0) = u_{01}t + u_{02}t^2 + \cdots + u_{0,q-1}t^{q-1} + t^q,$$
$$\varphi(z_i) = u_{i1}t + u_{i2}t^2 + \cdots + u_{i,q-1}t^{q-1}, \quad 1 \leq i \leq b.$$

The problem is to find generators for $\ker\varphi$.

The above homomorphism was first given by Bernard Morin in 1965 as the canonical form of some differentiable mappings [3]. In 1975, the same equations were obtained by Joel Roberts [4], as the canonical form of a generic projection of a smooth algebraic variety at a "unibranched" generic singularity of multiplicity q. The completion of the local ring at such a singular point is $\hat{R}/\ker\varphi\hat{R}$, useful to study the local properties at this point.

Let $f_i(t) = z_i - \varphi(z_i) \in R[t]$, $i = 0, \cdots, b$. Then $R[t]/(f_0(t))$ is a free R-module of rank q generated by $1, t, \cdots, t^{q-1}$.

Theorem 2.1. *(Salmon & - [7, Theorem 4.11], [13, §2]). With the notation above, let*

$$\psi_i : R[t]/(f_0(t)) \longrightarrow R[t]/(f_0(t))$$

be the multiplication by f_i for $i = 1, \cdots, b$. Then,

(i) The sequence of R-modules

$$(R[t]/(f_0(t)))^b \longrightarrow R[t]/(f_0(t)) \longrightarrow B \longrightarrow 0$$

is a finite presentation of B as an R-module, where the first map is $\psi = (\psi_1, \cdots, \psi_b)$ and the second map is defined by $\overline{\varphi}(gt^\ell) = \varphi(g)t^\ell$.

(ii) If M_i be the matrix of ψ_i with respect to the basis $1, t, \cdots, t^{q-1}$ so that

$$\mathcal{M} = [M_1 M_2 \cdots M_b]$$

is the matrix of ψ, then $\ker\varphi$ is generated by the maximal minors of $\mathcal{M}$.

Remark 2.2. *The case $q = 3$, i.e., the case of triple singularities was settled in 1998 for $b = 2$, and in 1991 for arbitrary b in joint papers with P. Salmon (see* [5] *and* [6]*).*

The main ingredient in the proof of the above theorem is the following.

Under some specialization (putting some u_{ij} equal to 0) and a dehomogenization (putting $z_0 = 1$), the matrix $\mathcal{M}$ becomes

$$\mathcal{M}' = [M_1' M_2' \cdots M_b']$$

where M_i' is a *circulat* matrix with distinct indeterminate entries in the first row, therefore in all rows. More precisely,

$$M_i' = \begin{bmatrix} z_i & u_{i1} & . & . & . & u_{i,q-1} \\ u_{i,q-1} & z_i & . & . & . & u_{i,q-2} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ u_{i1} & u_{i2} & . & . & . & z_i \end{bmatrix}.$$

We need to find a Göbner basis of the ideal of maximal minors of $\mathcal{M}'$ in order to prove that certain indeterminate is not a zero-divisor modulo the ideal of maximal minors. To state a more general result on the ideal of n-minors, we use a convenient notation.

Let $S = k[x_{ij} : 1 \le i \le b, 1 \le j \le q]$ be the polynomial ring in bq indeterminates over k and let $\mathcal{C} = \begin{bmatrix} C_1 & C_2 & \cdots & C_b \end{bmatrix}$ be a *generic pluri-circulant* matrix where

$$C_i = \begin{bmatrix} x_{i1} & x_{i2} & . & . & . & x_{iq} \\ x_{iq} & x_{i1} & . & . & . & x_{i,q-1} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ x_{i2} & x_{i3} & . & . & . & x_{i1} \end{bmatrix}$$

is a *generic circulant* matrix. Let $I_n(\mathcal{C}) \subset S$ be the ideal generated by n-minors of $\mathcal{C}$. Let $\mathcal{C}(n)$ be the matrix of the first n rows of $\mathcal{C}$. Let

$$\mathcal{T}(n) = \begin{bmatrix} T_1 & T_2 & \cdots & T_b \end{bmatrix}$$

be a matrix with n rows, where

$$T_i = \begin{bmatrix} x_{i1} & x_{i2} & \cdots & . & . & \cdots & x_{iq} \\ 0 & x_{i1} & \cdots & . & . & \cdots & x_{i,q-1} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & 0 & x_{i1} & \cdots & x_{i,q-n+1} \end{bmatrix}, \quad i = 1, 2, \cdots, b.$$

Proposition 2.3. [7, Theorem 3.3] *With the notation above, assume that k possesses the qth roots of unity and* $\mathrm{char}(k) \nmid q$*. Let G be the set of maximal minors of $\mathcal{C}(n)$ for which the corresponding maximal minors of $\mathcal{T}(n)$ have nonzero diagonals. Then under a suitable diagonal order, G is a Gröbner basis of $I_n(\mathcal{C})$.*

In fact, since a circulant matrix is diagonalizable over such a field k, there is the following similarity of matirices

$$\mathcal{C} \sim \mathcal{D} = [D_1 D_2 \cdots D_b],$$

where

$$D_i = \begin{bmatrix} y_{i1} & 0 & 0 & \cdots & 0 \\ 0 & y_{i2} & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots\vdots & \\ 0 & 0 & 0 & \cdots & y_{iq} \end{bmatrix},$$

with entries in a polynomial ring $S' = k[y_{ij} : 1 \leq i \leq b, 1 \leq j \leq q]$ where each y_{ij} is a linear combination of $x_{i1}, \cdots, x_{iq}$. Observe that $I_n(\mathcal{D})$ is a square-free monomial ideal, i.e., a Stanley-Reisner ideal. The Hilbert series of $I_n(\mathcal{D})$ can be computed. Comparing with the Hilbert series of the ideal generated by $\{\text{in}g : g \in G\}$, the result follows.

The rest of the proof of the theorem is to recover the results from $I_q(\mathcal{M}')$ to $I_q(\mathcal{M})$, using properties of Gröbner bases under specialization and homogenization.

Let me end my talk with a more recent result on $I_n(\mathcal{D})$ in combinatorial commutative algebra.

Theorem 2.4. [14, Theorem 3.7] *The ideal $I_n(\mathcal{D})$ has a natural cellular resolution.*

References

1. D. Eisenbud, *Commutative Algebra with a View Toward Algebraic Geometry*, Springer-Verlag, 1998.
2. W. Gröbner, Moderne Algebraische Geometrie, Springer-Verlag, Wien and Innsbruck, 1949.
3. B. Morin, *Forme canoniques des singularites d'une application differentiable*, C. R. Acad. Sci. Paris **260** (1965) 5662–5665.
4. J. Roberts, *Singularity subschemes and generic projections*, Trans. Amer Math. Soc. **212** (1975) 229–245.
5. P. Salmon and R. Zaare-Nahandi, *Sui ponti tripli con cono tangente triplo*, Atti Accad. Sci. Ist. Bologna, serie XIV-Tomo VI (1988-89) 93–100.
6. P. Salmon and R. Zaare-Nahandi, *Algebraic structure of some analytically irreducible triple points*, Rendi. Semi. Mat. Uiniv. Politec. Torino **49,1** (1991), ACGA 1990, 41–70.
7. P. Salmon and R. Zaare-Nahandi, *Ideals of minors defining generic singularities and their Gröbner bases*, Commun. Algebra **33 (8)** (2005) 2725–2747.
8. J. P. Serre, *Algebre Locale.Multiplicites*, Lecture Notes in Math. **11**, Springer-Verlag, 1965.
9. B. L. van der Wearden, *Modern Algebra*, Vol. 2, Fred. Ungar Pub. Co, New York, 1953.
10. B. L. van der Wearden, *Algebra*, Vol. 2, Fred. Ungar Pub. Co, New York, 1959.
11. A. Weil, *Foundation of Algebraic Geometry*, Colloquium Publications, Vol. 29, 1946.
12. Rahim Zaare-Nahandi and Rashid Zaare-Nahandi, *The minimal free resolution of a class of square-free monomial ideals*, J. Pure Appl. Algebra **189** (2004) 263-278.
13. R. Zaare-Nahandi, *A depth formula for generic singularities and their weak normality*, Commun. Algebra **35(12)** (2007) 4205-4224.
14. R. Zaare-Nahandi, *Cellular resolution for squarefree Veronese ideals and transversal monomial ideals*, preprint 2011.