COCOA School 2007
Approximate Methods in Commutative Algebra

Lorenzo Robbiano

Università di Genova
Dipartimento di Matematica

Contents

Introduction

1. The algebraic setting
2. From equations to points: the `Lex` method
3. From equations to points: Eigenvalues and Eigenvectors
4. From points to equations: the Buchberger-Möller Algorithm
5. Border Bases

References

Introduction I

- Some techniques borrowed from numerical linear algebra, together with new ideas about stability in the polynomial arena allow a new approach to several real world problems.
- Border bases, approximate Buchberger-Moeller algorithm, and the search for low degree polynomials in the "approximate vanishing ideal" of a finite set of points are among the most relevant objects in this fascinating new game.
- A new important entry: CoCoA 5 (project of J. Abbott and A. Bigatti)
- Recent developments in the collaboration between the CoCoA Team and industry highlight the importance of a new emerging field named Approximate Commutative Algebra (ApCoA).
- But do not forget that the basis of the game is still the **old fashioned** Commutative Algebra

Introduction II

- Approximate Commutative Algebra is the expression chosen by myself to name a conference held in Hagenberg-RISC (Linz, Austria) in 2006 in the frame of the SPECIAL SEMESTER ON GRÖBNER BASES AND RELATED METHODS.
- It is a risky name, and indeed it has already received some criticism (see Stetter [S1]),... but I like it!
- Invitation to contribute to Approximate Commutative Algebra. Submission of articles to be considered for inclusion

  15th September 2007

  http://www.dima.unige.it/~abbott/ApCoA.html

Polynomial systems

- Suppose we are given $f_1, \ldots, f_s$ in the polynomial ring $P = K[x_1, \ldots, x_n]$ over a field K. We want to solve the following system of polynomial equations:

$$\begin{cases} f_1(x_1, \ldots, x_n) & = & 0 \\ & \vdots & \\ f_s(x_1, \ldots, x_n) & = & 0 \end{cases}$$

- If the polynomials $f_1, \ldots, f_s$ have degrees ≤ 1, how to solve it is a well-known result in Linear Algebra. Moreover, the size of the set of solutions does not depend on the field K.
- However, as soon as at least one of the polynomials $f_1, \ldots, f_s$ has degree ≥ 2, it turns to be more appropriate to look for the set of solutions in $\overline{K}^n$, where $\overline{K}$ is the algebraic closure of K.
- A first observation is that solving the above system of equations means to determine the set of zeros of the ideal $I = (f_1, \ldots, f_s)$.

Notation

- In the sequel, let K be a field, let $P = K[x_1, \ldots, x_n]$, let $f_1, \ldots, f_s \in P$, and let $I = (f_1, \ldots, f_s)$. Moreover, let $\overline{K}$ be the algebraic closure of K , and let $\overline{P} = \overline{K}[x_1, \ldots, x_n]$.
- By $\mathcal{S}$ we shall denote the system of polynomial equations

$$\begin{cases} f_1(x_1, \ldots, x_n) = 0 \\ \qquad\vdots \\ f_s(x_1, \ldots, x_n) = 0 \end{cases}$$

- We recall that while $\mathcal{Z}(I)$ denotes the set of all the zeros of I in $\overline{K}^n$, we denote by $\mathcal{Z}_K(I)$ the set of all the zeros of I in K^n .
- Given a system $\mathcal{S}$ as above, there can be finitely or infinitely many solutions in $\overline{K}^n$, i.e. the set $\mathcal{Z}(I)$ may be finite or infinite. Next proposition provides an algorithmic criterion for finiteness.

Finiteness Criterion

Proposition (Finiteness Criterion)

Let σ be a term ordering on $\mathbb{T}^n$. The following conditions are equivalent.

1. *The system of equations $\mathcal{S}$ has only finitely many solutions.*
2. *The ideal $I\overline{P}$ is contained in only finitely maximal ideals of $\overline{P}$.*
3. *For $i = 1, \ldots, n$, we have $I \cap K[x_i] \neq (0)$.*
4. *The K-vector space $K[x_1, \ldots, x_n]/I$ is finite-dimensional.*
5. *The set $\mathbb{T}^n \setminus \mathrm{LT}_\sigma\{I\}$ is finite.*
6. *For every $i \in \{1, \ldots, n\}$, there exists a number $\alpha_i \geq 0$ such that we have $x_i^{\alpha_i} \in \mathrm{LT}_\sigma(I)$.*

Zero-dimensional ideals

Definition

An ideal $I = (f_1, \ldots, f_s)$ in $P = K[x_1, \ldots, x_n]$ is called zero-dimensional if it satisfies the equivalent conditions of the Finiteness Criterion.

Corollary

With the same assumptions and notation as in the Finiteness Criterion, let I and J be ideals in P.

1. *If I is maximal, then I is zero-dimensional.*
2. *If I is zero-dimensional and $I \subseteq J$, then J is zero-dimensional.*
3. *If I is zero-dimensional, then $I\overline{P}$ is also zero-dimensional and*

$$\dim_K(P/I) = \dim_{\overline{K}}(\overline{P}/I\overline{P})$$

We shall assume from now on that there are only finitely many such solutions, i.e. that the ideal $I = (f_1, \ldots, f_s)$ is zero-dimensional.

How many solutions?

The Finiteness Criterion yields an easy bound for the number of solutions of $\mathcal{S}$. For, we use condition (3) and deduce that the number of solutions of $\mathcal{S}$ is at most $\deg(g_1)\cdots\deg(g_n)$.

In fact, a **much sharper bound** is available and to prove it we need a ring-theoretic version of the Chinese Remainder Theorem.

Proposition (Bound for the Number of Solutions)

Let $f_1,\dots,f_s \in P$ *generate a zero-dimensional ideal* $I = (f_1,\dots,f_s)$. *Then the system of equations*

$$f_1(x_1,\dots,x_n) = \cdots = f_s(x_1,\dots,x_n) = 0$$

has at most $\dim_K(P/I)$ *solutions in* $\overline{K}^n$.

How many solutions?

Example

- Let us consider the three polynomials $f_1 = x^2 + y + z - 1$, $f_2 = x + y^2 + z - 1$, and $f_3 = x + y + z^2 - 1$ in $P = \mathbb{Q}[x, y, z]$. They define a system of polynomial equations $f_1 = f_2 = f_3 = 0$ and generate an ideal $I = (f_1, f_2, f_3)$ in P .
- We observe that $\{f_1, f_2, f_3\}$ is a `DegRevLex`-Gröbner Basis of I and deduce that $\mathrm{LT}_{\texttt{DegRevlex}}(I) = (x^2, y^2, z^2)$, so that $\dim_{\mathbb{Q}}(P/I) = 8$. Therefore 8 is an upper bound for the number of solutions. How sharp is this a bound?
- When we compute generators g_i of the elimination ideals $I \cap \mathbb{Q}[x_i]$ for $i = 1, 2, 3$ and factor them, we get

$$\begin{aligned}
g_1 &= x^6 - 4x^4 + 4x^3 - x^2 &&= x^2(x-1)^2(x+1+\sqrt{2})(x+1-\sqrt{2}) \\
g_2 &= y^6 - 4y^4 + 4y^3 - y^2 &&= y^2(y-1)^2(y+1+\sqrt{2})(y+1-\sqrt{2}) \\
g_3 &= z^6 - 4z^4 + 4z^3 - z^2 &&= z^2(z-1)^2(z+1+\sqrt{2})(z+1-\sqrt{2})
\end{aligned}$$

- Each of those polynomials has four different zeros. By substituting them into the original system of equations, we see that of the 64 possible combinations only the five tuples $\{(1,0,0), (0,1,0), (0,0,1), (-1+\sqrt{2}, -1+\sqrt{2}, -1+\sqrt{2}),$ $(-1-\sqrt{2}, -1-\sqrt{2}, -1-\sqrt{2})\}$ are actual solutions.

Radical ideals

- In this example, we see other phenomena emerging. For instance, it is clear that the last step of the procedure applied in this example breaks down if the zeros of the polynomials $g_1, \dots, g_n$ cannot be represented by radicals.

  Another important fact is that, while the bound given by the Proposition is 8, the actual number of solutions is 5.

- If a polynomial f vanishes at the set of solutions of $\mathcal{S}$, then also $\mathrm{sqfree}(f)$ vanishes at that set. Consequently, the system $\mathcal{S}$ has the same set of solutions as the system $\mathcal{S}'$, where $\mathcal{S}'$ is obtained from $\mathcal{S}$ by adding the squarefree parts of some polynomials in $\mathcal{S}$. Looking at the example above, we can now understand why the upper bound given by the Proposition is not sharp.

- We have $\mathcal{Z}(I) = \mathcal{Z}(\sqrt{I})$, and $\dim_K(P/I) \geq \dim_K(P/\sqrt{I})$.

- The radical of I, i.e. $\sqrt{I}$ can be computed if K has charachteristic zero or is a perfect field of characteristic $p > 0$ having effective p^{th} roots.

Exact number of solutions

If the system of polynomial equations $\mathcal{S}$ corresponds to a zero-dimensional radical ideal, and if the base field is perfect, the bound for the number of solutions given in the Proposition is sharp, i.e. we have the following formula for the exact number of solutions.

Theorem (Exact Number of Solutions)

Let I be a zero-dimensional radical ideal in P, let $\overline{K}$ be the algebraic closure of K, and let $\overline{P} = \overline{K}[x_1, \dots, x_n]$. If K is a perfect field, the number of solutions of the system of equations $\mathcal{S}$ is equal to the number of maximal ideals of $\overline{P}$ containing $I\overline{P}$, and this number is precisely $\dim_K(P/I)$.

Normal position

The Lex method is based on the idea of extending the technique of Gaussian elimination.

We want to solve a system $f_1 = \cdots = f_s = 0$ and may assume that $I = (f_1, \ldots, f_s)$ is a zero-dimensional radical ideal in $P = K[x_1, \ldots, x_n]$.

Our next goal is to perform a linear change of coordinates in such a way that the resulting system of equations has the additional property that its solutions in $\overline{K}^n$ have pairwise distinct last coordinates. Let us introduce the following name for this property.

Definition

Suppose that I is a zero-dimensional ideal in the polynomial ring P , and let $i \in \{1, \ldots, n\}$. We say that I is in normal x_i -position if any two zeros $(a_1, \ldots, a_n), (b_1, \ldots, b_n) \in \overline{K}^n$ of I satisfy $a_i \neq b_i$.

If the field K has enough elements (in particular if it is infinite), a linear transformation can be explicitly computed which puts the ideal I in normal x_i -position.

Shape

Theorem (The Shape Lemma)

Let K be a perfect field, let $I \subseteq P$ be a zero-dimensional radical ideal in normal x_n -position, let $g_n \in K[x_n]$ be the monic generator of the elimination ideal $I \cap K[x_n]$, and let $d = \deg(g_n)$.

1. *The reduced Gröbner basis of the ideal I with respect to* `Lex` *is of the form $\{x_1 - g_1, \dots, x_{n-1} - g_{n-1}, g_n\}$, where $g_1, \dots, g_{n-1} \in K[x_n]$.*
2. *The polynomial g_n has d distinct zeros $a_1, \dots, a_d \in \overline{K}$, and the set of zeros of I is*

$$\mathcal{Z}(I) = \{(g_1(a_i), \dots, g_{n-1}(a_i), a_i) \mid i = 1, \dots, d\}$$

Solving

Corollary (Solving Systems Effectively)

Let K be a field of characteristic zero or a perfect field of characteristic $p > 0$ having effective p^{th} roots. Furthermore, let $f_1, \dots, f_s \in P = K[x_1, \dots, x_n]$, and let $I = (f_1, \dots, f_s)$. Consider the following sequence of instructions.

1. *For $i = 1, \dots, n$, compute a generator g_i of the elimination ideal $I \cap K[x_i]$. If $g_i = 0$ for some $i \in \{1, \dots, n\}$, then return* `Infinite Solution Set` *and stop.*
2. *Compute $h_i = \mathrm{sqfree}(g_i)$ for $i = 1, \dots, n$, then replace I by $I + (h_1, \dots, h_n)$.*
3. *Compute $d = \#(\mathbb{T}^n \setminus \mathrm{LT}_\sigma\{I\})$.*
4. *Check if $\deg(h_n) = d$. In this case, let $(c_1, \dots, c_{n-1}) = (0, \dots, 0)$ and continue with step 8).*
5. *If K is finite, enlarge it so that it has more than $\binom{d}{2}$ elements.*
6. *Choose a tuple $(c_1, \dots, c_{n-1}) \in K^{n-1}$. Apply the coordinate transformation $x_1 \mapsto x_1, \dots, x_{n-1} \mapsto x_{n-1}$, $x_n \mapsto x_n - c_1 x_1 - \cdots - c_{n-1} x_{n-1}$ to I and get an ideal J.*
7. *Compute a generator of $J \cap K[x_n]$ and check if it has degree d. If not, repeat steps 6) and 7) until this is the case. Then rename J and call it I.*
8. *Compute the reduced Gröbner basis of I with respect to* `Lex`*. It has the shape $\{x_1 - g_1, \dots, x_{n-1} - g_{n-1}, g_n\}$ with polynomials $g_1, \dots, g_n \in K[x_n]$ and with $\deg(g_n) = d$. Return the tuples $(c_1, \dots, c_{n-1})$ and $(g_1, \dots, g_n)$ and stop.*

*This is an algorithm which decides whether the system of polynomial equations $\mathcal{S}$ given by $f_1 = \cdots = f_s = 0$ has finitely many solutions. In that case, it returns tuples $(c_1, \dots, c_{n-1}) \in K^{n-1}$ and $(g_1, \dots, g_n) \in K[x_n]^n$ such that, after we perform the linear change of coordinates $x_1 \mapsto x_1, \dots, x_{n-1} \mapsto x_{n-1}$, $x_n \mapsto x_n - c_1 x_1 - \cdots - c_{n-1} x_{n-1}$, the transformed system of equations has the set of solutions $\{(g_1(a_i), \dots, g_{n-1}(a_i), a_i) \mid i = 1, \dots, d\}$, where $a_1, \dots, a_d \in \overline{K}$ are the zeros of g_n.
In other words, the original system of equations has the set of solutions*

$$\{(g_1(a_i), \dots, g_{n-1}(a_i), a_i - c_1 g_1(a_i) - \cdots - c_{n-1} g_{n-1}(a_i)) \mid i = 1, \dots, d\}$$