MIT 6.972 Algebraic techniques and semidefinite optimization April 4, 2006

Lecture 14

Lecturer: Pablo A. Parrilo *Scribe: ???*

After a brief review of monomial orderings, we develop the basic ideas of Groebner bases, followed by examples and applications. For background and much more additional material, we recommend the textbook of Cox, Little, and O'Shea [CLO97]. Other good, more specialized references are [AL94, BW93, KR00].

1 Monomial orderings

Recall from last lecture the notion of a monomial ordering:

Definition 1. *A* monomial ordering *on* $\mathbb{C}[\mathbf{x}]$ *is a relation* $\succ$ *on* $\mathbb{Z}_+^n$ *(i.e., the monomial exponents), such that:*

1. *The relation* $\succ$ *is a total ordering.*
2. *If* $\alpha \succ \beta$*, and* $\gamma \in \mathbb{Z}_+^n$*, then* $\alpha + \gamma \succ \beta + \gamma$*.*
3. *The relation* $\succ$ *is a well-ordering (every nonempty subset has a smallest element).*

There are several term orderings of interest in computational algebra. Among them, we mention:

- Lexicographic ("dictionary"). Here $\alpha \succ_{\text{lex}} \beta$ if the left-most nonzero entry of $\alpha - \beta$ is positive. Notice that a particular order of the variables is assumed, and by changing this, we obtain $n!$ nonequivalent lexicographic orderings.
- Graded lexicographic. Sort first by total degree, then lexicographic, i.e., $\alpha \succ_{\text{grlex}} \beta$ if $|\alpha| > |\beta|$, or if $|\alpha| = |\beta|$ and $\alpha \succ_{\text{lex}} \beta$.
- Graded reverse lexicographic. Here $\alpha \succ_{\text{grevlex}} \beta$ if $|\alpha| > |\beta|$, or if $|\alpha| = |\beta|$ and the right-most nonzero entry of $\alpha - \beta$ is negative. This ordering, although somewhat nonintuitive, has some desirable computational properties.
- General matrix orderings. Described by a weight matrix $W \in \mathbb{R}^{k \times n} (k \leq n)$, where $\alpha \succ_W \beta$ if $(W\alpha) \succ_{\text{lex}} (W\beta)$. For W to correspond to a monomial ordering as defined, the first nonzero entry on each column must be positive.

It turns out that every monomial ordering can be described by an associated matrix W, i.e., every monomial ordering is a matrix ordering. What are the matrices corresponding to the first three orderings described?

Example 2. *Consider the polynomial ring* $\mathbb{C}[x, y]$*. In the lexicographic ordering (*$\prec_{\textbf{\textit{lex}}}$*) discussed, we have:*

$$1 \prec y \prec y^2 \prec \cdots \prec x \prec xy \prec xy^2 \prec \cdots \prec x^2 \prec x^2 y \prec x^2 y^2 \prec \cdots,$$

while for the other two orderings ($\prec_{\textbf{\textit{grlex}}}$ *and* $\prec_{\textbf{\textit{grevlex}}}$*), which in the special case of two variables coincide, we have:*

$$1 \prec y \prec x \prec y^2 \prec xy \prec x^2 \prec y^3 \prec xy^2 \prec x^2 y \prec x^3 \prec \cdots.$$

`Picture comparing different orderings` ToDo

Example 3. *Consider the monomials* $\alpha = x^3 y^2 z^8$ *and* $\beta = x^2 y^9 z^2$*. If the variables are ordered as* (x, y, z)*, we have*

$$\alpha \succ_{lex} \beta, \qquad \alpha \succ_{grlex} \beta, \qquad \alpha \prec_{grevlex} \beta.$$

Notice that $x \succ y \succ z$ *for all three orderings.*

2 Groebner bases

2.1 Monomial ideals

Before studying general ideals, it is convenient to introduce first a special class, known as *monomial ideals*.

Definition 4. *A* monomial ideal *is a polynomial ideal that can be generated by monomials.*

What are the possible monomials that belong to a given monomial ideal? Since $x^\alpha \in I \Rightarrow x^{\alpha+\beta} \in I$ for $\beta \geq 0$, we have that these sets are "closed upwards."

`Picture of monomial ideals` ToDo

Furthermore, a polynomial belongs to a monomial ideal I if and only if it all its terms are in I.

Theorem 5 (Dickson's lemma)**.** *Every monomial ideal is finitely generated.*

We consider next a special monomial ideal, associated to every polynomial ideal I. From now on, we assume a fixed monomial ordering (e.g., graded reverse lexicographic), and denote by $in(f)$ the "largest" monomial appearing in the polynomial $f \neq 0$.

Definition 6. *Consider an ideal $I \subset \mathbb{C}[x]$, and a fixed monomial ordering. The* initial ideal *of I, denoted $in(I)$, is the monomial ideal generated by the leading terms of all the elements in I, i.e.,*

$$in(I) := \langle in(f) : f \in I \setminus \{0\} \rangle.$$

A monomial x^α is called standard*, if it does not belong to the initial ideal $in(I)$.*

2.2 Groebner bases

Given an ideal $I = \langle f_1, \ldots, f_s \rangle$, we can construct two monomial ideals associated with it. On the one hand, we have the initial ideal $in(I)$, previously defined. However, we can also consider the monomial ideal generated by the initial monomials of the generators, i.e., $\langle in(f_1), \ldots, in(f_s) \rangle$. Although we always have $\langle in(f_1), \ldots, in(f_s) \rangle \subset in(I)$, in general these two monomial ideals are distinct.

Example 7. *Consider the ideal $I = \langle x^3 - 1, x^2 + 1 \rangle$. Since $1 = \frac{1}{2}(x-1)(x^3-1) - \frac{1}{2}(x^2 - x - 1)(x^2+1)$, we have $1 \in I$, and thus $in(I) = I = \mathbb{C}[x]$. On the other hand, $1 \notin \langle x^3, x^2 \rangle$.*

However, it may be possible to produce a set of generators for which these two ideals are the same. This is exactly the notion of a *Groebner basis*.

Definition 8. *Consider the polynomial ring $\mathbb{C}[x]$, with a fixed monomial ordering, and an ideal I. A finite set of polynomials $\{g_1, \ldots, g_s\} \subset I$ is a* Groebner basis *of I if the initial ideal of I is generated by the leading terms of the g_i, i.e.,*

$$in(I) = \langle in(g_1), \ldots, in(g_s) \rangle. \tag{1}$$

Theorem 9. *Every ideal I has a Groebner basis G. Furthermore, $I = \langle g_1, \ldots, g_s \rangle$.*

The previous theorem essentially establishes Hilbert's finiteness result, and gives an explicit characterization of a finite generating set for the ideal I. Furthermore, since there are explicit algorithms to compute Groebner bases, this is a constructive version of this theorem.

Even though the monomial ordering is fixed, Groebner bases as defined are not unique (why?). This can be easily fixed, by refining the concept to the so-called *reduced* Groebner bases, which are uniquely defined.

There are several possible algorithms to effectively compute Groebner bases. The traditional one is *Buchberger's algorithm*, developed by Bruno Buchberger around 1965, and many variants have been proposed since. There are also several newer methods, based on sparse linear algebra, that in some instances can significantly outperform the Buchberger approach. Good specialized programs for Groebner bases calculations (and much more) are CoCoA[CoC], Macaulay2 [GS] and Singular [GPS05].

2.3 Quotients and normal forms

Recall that if we have an ideal $I \subset \mathbb{C}[x]$, we defined the quotient ring $\mathbb{C}[x]/I$ as the set of equivalence classes modulo the ideal. For computational purposes, we want a "good" representation of these classes, and in particular, a way to provide a "unique representative" to every polynomial. This can in fact be easily done once we have computed a Groebner basis. To each polynomial $p \in \mathbb{C}[x]$, we can associate a unique "normal form", defined below.

Lemma 10. *Let G be a Groebner basis of the ideal $I \subset \mathbb{C}[x]$. Given any $p \in \mathbb{C}[x]$, there exists a unique polynomial $\bar{p}$, called the* normal form *of p, such that*

1. *The polynomials p and $\bar{p}$ are congruent mod I, i.e., $p - \bar{p} \in I$.*
2. *Only standard monomials appear in $\bar{p}$.*

Notice that we have $p = q_1 g_1 + \cdots + q_s g_s + \bar{p}$. Thus, the normal form can be interpreted as the "remainder" after a division-like process by the generators g_i. The key property (1) guarantees that this remainder is uniquely defined.

As a consequence of this, we can solve the ideal membership problem: to check if a polynomial $p(x)$ is in a given ideal I, compute a Groebner basis G of I, and check if the normal form of $p(x)$ is the zero polynomial, i.e., $p \in I \Leftrightarrow \bar{p} = 0$.

3 Applications and examples

Groebner bases enable the algorithmic solution of many problems in computational algebraic geometry. We discuss some these below.

- Ideal membership. As we have seen, given an ideal I and a polynomial p, we can check if $p \in I$ by computing the normal form of p.
- Radical membership. Consider an ideal $I = \langle f_1, \ldots, f_s \rangle \subset \mathbb{C}[x]$, and a polynomial p, for which we want to check whether $p \in \sqrt{I}$. Since $\sqrt{I}$ is also an ideal, we could compute a Groebner basis for it, and then reduce the problem to the previous one. However, it is often more efficient to instead use the following result ("Rabinowitch's trick"):

  $$p \in \sqrt{I} \qquad \Leftrightarrow \qquad 1 \in \langle f_1, \ldots, f_s, 1 - yp \rangle,$$

  where y is a (new) additional variable.
- Consistency of polynomial equations. Consider a finite set of polynomial equations $\{f_i = 0\}$, and let $I = \langle f_i \rangle$ be the corresponding ideal. By the Nullstellensatz, the given equations are infeasible if and only if $\{1\}$ is the reduced Groebner basis of I.
- Elimination. For notational simplicity, consider an ideal $I \subset \mathbb{C}[x, y, z]$. Suppose that we want to compute all the polynomials in I, that *do not* depend on the variable z, i.e., $I \cap \mathbb{C}[x, y]$. Geometrically, this elimination of variables corresponds to (the Zariski closure of) the projection of the corresponding variety into (x, y). This intersection (or projection) can be easily obtained, by computing a Groebner basis G of I with respect to a lexicographic (or elimination) ordering. The corresponding ideal is then generated by $G \cap \mathbb{C}[x, y]$.

4 Zero-dimensional ideals

In practice, we are often interested in polynomial systems that have only a finite number of solutions (the "zero-dimensional" case), and many interesting things happen in this case. Among other properties, the quotient ring $\mathbb{C}[x]/I$ is now a finite dimensional vector space, with its dimension being equal to the number of standard monomials. Furthermore, Groebner bases can be used to fully reduce their solution to a classical eigenvalue problem, generalizing the "companion matrix" notion from the univariate case. All this, and much more, next time...

References

[AL94] W.W. Adams and P. Loustaunau. *An introduction to Gröbner bases*, volume 3 of *Graduate Studies in Mathematics*. American Mathematical Society, Providence, RI, 1994.

[BW93] T. Becker and V. Weispfenning. *Gröbner bases*, volume 141 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1993.

[CLO97] D. A. Cox, J. B. Little, and D. O'Shea. *Ideals, varieties, and algorithms: an introduction to computational algebraic geometry and commutative algebra*. Springer, 1997.

[CoC] CoCoATeam. CoCoA: a system for doing Computations in Commutative Algebra. Available at `http://cocoa.dima.unige.it`.

[GPS05] G.-M. Greuel, G. Pfister, and H. Schönemann. SINGULAR 3.0. A Computer Algebra System for Polynomial Computations, Centre for Computer Algebra, University of Kaiserslautern, 2005. `http://www.singular.uni-kl.de`.

[GS] D.R. Grayson and M. E. Stillman. Macaulay 2, a software system for research in algebraic geometry. Available at `http://www.math.uiuc.edu/Macaulay2/`.

[KR00] M. Kreuzer and L. Robbiano. *Computational commutative algebra. 1*. Springer-Verlag, Berlin, 2000.