Operations Research Seminar: Gröbner Bases and Integer Programming
Speaker: Adam Van Tuyl

Introduction

In this talk I will discuss how to use some of the tools of commutative algebra and algebraic geometry to solve some integer programs. The key piece of machinery that we will need is a *Gröbner Basis.* Gröbner bases were developed by Buchberger in the 1960's (although there are some examples of their use before that time). The advent of powerful computing has enabled us to implement Buchberger's algorithms to construct Gröbner bases.

There are a number of excellent textbooks that introduce Gröbner Bases. The one which I am must familiar with is Cox, Little, and O'Shea's textbook *Ideals, Varieties, and Algorithms* [3]. The material of this talk is based upon a sequel of this book, entitled *Using Algebraic Geometry* [4]. This talk is also heavily indebted to David Cox's tutorial on Gröbner Bases given at ISAAC 2007 in Waterloo. You can download copies of this tutorial from David Cox's website [2].

Basic Terminology

Let k denote a field, usually $\mathbb{R}$ or $\mathbb{C}$. We then let $R = k[x_1, \ldots, x_n]$ denote the *polynomial ring* in the indeterminates $x_1, \ldots, x_n$ over the field k. A *monomial* is a product of the variables, i.e.,

$$x^\alpha := x_1^{a_1} x_2^{a_2} \cdots x_n^{a_n}$$

where $\alpha := (a_1, \ldots, a_n) \in \mathbb{N}^n$. The *degree* of a monomial x^α is $a_1 + \cdots + a_n$. A polynomial of R, i.e., an element of R, is then a linear combination of monomials, i.e.,

$$f = c_1 x^{\alpha_1} + c_2 x^{\alpha_2} + \cdots + c_s x^{\alpha_s}.$$

In the special case that $R = k[x]$, then all the polynomials of R have the form

$$f = c_d x^d + c_{d-1} x^{d-1} + \cdots + c_1 x + c_0.$$

We let $d = \deg f$ be the degree of f. So, in $R = k[x]$, each polynomial will have a largest monomial of degree d. We call cx^d the leading term of f, and x^d the leading monomial.

We quickly run into difficulty when we try to extend these two terms to a polynomial ring in many variables. For example, in $R = k[x_1, x_2]$, consider

$$f = 4x_1^2 x_2 + 2x_1 x_2^2 + 3x_2^2.$$

The degrees of the monomials that appear are $3, 3$, and 2, respectively. Your intuition probably tells you that $3x_2^2$ should be the smallest term. But what term should be the largest? To decide this, we need to introduce monomial orders.

Definition 1. A *monomial order* is a total order (i.e., there are no incomparable elements) $>$ on the set of monomials of $R = k[x_1, \ldots, x_n]$ such that

1. $x^\alpha > x^\beta$ implies $x^\alpha x^\gamma > x^\beta x^\gamma$ for all x^γ, and
2. $x^\alpha > 1$ for all $x^\alpha \neq 1$.

One can then prove that a monomial ordering is a well-ordering (i.e., every set has a minimal element) on the set of monomials.

Definition 2. The *lexicographical order* is the classical example of a monomial ordering. In $R = k[x_1, \dots, x_n]$ we set $x_1 > x_2 > \cdots > x_n$. Then $x^\alpha >_{\text{lex}} x^\beta$ if and only if

$$a_1 > b_1, \text{ or } a_1 = b_1 \text{ and } a_2 > b_2, \text{ or} \dots$$

or equivalently, the first nonzero entry of $\alpha - \beta \in \mathbb{N}^n$ is positive.

We can now generalize the notions of leading term and leading monomial.

Definition 3. Fix a monomial ordering $>$ and let f be a polynomial of $k[x_1, \dots, x_n]$. Suppose that

$$f = cx^\alpha + \text{monomial terms of the form } x^\beta \text{ with } \beta \neq \alpha$$

where $c \neq 0$ and for every term of the form x^β, $x^\alpha > x^\beta$ with respect to the order $>$. Then

1. $\mathrm{LT}(f) = cx^\alpha$ is the *leading term.*
2. $\mathrm{LM}(f) = x^\alpha$ is the *leading monomial.*

In our example,

$$f = 4x_1^2x_2 + 2x_1x_2^2 + 3x_2^2$$

if we use the lexicographical ordering, $4x_1^2x_2$ is the leading term, and $x_1^2x_2$ is the leading monomial.

The Division Algorithm

A monomial ordering is needed to generalize the division algorithm of $R = k[x]$ to a polynomial ring of many variables. Precisely,

Theorem 4 (Division Algorithm)**.** *Fix a monomial ordering $>$ in $R = k[x_1, \dots, x_n]$ and fix $f_1, \dots, f_s \in R$. Then, for every $f \in R$, there exists $q_1, \dots, q_s$ and r in R such that*

$$f = f_1q_1 + \cdots + f_sq_s + r$$

where no term of r is divisible by $LT(f_1), \dots, LT(f_s)$. The polynomial r is called the remainder *of f on division by $f_1, \dots, f_s$. The remainder is sometimes written as f^F where $F = \{f_1, \dots, f_s\}$.*

Recall that a subset $\emptyset \neq I \subseteq R$ is called an *ideal* if

- for every $x, y \in I$, then $x - y \in I$, and
- for every $x \in I$ and every $y \in R$, then $xy \in I$.

We write $(f_1, \dots, f_s)$ for the ideal generated by a subset $F = \{f_1, \dots, f_s\} \subseteq R$. In particular

$$(f_1, \dots, f_s) = \{a_1f_1 + \cdots + a_sf_s \mid a_i \in R\}.$$

We can think of $(f_1, \dots, f_s)$ as the smallest ideal that contains F. A very important theorem in commutative algebra (the Hilbert Basis Theorem) states that every ideal of R is *finitely generated*, that is, given any ideal $I \subseteq R$, there exists a finite set $\{f_1, \dots, f_s\} \subseteq I$ such that $(f_1, \dots, f_s) = I$.

We are then led to the problem:

Question 5 (The Ideal Membership Problem)**.** *Let I be an ideal of R, and suppose that $g \in R$. Is $g \in I$?*

One way to answer this question is to use the Division Algorithm. In particular, suppose that $F = \{f_1, \dots, f_s\}$ are generators for I. If $g^F = 0$, that is, if

$$g = f_1 q_1 + \cdots + f_s q_s \text{ for some } q_i \in R$$

then it is clear that $g \in (f_1, \dots, f_s) = I$. However, there is a problem. Examples can constructed where $F = \{f_1, \dots, f_s\}$ generate the ideal I, we know that $g \in I$, but the division algorithm applied to F and g gives $g^F \neq 0$.

This is where Gröbner bases come to our rescue. A Gröbner basis is a "good" set of generators $G = \{g_1, \dots, g_s\}$ of the ideal I. In particular, we get that $g \in I$ if and only if $g^G = 0$. We expand upon this idea in the next section.

Gröbner Bases

We begin by defining the ideal of leading terms.

Definition 6. Fix a monomial order $>$ on $R = k[x_1, \dots, x_n]$, and let I be an ideal. Then the *ideal of leading terms* is the monomial ideal (i.e., generated by monomials)

$$\mathrm{LT}(I) := (\mathrm{LT}(f) \mid f \in I).$$

If $\{f_1, \dots, f_s\}$ is a set of generators of I, then

$$(\mathrm{LT}(f_1), \dots, \mathrm{LT}(f_s)) \subseteq \mathrm{LT}(I).$$

Of course, we may not have an equality. A Gröbner basis is a set of generators that give us equality:

Definition 7. Fix a monomial ideal $>$. Given an ideal I of $R = k[x_1, \dots, x_n]$, a finite set $G = \{g_1, \dots, g_s\}$ (where $g_i \neq 0$) is a *Gröbner basis* if

$$(\mathrm{LT}(g_1), \dots, \mathrm{LT}(g_s)) = \mathrm{LT}(I).$$

We then have the following important results about Gröbner bases:

Theorem 8. *Fix a monomial ideal $>$. Let I be an ideal of $R = k[x_1, \dots, x_n]$.*

1. *There exists a Gröbner basis of I.*
2. *If $G = \{g_1, \dots, g_s\}$ is a Gröbner basis of I, then $I = (g_1, \dots, g_s)$.*
3. *If $G = \{g_1, \dots, g_s\}$ is Gröbner basis of I, then $g \in I$ if and only if $g^G = 0$.*

Gröbner bases and integer programming problems

Let us consider the integer program:

$$\begin{array}{rrcl} \text{Maximize:} & 11x_1 + 15x_2 & & \\ \text{Subject to:} & 4x_1 + 5x_2 & \leq & 37 \\ & 2x_1 + 3x_2 & \leq & 20 \\ & x_1, x_2 & \geq & 0. \end{array}$$

Just as we did in the linear programming situation, we introduce slack variables (in this case, x_3 and x_4). We then get the equations:

$$\begin{array}{rrcl} \text{Maximize:} & 11x_1 + 15x_2 + 0x_3 + 0x_4 & & \\ \text{Subject to:} & 4x_1 + 5x_2 + x_3 & = & 37 \\ & 2x_1 + 3x_2 + x_4 & = & 20 \\ & x_1, x_2, x_3, x_4 & \geq & 0. \end{array}$$

We define a map $\varphi : k[w_1, w_2, w_3, w_4] \to k[z_1, z_2]$ by sending

$$\begin{array}{rcl} w_1 & \mapsto & z_1^4 z_2^2 \\ w_2 & \mapsto & z_1^5 z_2^3 \\ w_3 & \mapsto & z_1 \\ w_4 & \mapsto & z_2. \end{array}$$

We can extend this to a ring homomorphism, i.e., the map φ has the properties $\varphi(a+b) = \varphi(a)+\varphi(b)$ and $\varphi(ab) = \varphi(a)\varphi(b)$ for all $a, b \in k[w_1, w_2, w_3, w_4]$.

The map φ is onto; indeed, consider any polynomial $f(z_1, z_2) \in k[z_1, z_2]$. Note that $f(w_3, w_4)$ will map to the polynomial. For example, consider $f(z_1, z_2) = 3z_1^3 + 4z_1 z_2^4$. Then $f(w_3, w_4) = 3w_3^3 + 4w_3 w_4^4 \in k[w_1, w_2, w_3, w_4]$, and

$$\varphi(f(w_3, w_4)) = \varphi(3w_3^3) + \varphi(4w_3 w_4^4) = 3\varphi(w_3)^3 + 4\varphi(w_3)\varphi(w_4)^4 = 3z_1^3 + 4z_1 z_2^4.$$

The feasible region of our integer program can then be described in terms of the map φ. In particular, (A, B, C, D) is in the feasible region if and only if $\varphi(w_1^A w_2^B w_3^C w_4^D) = z_1^{37} z_2^{20}$. To see why this is true, note that

$$\begin{array}{rcl} \varphi(w_1^A w_2^B w_3^C w_4^D) & = & \varphi(w_1)^A \varphi(w_2)^B \varphi(w_3)^C \varphi(w_4)^D \\ & = & (z_1^{4A} z_2^{2A})(z_1^{5B} z_2^{3B})(z_1^C)(z_2^D) \\ & = & z_1^{4A+5B+C} z_2^{2A+3B+D}. \end{array}$$

So $\varphi(w_1^A w_2^B w_3^C w_4^D) = z_1^{37} z_2^{20}$ if and only if $4A + 5B + C = 37$ and $2A + 3B + D = 20$. So, what we want to do is describe all monomials $w_1^A w_2^B w_3^C w_4^D$ that map to $z_1^{37} z_2^{20}$, and in particular, we want to identify the monomial that also maximizes our objective function $11x_1 + 15x_2$.

We will now describe an elegant solution to this problem based upon the ideas of Conti and Traverso [1] who originally devised this method. Consider the larger polynomial ring $k[z_1, z_2, w_1, w_2, w_3, w_4]$, and put an monomial ordering on this ring such that any monomial containing any of the z_i's is greater than any containing the of the w_js (the lex ordering with $z_i > w_j$ for all i and j is such an order). Let G be a Gröbner basis for the ideal

$$(z_1^4 z_2 - w_1, z_1^5 z_2^3 - w_2, z_1 - w_3, z_2 - w_4) \subseteq k[z_1, z_2, w_1, w_2, w_3, w_4].$$

Claim. Consider $f = z_1^{37} z_2^{20}$ and let $g = f^G$. Then g is a monomial of $k[w_1, w_2, w_3, w_4]$, i.e., $g = w_1^A w_2^B w_3^C w_4^D$, and furthermore, (A, B, C, D) is a feasible solution.

Proof. The fact that g is a monomial belonging to $k[w_1, w_2, w_3, w_4]$ is a consequence of the more general theory of Gröbner bases. See, in particular, Theorem 1.11 of Chapter 8 in [4]. We will show that the second part of the claim. Let $G = \{g_1, \ldots, g_s\}$ be the Gröbner basis. Then we are given that

$$z_1^{37} z_2^{20} = g_1 f_1 + \cdots + g_s f_s + g$$

where $f_i \in k[z_1, z_2, w_1, w_2, w_3, w_4]$. Note that $g = g(w_1, w_2, w_3, w_4)$ and for each i,

$$g_i f_i = g_i(z_1, z_2, w_1, w_2, w_3, w_4) f_i(z_1, z_2, w_1, w_2, w_3, w_4).$$

Now substitute w_i with $\varphi(w_i)$. That is, we have

$$\begin{aligned} z_1^{37}z_2^{20} &= g_1(z_1,z_2,z_1^4z_2,z_1^5z_2^3,z_1,z_2)f_1(z_1,z_2,z_1^4z_2,z_1^5z_2^3,z_1,z_2)+\cdots+ \\ &\quad g_s(z_1,z_2,z_1^4z_2,z_1^5z_2^3,z_1,z_2)f_s(z_1,z_2,z_1^4z_2,z_1^5z_2^3,z_1,z_2)+g(z_1^4z_2,z_1^5z_2^3,z_1,z_2). \end{aligned}$$

But each g_i is in $(z_1^4z_2-w_1, z_1^5z_2^3-w_2, z_1-w_3, z_2-w_4)$, that is,

$$g_i = a_1(z_1^4z_2-w_1)+a_2(z_1^5z_2^3-w_2)+a_3(z_1-w_2)+a_4(z_2{-}_4),$$

for some polynomials a_i. Thus, for each i, $g_i(z_1,z_2,z_1^4z_2,z_1^5z_2^3,z_1,z_2)=0$, and so

$$z_1^{37}z_2^{20}=g(z_1^4z_2,z_1^5z_2^3,z_1,z_2)=\varphi(g)=\varphi(w_1^Aw_2^Bw_3^Cw_4^D).$$

□

Gröbner bases therefore allow us to get our hands on one feasible solution. To get the optimal solution, the key idea is to use the objective function in constructing the monomial ordering. Before doing this, we are going to change our objective function slightly. Notice that to maximize $\ell(x_1,x_2)=11x_1+15x_2$, it is enough to minimize the function $\ell'(x_1,x_2)=-11x_1-15x_2$. So, we can turn our maximizing problem into a minimizing problem.

Definition 9. Let $\ell(z_1,\ldots,z_n)$ denote the objective function of the integer program. A monomial ordering $>$ of $k[z_1,\ldots,z_m,w_1,\ldots,w_n]$ is an *adapted* monomial order if

1. Any monomial containing one of the z_i is greater than any monomial in the w_j's alone.
2. Suppose that $(A_1,\ldots,A_n)$ and $(A_1',\ldots,A_n')$ are two tuples such that $\varphi(w_1^{A_1}\cdots w_n^{A_n}) = \varphi(w_1^{A_1'}\cdots w_n^{A_n'})$ and $\ell(A_1,\ldots,A_n)>\ell(A_1',\ldots,A_n')$. Then $w_1^{A_1}\cdots w_n^{A_n} > w_1^{A_1'}\cdots w_n^{A_n'}$.

We now have all the pieces we need to get a minimal solution as summarized in the following theorem.

Theorem 10. *Consider an integer program of the form*

$$\begin{array}{rrcl} \textit{Minimize:} & c_1x_1+\cdots+c_nx_n & & \\ \textit{Subject to:} & a_{11}x_1+\cdots+a_{1n}x_n & = & b_1 \\ & a_{21}x_1+\cdots+a_{2n}x_n & = & b_2 \\ & & \vdots & \\ & a_{m1}x_1+\cdots+a_{mn}x_n & = & b_m \\ & x_1,\ldots,x_n & \geq & 0. \end{array}$$

and assume all $a_{ij}, b_i \geq 0$. *Let* $f_j=\prod_{i=1}^m z_i^{a_{ij}}$. *Let* G *be a Gröbner Basis of the ideal*

$$(f_1-w_1,\ldots,f_n-w_n)\subseteq k[z_1,\ldots,z_m,w_1,\ldots,w_n]$$

with respect to an adopted monomial ordering. If $f=w_1^{b_1}\cdots w_m^{b_m}$, *then the exponents of* f^G *give a solution to* $\ell(x_1,\ldots,x_n)=c_1x_1+\cdots+c_nx_n$ *that minimizes* ℓ.

To finish our example, a suitable adapted monomial order on $k[z_1,z_2,w_1,w_2,w_3,w_4]$ is the lex ordering with the variables ordered by

$$z_1>z_2>w_4>w_3>w_2>w_1.$$

We then use our favorite computer algebra system that can compute Gröbner bases to compute the the basis of the ideal

$$(z_1^4z_2-w_1, z_1^5z_2^3-w_2, z_1-w_3, z_2-w_4)\subseteq k[z_1,z_2,w_1,w_2,w_3,w_4].$$

With this basis $G = \{g_1, \dots, g_s\}$, we then compute $(z_1^{37} z_2^{20})^G$ and find $(z_1^{37} z_2^{20})^G = w_2^4 w_1^4 w_3$, which gives the optimal solution of $x_1 = 4$ and $x_2 = 4$. (Please note that I skipped many, many details!)

Concluding Remarks

One or two lectures cannot begin to capture all the subtleties of this method. In fact, it is quite possible to spend an entire semester discussing Gröbner Bases. I am well aware of the limitations of this lecture; for example, I have not talked about such things as (1) how do I find a Gröbner Basis? and (2) how do I cook up an adapted order? My hope is that from this lecture you will take away the fact that commutative algebra and algebraic geometry provide new tools of looking at this problem. Note that Conti and Traverso's original paper [1] is not even 20 years old which makes this a very recent approach to integer programming problems. For more information on this topic, the references below provide an initial starting point to the literature.

Problems from Lecture 4

1. Generalize the proof used in the claim to the general case. That is, consider an integer program of the form

$$\begin{array}{rrcl} \text{Minimize:} & c_1x_1+\cdots+c_nx_n & & \\ \text{Subject to:} & a_{11}x_1+\cdots+a_{1n}x_n & = & b_1 \\ & a_{21}x_1+\cdots+a_{2n}x_n & = & b_2 \\ & & \vdots & \\ & a_{m1}x_1+\cdots+a_{mn}x_n & = & b_m \\ & x_1,\ldots,x_n & \geq & 0. \end{array}$$

and assume all $a_{ij}, b_i \geq 0$. Let $f_j = \prod_{i=1}^m z_i^{a_{ij}}$. Let G be a Gröbner Basis of the ideal

$$(f_1-w_1,\ldots,f_n-w_n) \subseteq k[z_1,\ldots,z_m,w_1,\ldots,w_n]$$

with respect to a monomial ordering with the elimination property: any monomial contain one of the z_i is greater than any monomial containing only the w_j. Let $\varphi : k[w_1,\ldots,w_n] \to k[z_1,\ldots,z_m]$ be the map given by $\varphi(w_i) = f_i$. Let $f = z_1^{b_1}\cdots z_m^{b_m}$, and suppose that $f^G \in k[w_1,\ldots,w_n]$. Show that $\varphi(f^G) = f$.

For more on Gröbner Bases check out the books:

References

[1] Adams, William W.; Loustaunau, Philippe, *An introduction to Gröbner bases.* Graduate Studies in Mathematics, 3. American Mathematical Society, Providence, RI, 1994.

[2] Cox, David, Gröbner Bases Tutorials. Lecture notes available at `http://www.amherst.edu/~dacox/`

[3] Cox, David; Little, John; O'Shea, Donal *Ideals, varieties, and algorithms. An introduction to computational algebraic geometry and commutative algebra. Second edition.* Undergraduate Texts in Mathematics. Springer-Verlag, New York, 1997.

[4] Cox, David; Little, John; O'Shea, Donal *Using algebraic geometry.* Graduate Texts in Mathematics, 185. Springer-Verlag, New York, 1998.

[5] Fröberg, Ralf(S-STOC) *An introduction to Gröbner bases.* Pure and Applied Mathematics (New York). John Wiley & Sons, Ltd., Chichester, 1997.

[6] Kreuzer, Martin; Robbiano, Lorenzo, *Computational commutative algebra. 1.* Springer-Verlag, Berlin, 2000.

For more on Integer Programming using Commutative Algebra and Algebraic Geometry, see Chapter of 8 of [4] (this talk was heavily indebted to this chapter). As well, see

References

[1] Conti, Pasqualina; Traverso, Carlo, Buchberger algorithm and integer programming. Applied algebra, algebraic algorithms and error-correcting codes (New Orleans, LA, 1991), 130–139, Lecture Notes in Comput. Sci., 539, Springer, Berlin, 1991.

[2] Hoşten, Serkan; Thomas, Rekha, *Gröbner bases and integer programming.* Gröbner bases and applications (Linz, 1998), 144–158, London Math. Soc. Lecture Note Ser., 251, Cambridge Univ. Press, Cambridge, 1998.