Lecture 14: Algebraic Geometry I

Today...

- 0/1-integer programming and systems of polynomial equations
- The division algorithm for polynomials of one variable
- Multivariate polynomials
- Ideals and affine varieties
- A division algorithm for multivariate polynomials
- Dickson's Lemma for monomial ideals
- Hilbert Basis Theorem
- Gröbner bases

0/1-Integer Programming Feasibility

- Normally,

$$\sum_{j=1}^{n} a_{ij}x_j = b_i \qquad i = 1, \dots m$$
$$x_j \in \{0,1\} \qquad j = 1, \dots, n$$

- Equivalently,

$$\sum_{j=1}^{n} a_{ij}x_j - b_i = 0 \qquad i = 1, \dots m$$
$$x_j^2 - x_j = 0 \qquad j = 1, \dots, n$$

- Motivates study of systems of polynomial equations

Refresher: Polynomials of One Variable

Some basics:

- Let $f = a_0x^m + a_1x^{m-1} + \cdots + a_m$, where $a_0 \neq 0$.
- We call m the *degree* of f, written $m = \deg(f)$.
- We say a_0x^m is the *leading term* of f, written $\mathrm{LT}(f) = a_0x^m$.
- For example, if $f = 2x^3 - 4x + 3$, then $\deg(f) = 3$ and $\mathrm{LT}(f) = 2x^3$.

- If f and g are nonzero polynomials, then

$$\deg(f) \leq \deg(g) \Longleftrightarrow \mathrm{LT}(f) \text{ divides } \mathrm{LT}(g).$$

The Division Algorithm:

In: g, f

Out: q, r such that $f = q\,g + r$ and $r = 0$ or $\deg(r) < \deg(g)$

1. $q := 0$; $r := f$
2. WHILE $r \neq 0$ AND $\mathrm{LT}(g)$ divides $\mathrm{LT}(r)$ DO
3. $\quad q := q + \mathrm{LT}(r)/\mathrm{LT}(g)$
4. $\quad r := r - (\mathrm{LT}(r)/\mathrm{LT}(g))g$

Polynomials of More than One Variable

Fields:

- A *field* consists of a set k and two binary operations "$\cdot$" and "$+$" which satisfy the following conditions:
  - $(a + b) + c = a + (b + c)$ and $(a \cdot b) \cdot c = a \cdot (b \cdot c)$,
  - $a + b = b + a$ and $a \cdot b = b \cdot a$,
  - $a \cdot (b + c) = a \cdot b + a \cdot c$,
  - there are $0, 1 \in k$ such that $a + 0 = a \cdot 1 = a$,
  - given $a \in k$ there is $b \in k$ such that $a + b = 0$,
  - given $a \in k$, $a \neq 0$, there is $c \in k$ such that $a \cdot c = 1$.
- Examples include $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$.

Monomials:

- A *monomial* in $x_1, \ldots, x_n$ is a product of the form

  $$x_1^{\alpha_1} \cdot x_2^{\alpha_2} \cdot \ldots \cdot x_n^{\alpha_n},$$

  with $\alpha_1, \ldots, \alpha_n \in \mathbb{Z}_+$.
- We also let $\alpha := (\alpha_1, \ldots, \alpha_n)$ and set

  $$x^\alpha := x_1^{\alpha_1} \cdot x_2^{\alpha_2} \cdot \ldots \cdot x_n^{\alpha_n}.$$
- The *total degree* of x^α is $|\alpha| := \alpha_1 + \cdots + \alpha_n$.

Polynomials:

- A *polynomial* in $x_1, \dots, x_n$ is a finite linear combination of monomials,

$$f = \sum_{\alpha \in S} a_\alpha x^\alpha,$$

where $a_\alpha \in k$ for all $\alpha \in S$, and $S \subseteq \mathbb{Z}_+^n$ is finite.

- The set of all polynomials in $x_1, \dots, x_n$ with coefficients in k is denoted by $k[x_1, \dots, x_n]$.
- We call a_α the *coefficient* of the monomial x^α.
- If $a_\alpha \neq 0$, then $a_\alpha x^\alpha$ is a term of f.
- The *total degree* of f, $\deg(f)$, is the maximum $|\alpha|$ such that $a_\alpha \neq 0$.

Example:

- $f = 2x^3y^2z + \frac{3}{2}y^3z^3 - 3xyz + y^2$
- Four terms, total degree six
- Two terms of max total degree, which cannot happen in one variable
- What is the leading term?

Orderings on the Monomials in $k[x_1, \dots, x_n]$

- For the division algorithm on polynomials in one variable, $\cdots > x^{m+1} > x^m > \cdots > x^2 > x > 1$.
- In Gaussian elimination for systems of linear equations, $x_1 > x_2 > \cdots > x_n$.
- Note that there is a one-to-one correspondence between the monomials in $k[x_1, \dots, x_n]$ and $\mathbb{Z}_+^n$.
- A *monomial ordering* on $k[x_1, \dots, x_n]$ is any relation $>$ on $\mathbb{Z}_+^n$ that satisfies
  1. $>$ is a total ordering,
  2. if $\alpha > \beta$ and $\gamma \in \mathbb{Z}_+^n$, then $\alpha + \gamma > \beta + \gamma$,
  3. every nonempty subset of $\mathbb{Z}_+^n$ has a smallest element under $>$.

Examples of Monomial Orderings

- Lex Order: For $\alpha, \beta \in \mathbb{Z}_+^n$, $\alpha >_{\text{lex}} \beta$ if the left-most nonzero entry of $\alpha - \beta$ is positive. We write $x^\alpha >_{\text{lex}} x^\beta$ if $\alpha >_{\text{lex}} \beta$.
  - For example, $(1, 2, 0) >_{\text{lex}} (0, 3, 4)$ and $(3, 2, 4) >_{\text{lex}} (3, 2, 1)$.
  - Also, $x_1 >_{\text{lex}} x_2^5 x_3^3$.
- Graded Lex Order: For $\alpha, \beta \in \mathbb{Z}_+^n$, $\alpha >_{\text{grlex}} \beta$ if $|\alpha| > |\beta|$ or $|\alpha| = |\beta|$ and $\alpha >_{\text{lex}} \beta$.
  - For example, $(1, 2, 3) >_{\text{grlex}} (3, 2, 0)$ and $(1, 2, 4) >_{\text{grlex}} (1, 1, 5)$.

Further Definitions

Let $f = \sum_\alpha a_\alpha x^\alpha$ be a nonzero polynomial in $k[x_1, \dots, x_n]$ and let $>$ be a monomial order.

- The *multidegree* of f is

$$\text{multideg}(f) := \max_{>}\{\alpha \in \mathbb{Z}^n_+ : a_\alpha \neq 0\}.$$

- The *leading coefficient* of f is

$$\text{LC}(f) := a_{\text{multideg}(f)}.$$

- The *leading monomial* of f is

$$\text{LM}(f) := x^{\text{multideg}(f)}.$$

- The *leading term* of f is

$$\text{LT}(f) := \text{LC}(f) \cdot \text{LM}(f).$$

Example

Let $f = 4xy^2z + 4z^2 - 5x^3 + 7x^2z^2$ and let $>$ denote the lex order. Then

$$\text{multideg}(f) = (3, 0, 0),$$

$$\text{LC}(f) = -5,$$

$$\text{LM}(f) = x^3$$

$$\text{LT}(f) = -5x^3.$$

The Basic Algebraic Object of this Lecture

- A subset $I \subseteq k[x_1, \dots x_n]$ is an *ideal* if it satisfies:
  1. $0 \in I$,
  2. if $f, g \in I$, then $f + g \in I$,
  3. if $f \in I$ and $h \in k[x_1, \dots x_n]$, then $h\,f \in I$.

- Let $f_1, \dots, f_s \in k[x_1, \dots x_n]$. Then

$$\langle f_1, \dots, f_s \rangle := \left\{ \sum_{i=1}^{s} h_i\, f_i : h_1, \dots, h_s \in k[x_1, \dots x_n] \right\}$$

  is an ideal of $k[x_1, \dots x_n]$. (We call it the ideal *generated by* $f_1, \dots, f_s$.)

- An ideal I is *finitely generated* if $I = \langle f_1, \dots, f_s \rangle$, and we say that $f_1, \dots, f_s$ are a *basis* of I.

Polynomial Equations

Given $f_1, \dots, f_s \in k[x_1, \dots x_n]$, we get the system of equations

$$f_1 = 0, \dots, f_s = 0.$$

If we multiply the first equation by h_1, the second one by h_2, and so on, we obtain

$$h_1 f_1 + h_2 f_2 + \cdots + h_s f_s = 0,$$

which is a consequence of the original system.

Thus, we can think of $\langle f_1, \dots, f_s \rangle$ as consisting of all "polynomial consequences" of $f_1 = f_2 = \cdots = f_s = 0$.

- Let $f_1, \dots, f_s \in k[x_1, \dots x_n]$. Then we set

  $$V(f_1, \dots, f_s) := \{(a_1, \dots, a_n) \in k^n : f_i(a_1, \dots, a_n) = 0, i = 1, \dots, s\}$$

  and call $V(f_1, \dots, f_s)$ an *affine variety.*

- If $\langle f_1, \dots, f_s \rangle = \langle g_1, \dots, g_t \rangle$, then $V(f_1, \dots, f_s) = V(g_1, \dots, g_t)$.

- Let $V \subseteq k^n$ be an affine variety. Then we set

  $$I(V) := \{f \in k[x_1, \dots, x_n] : f(a_1, \dots, a_n) = 0 \text{ for all } (a_1, \dots, a_n) \in V\}.$$

- If V is an affine variety, then $I(V)$ is an ideal.

Driving Questions

- Does every ideal have a finite generating set?

- Given $f \in k[x_1, \dots, x_n]$ and $I = \langle f_1, \dots, f_s \rangle$, is $f \in I$?

- Find all solutions in k^n of a system of polynomial equations

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

- Find a "nice" basis for $\langle f_1, \dots, f_s \rangle$.

A Division Algorithm in $k[x_1, \dots, x_n]$

- Goal: Divide f by $f_1, \dots, f_s$.

- Example 1: Divide $f = xy^2 + 1$ by $f_1 = xy + 1$ and $f_2 = y + 1$, using lex order with $x > y$. This leads to

  $$xy^2 + 1 = y \cdot (xy + 1) + (-1) \cdot (y + 1) + 2.$$

- Example 2a: Divide $f = x^2y + xy^2 + y^2$ by $f_1 = xy - 1$ and $f_2 = y^2 - 1$, using lex order with $x > y$. This eventually leads to

  $$x^2y + xy^2 + y^2 = (x + y) \cdot (xy - 1) + 1 \cdot (y^2 - 1) + x + y + 1.$$

Theorem 1. *Fix a monomial order on $\mathbb{Z}_+^n$, and let $(f_1, \dots, f_s)$ be an ordered tuple of polynomials in $k[x_1, \dots, x_n]$. Then every $f \in k[x_1, \dots, x_n]$ can be written as*

$$f = a_1 + \cdots a_s f_s + r,$$

where $a_i, r \in k[x_1, \dots, x_n]$, and either $r = 0$ or r is a linear combination, with coefficients in k, of monomials, none of which is divisible by any of $LT(f_1), \dots, LT(f_s)$.

We call r a remainder *of f on division by $(f_1, \dots, f_s)$. If $a_i f_i \neq 0$, then*

$$multideg(f) \geq multideg(a_i f_i).$$

```
a_1 := 0; ..., a_s := 0; r := 0
p := f
WHILE p ≠ 0 DO
    i := 1
    WHILE i ≤ s AND no division occurred DO
        IF LT(f_i) divides LT(p) THEN
            a_i := a_i + LT(p)/LT(f_i)
            p := p − (LT(p)/LT(f_i))f_i
        ELSE
            i := i + 1
    IF no division occured THEN
        r := r + LT(p)
        p := p − LT(p)
```

More Examples

- Example 2b: Divide $f = x^2y + xy^2 + y^2$ by $f_1 = y^2 - 1$ and $f_2 = xy - 1$, using lex order with $x > y$. This leads to

$$x^2y + xy^2 + y^2 = (x+1) \cdot (y^2 - 1) + x \cdot (xy - 1) + 2x + 1.$$

- The remainder is different from the one in Example 2a!
- Example 3a: Divide $f = xy^2 - x$ by $f_1 = xy + 1$ and $f_2 = y^2 - 1$ with the lex order. The result is

$$xy^2 - x = y \cdot (xy + 1) + 0 \cdot (y^2 - 1) + (-x - y).$$

- Example 3b: Divide $f = xy^2 - x$ by $f_1 = y^2 - 1$ and $f_2 = xy + 1$ with the lex order. The result is

$$xy^2 - x = x \cdot (y^2 - 1) + 0 \cdot (xy + 1) + 0.$$

- The second calculation shows $f \in \langle f_1, f_2 \rangle$, but the first does not!

Monomial Ideals

- An ideal I is a *monomial ideal* if there is $A \subseteq \mathbb{Z}_+^n$ such that I consists of all finite sums $\sum_{\alpha \in A} h_\alpha x^\alpha$. We write $I = \langle x^\alpha : \alpha \in A \rangle$.

- Let $I = \langle x^\alpha : \alpha \in A \rangle$. Then $x^\beta \in I$ iff x^β is divisible by x^α for some $\alpha \in A$.

- x^β is divisible by x^α iff $\beta = \alpha + \gamma$ for some $\gamma \in \mathbb{Z}_+^n$. Thus,

$$\alpha + \mathbb{Z}_+^n$$

  consists of the exponents of all monomials divisible by x^α.

- If I is a monomial ideal, then $f \in I$ iff every term of f lies in I.

Dickson's Lemma

- Let $A \subseteq \mathbb{Z}_+^n$. Then

$$\bigcup_{\alpha \in A} (\alpha + \mathbb{Z}_+^n)$$

  can be expressed as the union of a finite subset of the $\alpha + \mathbb{Z}_+^n$.

- A monomial ideal $I = \langle x^\alpha : \alpha \in A \rangle$ can be written in the form $I = \langle x^{\alpha(1)}, \ldots, x^{\alpha(s)} \rangle$, where $\alpha(1), \ldots, \alpha(s) \in A$.

Hilbert Basis Theorem: Preliminaries

Let $I \subseteq k[x_1, \ldots, x_n]$ be an ideal other than $\{0\}$.

- Let $\mathrm{LT}(I)$ = the set of leading terms of elements in I.

- $\langle \mathrm{LT}(I) \rangle$ is a monomial ideal.

- There are $g_1, \ldots, g_s \in I$ such that

$$\langle \mathrm{LT}(I) \rangle = \langle \mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_s) \rangle.$$

Hilbert Basis Theorem

Theorem 2 (Hilbert 1888)**.** *Every ideal $I \subseteq k[x_1, \ldots, x_n]$ has a finite generating set. That is, $I = \langle g_1, \ldots, g_s \rangle$ for some $g_1, \ldots, g_s \in I$.*

Hilbert Basis Theorem: Proof

- Let $I \neq \{0\}$. Recall that $\langle \mathrm{LT}(I) \rangle = \langle \mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_s) \rangle$.

- Claim: $\langle I \rangle = \langle g_1, \ldots, g_s \rangle$.

- Let $f \in I$. If we divide f by $g_1, \ldots, g_s$, we get

$$f = a_1 g_1 + \cdots + a_s g_s + r,$$

where no term of r is divisible by any of $\mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_s)$.

- Claim: $r = 0$.

- Suppose $r \neq 0$. Note that $r \in I$.

- Hence, $\mathrm{LT}(r) \in \langle \mathrm{LT}(I) \rangle = \langle \mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_s) \rangle$.

- So $\mathrm{LT}(r)$ must be divisible by some $\mathrm{LT}(g_i)$. Contradiction!

- Thus, $f = a_1 g_1 + \cdots + a_s g_s$, which shows $I \subseteq \langle g_1, \ldots, g_s \rangle$.

Gröbner Bases

Fix a monomial order.

- A subset $\{g_1, \ldots, g_s\}$ of an ideal I is called a *Gröbner basis* if

$$\langle \mathrm{LT}(I) \rangle = \langle \mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_s) \rangle.$$

- Equivalently, $\{g_1, \ldots, g_s\}$ is a Gröbner basis of I iff the leading term of any element in I is divisible by one of the $\mathrm{LT}(g_i)$.

- Note that every ideal $I \neq \{0\}$ has a Gröbner basis. Moreover, any Gröbner basis of I is a basis of I.

Next Time

- Properties of Gröbner bases

- Computation of Gröbner bases (Buchberger's Algorithm)

- Solving 0/1-integer programs

- Solving (general) integer programs