Lecture 15: Algebraic Geometry II

Today...

- Ideals in \( k[x] \)
- Properties of Gröbner bases
- Buchberger’s algorithm
- Elimination theory
- The Weak Nullstellensatz
- 0/1-Integer Programming

The Structure of Ideals in \( k[x] \)

**Theorem 1.** If \( k \) is a field, then every ideal of \( k[x] \) is of the form \( \langle f \rangle \) for some \( f \in k[x] \). Moreover, \( f \) is unique up to multiplication by a nonzero constant in \( k \).

**Proof:**

- If \( I = \{0\} \), then \( I = \langle 0 \rangle \). So assume \( I \neq \{0\} \).
- Let \( f \) be a nonzero polynomial of minimum degree in \( I \). Claim: \( \langle f \rangle = I \).
- Clearly, \( \langle f \rangle \subseteq I \). Let \( g \in I \) be arbitrary.
- The division algorithm yields \( g = qf + r \), where either \( r = 0 \) or \( \deg(r) < \deg(f) \).
- \( I \) is an ideal, so \( qf \in I \), and, thus, \( r = g - qf \in I \).
- By the choice of \( f \), \( r = 0 \).
- But then \( g = qf \in \langle f \rangle \).

Reminder: Gröbner Bases

- Fix a monomial order. A subset \( \{g_1, \ldots, g_s\} \) of an ideal \( I \) is a **Gröbner basis of \( I \)** if
  \[
  \langle \LT(g_1), \ldots, \LT(g_s) \rangle = \langle \LT(I) \rangle.
  \]
- Equivalently, \( \{g_1, \ldots, g_s\} \subseteq I \) is a Gröbner basis of \( I \) iff the leading term of any element in \( I \) is divisible by one of the \( \LT(g_i) \).
Properties of Gröbner Bases I

**Theorem 2.** Let $G = \{g_1, \ldots, g_s\}$ be a Gröbner basis for an ideal $I$, and let $f \in k[x_1, \ldots, x_n]$. Then the remainder $r$ on division of $f$ by $G$ is unique, no matter how the elements of $G$ are listed when using the division algorithm.

**Proof:**

- First, recall the following result: Let $I = \langle x^\alpha : \alpha \in A \rangle$ be a monomial ideal. Then a monomial $x^\beta$ lies in $I$ iff $x^\beta$ is divisible by $x^\alpha$ for some $\alpha \in A$.
- Suppose $f = a_1g_1 + \cdots + a_sg_s + r = a'_1g_1 + \cdots + a'_sg_s + r'$ with $r \neq r'$.
- Then $r - r' \in I$ and, thus, $\text{LT}(r - r') \in \langle \text{LT}(I) \rangle = \langle \text{LT}(g_1), \ldots, \text{LT}(g_s) \rangle$.
- The lemma implies that $\text{LT}(r - r')$ is divisible by one of $\text{LT}(g_1), \ldots, \text{LT}(g_s)$.
- This is impossible since no term of $r, r'$ is divisible by one of $\text{LT}(g_1), \ldots, \text{LT}(g_s)$.

S-Polynomials

- Let $I = \langle f_1, \ldots, f_t \rangle$.
- We show that, in general, $\langle \text{LT}(I) \rangle$ can be strictly larger than $\langle \text{LT}(f_1), \ldots, \text{LT}(f_t) \rangle$.
- Consider $I = \langle f_1, f_2 \rangle$, where $f_1 = x^3 - 2xy$ and $f_2 = x^2y - 2y^2 + x$ with grlex order.
- Note that
  \[ x \cdot (x^2y - 2y^2 + x) - y \cdot (x^3 - 2xy) = x^2, \]
  so $x^2 \in I$. Thus $x^2 = \text{LT}(x^2) \in \langle \text{LT}(I) \rangle$.
- However, $x^2$ is not divisible by $\text{LT}(f_1) = x^3$ or $\text{LT}(f_2) = x^2y$, so that $x^2 \notin \langle \text{LT}(f_1), \text{LT}(f_2) \rangle$.
- What happened?

- The leading terms in a suitable combination
  \[ ax^\alpha f_i - bx^\beta f_j \]
  may cancel, leaving only smaller terms.

- On the other hand, $ax^\alpha f_i - bx^\beta f_j \in I$, so its leading term is in $\langle \text{LT}(I) \rangle$.
- This is an “obstruction” to $\{f_1, \ldots, f_t\}$ being a Gröbner basis.

- Let $f, g \in k[x_1, \ldots, x_n]$ be nonzero polynomials with $\text{multideg}(f) = \alpha$ and $\text{multideg}(g) = \beta$.
- Let $\gamma_i = \max(\alpha_i, \beta_i)$. We call $x^\gamma$ the least common multiple of $\text{LM}(f)$ and $\text{LM}(g)$.
- The S-polynomial of $f$ and $g$ is defined as
  \[ S(f, g) = \frac{x^\gamma}{\text{LT}(f)} \cdot f - \frac{x^\gamma}{\text{LT}(g)} \cdot g. \]
• An S-polynomial is designed to produce cancellation of leading terms.

Example:

• Let \( f = x^3 y^2 - x^2 y^3 + x \) and \( g = 3x^4 y + y^2 \) with the grlex order.

• Then \( \gamma = (4, 2) \).

• Moreover,

\[
S(f, g) = \frac{x^4 y^2}{x^3 y^2} \cdot f - \frac{x^4 y^2}{3x^4 y} \cdot g = x \cdot f - \frac{1}{3} y \cdot g = -x^3 y^3 + x^2 \cdot \frac{1}{3} y^3
\]

• Consider \( \sum_{i=1}^{t} c_i f_i \), where \( c_i \in k \) and \( \text{multideg}(f_i) = \delta \in \mathbb{Z}^n_+ \) for all \( i \).

• If \( \text{multideg}(\sum_{i=1}^{t} c_i f_i) < \delta \), then \( \sum_{i=1}^{t} c_i f_i \) is a linear combination, with coefficients in \( k \), of the S-polynomials \( S(f_j, f_k) \) for \( 1 \leq j, k \leq t \).

• Moreover, each \( S(f_j, f_k) \) has multidegree \( < \delta \).

\[
\sum_{i=1}^{t} c_i f_i = \sum_{j, k} c_{jk} S(f_j, f_k)
\]

Properties of Gröbner Bases II

**Theorem 3.** A basis \( G = \{g_1, \ldots, g_s\} \) for an ideal \( I \) is a Gröbner basis iff for all pairs \( i \neq j \), the remainder on division of \( S(g_i, g_j) \) by \( G \) is zero.

Sketch of proof:

• Let \( f \in I \) be a nonzero polynomial. There are polynomials \( h_i \) such that \( f = \sum_{i=1}^{s} h_i g_i \).

• It follows that \( \text{multideg}(f) \leq \max(\text{multideg}(h_i g_i)) \).

• If “\( < \)”, then some cancellation of leading terms must occur.

• These can be rewritten as S-polynomials.

• The assumption allows us to replace S-polynomials by expressions that involve less cancellation.

• We eventually find an expression for \( f \) such that \( \text{multideg}(f) = \text{multideg}(h_i g_i) \) for some \( i \).

• It follows that \( \text{LT}(f) \) is divisible by \( \text{LT}(g_i) \).

• This shows that \( \text{LT}(f) \in \langle \text{LT}(g_1), \ldots, \text{LT}(g_s) \rangle \). \qed
Buchberger’s Algorithm

- Consider \( I = \langle f_1, f_2 \rangle \), where \( f_1 = x^3 - 2xy \) and \( f_2 = x^2y - 2y^2 + x \) with grlex order. Let \( F = (f_1, f_2) \).
- \( S(f_1, f_2) = -x^2 \); its remainder on division by \( F \) is \(-x^2\).
- Add \( f_3 = -x^2 \) to the generating set \( F \).
- \( S(f_1, f_3) = -2xy \); its remainder on division by \( F \) is \(-2xy\).
- Add \( f_4 = -2xy \) to the generating set \( F \).
- \( S(f_1, f_4) = -2xy^2 \); its remainder on division by \( F \) is 0.
- \( S(f_2, f_3) = -2y^2 + x \); its remainder is \(-2y^2 + x\).
- Add \( f_5 = -2y^2 + x \) to the generating set \( F \).
- The resulting set \( F \) satisfies the “S-pair criterion,” so it is a Gröbner basis.

Buchberger’s Algorithm

The algorithm:

In: \( F = (f_1, \ldots, f_t) \) \{defining \( I = \langle f_1, \ldots, f_t \rangle \} \)

Out: Gröbner basis \( G = (g_1, \ldots, g_s) \) for \( I \), with \( F \subseteq G \)

1. \( G := F \)

2. REPEAT

3. \( G' := G \)

4. FOR each pair \( p \neq q \) in \( G' \) DO

5. \( S := \) remainder of \( S(p, q) \) on division by \( G' \)

6. IF \( S \neq 0 \) THEN \( G := G \cup \{S\} \)

7. UNTIL \( G = G' \)

Buchberger’s Algorithm

Proof of correctness:
- The algorithm terminates when \( G = G' \), which means that \( G \) satisfies the S-pair criterion.

Proof of finiteness:
- The ideals \( \langle \text{LT}(G') \rangle \) from successive iterations form an ascending chain.
Let us call this chain \( J_1 \subset J_2 \subset J_3 \subset \cdots \).

Their union \( J = \bigcup_{i=1}^{\infty} J_i \) is an ideal as well. By Hilbert’s Basis Theorem, it is finitely generated: \( J = \langle h_1, \ldots, h_r \rangle \).

Each of the \( h_i \) is contained in one of the \( J_i \). Let \( N \) be the maximum such index \( i \).

Then \( J = \langle h_1, \ldots, h_r \rangle \subseteq J_N \subset J_{N+1} \subset \cdots \subset J \).

So the chain stabilizes with \( J_N \), and the algorithm terminates after a finite number of steps.

\( \square \)

**Minimal Gröbner Basis**

- Let \( G \) be a Gröbner basis for \( I \), and let \( p \in G \) be such that \( \text{LT}(p) \in \langle \text{LT}(G \setminus \{p\}) \rangle \). Then \( G \setminus \{p\} \) is also a Gröbner basis for \( I \).

- A **minimal Gröbner basis** for an ideal \( I \) is a Gröbner basis \( G \) for \( I \) such that
  1. \( \text{LC}(p) = 1 \) for all \( p \in G \).
  2. For all \( p \in G \), \( \text{LT}(p) \notin \langle \text{LT}(G \setminus \{p\}) \rangle \).

- A given ideal may have many minimal Gröbner bases. But we can single one out that is “better” than the others:

- A **reduced Gröbner basis** for an ideal \( I \) is a Gröbner basis \( G \) for \( I \) such that
  1. \( \text{LC}(p) = 1 \) for all \( p \in G \).
  2. For all \( p \in G \), no monomial of \( p \) lies in \( \langle \text{LT}(G \setminus \{p\}) \rangle \).

**Reduced Gröbner Basis**

**Lemma 4.** Let \( I \neq \{0\} \) be an ideal. Then, for a given monomial ordering, \( I \) has a unique reduced Gröbner basis.

(One can obtain a reduced Gröbner basis from a minimal one by replacing \( g \in G \) by the remainder of \( g \) on division by \( G \setminus \{g\} \), and repeating.)

**Elimination Theory**

- Systematic methods for eliminating variables from systems of polynomial equations.

- For example, consider

\[
x_1 + 2x_2 + 3x_3 + 4x_4 + 5x_5 + 15x_6 - 15 = 0, x_1^2 - x_1 = 0, \ldots, x_6^2 - x_6 = 0.
\]

- The reduced Gröbner basis with respect to lex order is \( G = \{x_6^2 - x_6, x_5 + x_6 - 1, x_4 + x_6 - 1, x_3 + x_6 - 1, x_2 + x_6 - 1, x_1 + x_6 - 1\} \).

- So the original system has exactly two solutions: \( \bar{x} = (1,1,1,1,1,0) \) or \( \bar{x} = (0,0,0,0,0,1) \)
• Given $I = \langle f_1, \ldots, f_s \rangle \subseteq k[x_1, \ldots, x_n]$, the $\ell$-th elimination ideal $I_\ell$ is the ideal of $k[x_{\ell+1}, \ldots, x_n]$ defined by

$$I_\ell = I \cap k[x_{\ell+1}, \ldots, x_n].$$

• $I_\ell$ consists of all consequences of $f_1 = f_2 = \cdots = f_s = 0$ which eliminate the variables $x_1, \ldots, x_\ell$.

• Eliminating $x_1, \ldots, x_\ell$ means finding nonzero polynomials in $I_\ell$.

**Theorem 5.** Let $I \subseteq k[x_1, \ldots, x_n]$ be an ideal, and let $G$ be a Gröbner basis of $I$ with respect to lex order where $x_1 > x_2 > \cdots > x_n$. Then, for every $0 \leq \ell \leq n - 1$, the set

$$G_\ell = G \cap k[x_{\ell+1}, \ldots, x_n]$$

is a Gröbner basis of the $\ell$-th elimination ideal $I_\ell$.

**Proof:**

• It suffices to show that $\langle \text{LT}(I_\ell) \rangle \subseteq \langle \text{LT}(G_\ell) \rangle$.

• We show that $\text{LT}(f)$, for $f \in I_\ell$ arbitrary, is divisible by $\text{LT}(g)$ for some $g \in G_\ell$.

• Note that $\text{LT}(f)$ is divisible by $\text{LT}(g)$ for some $g \in G$.

• Since $f \in I_\ell$, this means that $\text{LT}(g)$ involves only $x_{\ell+1}, \ldots, x_n$.

• Any monomial involving $x_1, \ldots, x_\ell$ is greater than all monomials in $k[x_{\ell+1}, \ldots, x_n]$.

• Hence, $\text{LT}(g) \in k[x_{\ell+1}, \ldots, x_n]$ implies $g \in k[x_{\ell+1}, \ldots, x_n]$.

• Therefore, $g \in G_\ell$.

**The Weak Nullstellensatz**

• Recall that a variety $V \subseteq k^n$ can be studied via the ideal

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

• This gives a map $V \rightarrow I(V)$.

• On the other hand, given an ideal $I$,

$$V(I) = \{ x \in k^n : f(x) = 0 \text{ for all } f \in I \}.$$ 

is an affine variety, by Hilbert’s Basis Theorem.

• This gives a map $I \rightarrow V(I)$.

• Note that the map “$V$” is not one-to-one: for example, $V(x) = V(x^2) = \{0\}$.

• Recall that $k$ is algebraically closed if every nonconstant polynomial in $k[x]$ has a root in $k$. 
- Also recall that $\mathbb{C}$ is algebraically closed (Fundamental Theorem of Algebra).
- Consider $1, 1 + x^2,$ and $1 + x^2 + x^4$ in $\mathbb{R}[x]$. They generate different ideals:
  \[ I_1 = \langle 1 \rangle = \mathbb{R}[x], \quad I_2 = \langle 1 + x^2 \rangle, \quad I_3 = \langle 1 + x^2 + x^4 \rangle. \]
  However, $V(I_1) = V(I_2) = V(I_3) = \emptyset$.
- This problem goes away in the one-variable case if $k$ is algebraically closed:
- Let $I$ be an ideal in $k[x]$, where $k$ is algebraically closed.
- Then $I = \langle f \rangle$, and $V(I)$ are the roots of $f$.
- Since every nonconstant polynomial has a root, $V(I) = \emptyset$ implies that $f$ is a nonzero constant.
- Hence, $1/f \in k$. Thus, $1 = (1/f) \cdot f \in I$.
- Consequently, $g \cdot 1 = g \in I$ for all $g \in k[x]$.
- It follows that $I = k[x]$ is the only ideal of $k[x]$ that represents the empty variety when $k$ is algebraically closed.
- The same holds when there is more than one variable!

**Theorem 6.** Let $k$ be an algebraically closed field, and let $I \subseteq k[x_1, \ldots, x_n]$ be an ideal satisfying $V(I) = \emptyset$. Then $I = k[x_1, \ldots, x_n]$.

(Can be thought of as the “Fundamental Theorem of Algebra for Multivariate Polynomials:” every system of polynomials that generates an ideal smaller than $\mathbb{C}[x_1, \ldots, x_n]$ has a common zero in $\mathbb{C}^n$.)

- The system
  \[ f_1 = 0, \ f_2 = 0, \ldots, \ f_s = 0 \]
  does not have a common solution in $\mathbb{C}^n$ iff $V(f_1, \ldots, f_s) = \emptyset$.
- By the Weak Nullstellensatz, this happens iff $1 \in \langle f_1, \ldots, f_s \rangle$.
- Regardless of the monomial ordering, $\{1\}$ is the only reduced Gröbner basis for the ideal $\langle 1 \rangle$.

**Proof:**
- Let $g_1, \ldots, g_s$ be a Gröbner basis of $I = \langle 1 \rangle$.
- Thus, $1 \in \langle \text{LT}(I) \rangle = \langle \text{LT}(g_1), \ldots, \text{LT}(g_s) \rangle$.
- Hence, $1$ is divisible by some $\text{LT}(g_i)$, say $\text{LT}(g_1)$.
- So $\text{LT}(g_1)$ is constant.
- Then every other $\text{LT}(g_i)$ is a multiple of that constant, so $g_2, \ldots, g_s$ can be removed from the Gröbner basis.
- Since $\text{LT}(g_1)$ is constant, $g_1$ itself is constant. \qed
0/1-Integer Programming: Feasibility

- Normally,
\[ \sum_{j=1}^{n} a_{ij}x_j = b_i \quad i = 1, \ldots, m \]
\[ x_j \in \{0, 1\} \quad j = 1, \ldots, n \]

- Equivalently,
\[ f_i := \sum_{j=1}^{n} a_{ij}x_j - b_i = 0 \quad i = 1, \ldots, m \]
\[ g_j := x_j^2 - x_j = 0 \quad j = 1, \ldots, n \]

An algorithm:

In: \( A \in \mathbb{Z}^{m \times n}, b \in \mathbb{Z}^m \)
Out: a feasible solution \( \bar{x} \) to \( Ax = b, x \in \{0, 1\}^n \)

1. \( I := \langle f_1, \ldots, f_m, g_1, \ldots, g_n \rangle \)
2. Compute a Gröbner basis \( G \) of \( I \) using lex order
3. IF \( G = \{1\} \) THEN
4. “infeasible”
5. ELSE
6. Find \( \bar{x}_n \) in \( V(G_{n_1}) \)
7. FOR \( l = n - 1 \) TO \( 1 \) DO
8. Extend \((\bar{x}_{l+1}, \ldots, \bar{x}_n)\) to \((\bar{x}_l, \ldots, \bar{x}_n) \in V(G_{l-1})\)

Example:
- Consider
\[ x_1 + 2x_2 + 3x_3 + 4x_4 + 5x_5 + 15x_6 = 15 \]
\[ x_1, x_2, \ldots, x_6 \in \{0, 1\} \]
- The reduced Gröbner basis is \( G = \{x_6^2 - x_6, x_5 + x_6 - 1, x_4 + x_6 - 1, x_3 + x_6 - 1, x_2 + x_6 - 1, x_1 + x_6 - 1\} \)
- \( G_5 = \{x_6^2 - x_6\} \), so \( \bar{x}_6 = 0 \) and \( \bar{x}_6 = 1 \) are possible solutions
- We get \( \bar{x} = (1, 1, 1, 1, 0) \) or \( \bar{x} = (0, 0, 0, 0, 1) \)
Structural insights:

- The polynomials in the reduced Gröbner basis can be partitioned into $n$ sets:
  - $S_n$ contains only one polynomial, which is either $x_n$, $x_n - 1$, or $x_n^2 - x_n$.
  - $S_i$, for $1 \leq i \leq n - 1$, contains polynomials in $x_n, \ldots, x_i$.

- Similar to row echelon form in Gaussian elimination.

- Allows solving the system variable by variable.

Example:

Consider

$$x_1 + 2x_2 + 3x_3 + 4x_4 + 6x_5 = 6, \quad x_1, \ldots, x_5 \in \{0, 1\}$$

The reduced Gröbner basis is

$$\{x_5^2 - x_5, x_4x_5, x_4^2 - x_4, x_3 + x_4 + x_5 - 1, x_2 + x_5 - 1, x_1 + x_4 + x_5 - 1\}$$

- The sets are

$$S_5 = \{x_5^2 - x_5\}$$
$$S_4 = \{x_4x_5, x_4^2 - x_4\}$$
$$S_3 = \{x_3 + x_4 + x_5 - 1\}$$
$$S_2 = \{x_2 + x_5 - 1\}$$
$$S_1 = \{x_1 + x_4 + x_5 - 1\}$$

0/1-Integer Programming: Optimization

Modify the algorithm as follows:

- Let $h = y - \sum_{j=1}^{n} c_j x_j$.

- Consider $k[x_1, \ldots, x_n, y]$ and $V(f_1, \ldots, f_m, g_1, \ldots, g_m, h)$.

- Use lex order with $x_1 > \cdots > x_n > y$.

- The reduced Gröbner basis is either $\{1\}$ or its intersection with $k[y]$ is a polynomial in $y$.

- Every root of this polynomial is an objective function value that can be feasibly attained.

- Find the minimum root, and work backwards to get the associated values of $x_n, \ldots, x_1$.

Example:

min $\{x_1 + 2x_2 + 3x_3 : x_1 + 2x_2 + 2x_3 = 3, x_1, \ldots, x_3 \in \{0, 1\}\}$.

The reduced Gröbner basis is

$$\{12 - 7y + y^2, 3 + x_3 - y, -4 + x_2 + y, 1 - x_1\}.$$

- The two roots of $12 - 7y + y^2$ are 3 and 4.

- The minimum value is $y = 3$, and the corresponding solution is $(1, 1, 0)$. 