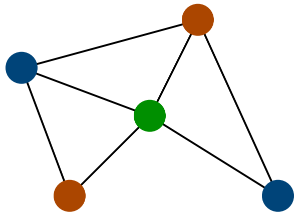
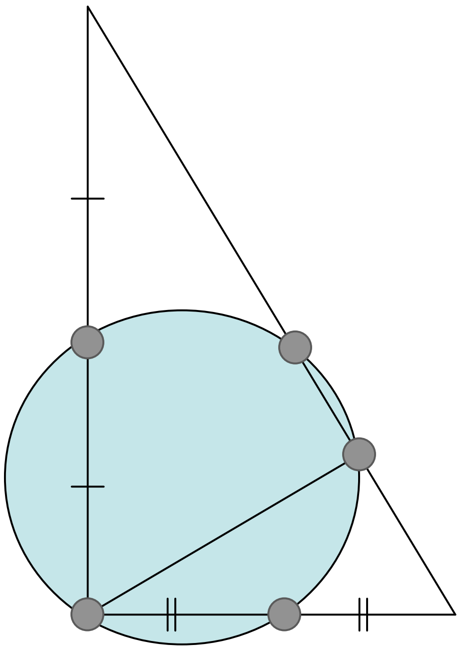


$$\Longrightarrow \qquad I_{G,k} = \langle g_1, \ldots, g_n \rangle$$

Gröbner Bases and Applications



Christopher Hillar
(MSRI)

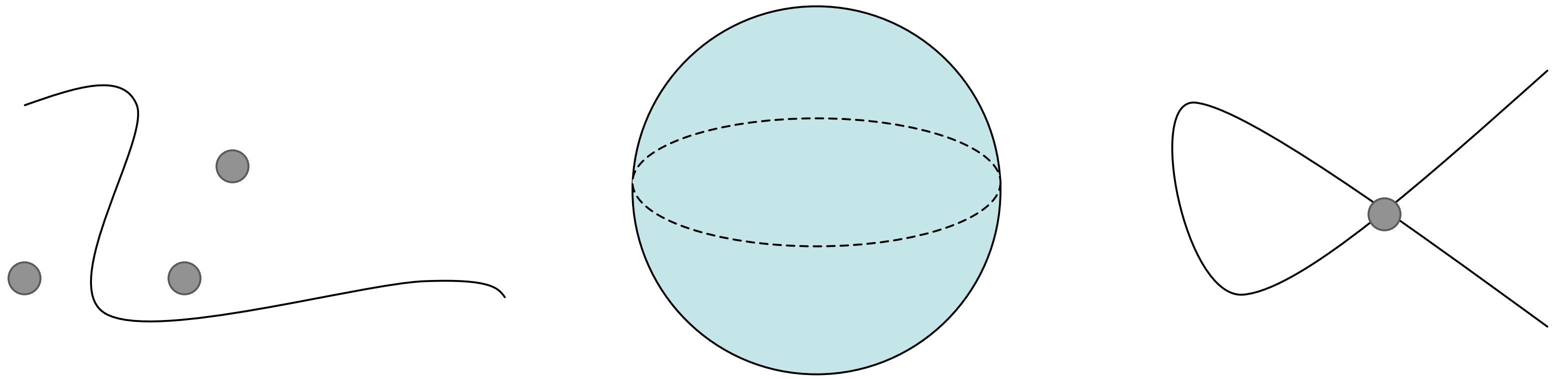
Outline of talk

- Introduction: Varieties and Ideals
- Gröbner Bases: Term Orderings, Polynomial Reduction, Basic Properties
- Algorithms: Buchberger's Criterion
- Applications: Elimination Theory, Theorem Proving, Graph Coloring, Integer Programming

Algebraic Geometry

Given a set of polynomials $F \subseteq \mathbf{C}[x_1,\ldots,x_n]$,
we would like to understand the variety:

$$V(F) = \{ (v_1,\ldots,v_n) \in \mathbf{C}^n \mid f(v) = 0 \text{ for all } f \text{ in } F\}$$



#points, dimension, singularities, ...

Ideals and Varieties

Definition: The ideal $I = \langle F \rangle$ generated by F is

$$I = \{p_1 f_1 + \cdots + p_m f_m \mid p_i \in \mathrm{C}[x_1,\ldots,x_n],\ f_i \in F\}$$

Notice that

$$\mathrm{V}(I) = \mathrm{V}(\langle F \rangle) = \mathrm{V}(F)$$

Important facts:

(HBT) Hilbert's Basis Theorem: If $F \subseteq \mathrm{C}[x_1,\ldots,x_n]$, then

$$\langle F \rangle = \langle f_1, f_2, \ldots, f_m \rangle \text{ for some } f_i \in F$$

(HN) Hilbert's Nullstellensatz:

$$\mathrm{V}(I) = \varnothing \quad \Leftrightarrow \quad I = \langle 1 \rangle = \mathrm{C}[x_1,\ldots,x_n]$$

Ideals and Varieties

These theorems allow us to do computational mathematics with varieties.

Hilbert's Basis Theorem (HBT): Every chain

$$I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots \subseteq I_n \subseteq I_{n+1} \cdots$$

eventually stabilizes

$$I_N = I_{N+1} = I_{N+2} = \cdots \quad \text{for some } N$$

Hilbert's Nullstellensatz (HN): There is an algebraic witness to a variety being empty:

$$V(\langle F \rangle) = \emptyset \quad \Leftrightarrow \quad 1 = p_1 f_1 + \cdots + p_m f_m$$

PID's ($n = 1$)

For intuition, first consider polynomial rings $\mathbb{C}[x]$ in a single indeterminate x

HBT (PID): For any set of polynomials F, there is a polynomial g such that

$$\langle g \rangle = \langle F \rangle$$

g is the greatest common divisor GCD(F) of all polynomials in F. Finding g is the Euclidean Algorithm

---

HN (PID): There is a no common zero of all the polynomials in F if and only if g = GCD(F) = 1

$$1 = p_1 f_1 + \cdots + p_m f_m$$

Algorithmic Motivation

The Nullstellensatz reduces the decidability question:

$$V(F) \text{ empty} \quad \Leftrightarrow \quad 1 \in \langle F \rangle$$

More generally, given an ideal $I = \langle F \rangle$ and an arbitrary polynomial h, we would like to answer

Ideal Membership: Is $h \in I$?

Solution: Compute a nicer representation $I = \langle G \rangle$ of the ideal $I = \langle F \rangle$. The set G is a Grobner Basis for F

$$F \xrightarrow{\text{Buchberger}} G \xrightarrow{\text{Reduction}} nf_G(h) = 0?$$

Monomial Term Orders

Definition: A term order (or monomial order) is a total order $<$ on the set of monomials $\mathbf{x}^{\mathbf{a}} = x_1^{a1} x_2^{a2} \cdots x_n^{an}$ s.t.:

(1) it is multiplicative: $\mathbf{x}^{\mathbf{a}} < \mathbf{x}^{\mathbf{b}} \Rightarrow \mathbf{x}^{\mathbf{a+c}} < \mathbf{x}^{\mathbf{b+c}}$

(2) the constant monomial is smallest, i.e.

$$1 < \mathbf{x}^{\mathbf{a}} \quad \text{for all} \quad \mathbf{a} \text{ in } \mathbf{N}^n \backslash \{0\}$$

In one variable, only one order: $1 < x < x^2 < x^3 < \cdots$

For n = 2, we have

degree lexicographic order

$$1 < x_1 < x_2 < x_1^2 < x_1x_2 < x_2^2 < x_1^3 < x_1^2x_2 < \cdots$$

purely lexicographic order

$$1 < x_1 < x_1^2 < x_1^3 < \cdots < x_2 < x_1x_2 < x_1^2x_2 < \cdots$$

Initial monomials and Ideals

When $n = 1$, clear notion of largest term. For $n > 1$, Term orders necessary for the Buchberger Algorithm.

Definition: Every polynomial $f \in \mathbf{C}[x_1,\ldots,x_n]$ has an initial monomial (given a term order) denoted by $in_<(f)$

Example: if n = 2 and our term order is degree lex,

$$in_<(x_1 + 2x_1^3x_2^2 + 5x_2^4 + 3x_1^2x_2^3) = 3x_1^2x_2^3$$

Definition: For every ideal I of $\mathbf{C}[x_1,\ldots,x_n]$, we can form the initial ideal of I (with respect to <) generated by all initial monomials of polynomials in I:

$$in_<(I) = \langle\, in_<(f) \mid f \in I \,\rangle$$

Defining Gröbner Bases

Definition: A finite subset G of an ideal I is a Gröbner basis (w.r.t to <) if

$$\mathrm{in}_<(I) = \langle\, \mathrm{in}_<(g) \;\mid\; g \in G \,\rangle$$

Example: (pure lex) Let $F = \{x_2^2 - x_1,\ x_2\}$. Then F is not a Gröbner basis for $I = \langle F \rangle$ since

$$x_1 = x_2 \cdot x_2 - 1 \cdot (x_2^2 - x_1) \in I$$

so that $x_1 \in \mathrm{in}_<(I)$ but

$$x_1 \notin \langle x_2^2, x_2 \rangle = \langle x_2 \rangle$$

However, $G = \{x_1, x_2\}$ is a Gröbner basis

Gröbner Bases

Fact: *A* Gröbner **basis** generates the ideal I

Theorem: Fixing an ideal I contained in $\mathbf{C}[x_1,\ldots,x_n]$ and a term order <, there is an algorithm to find a unique reduced Gröbner Basis G for I

- Existence of a Gröbner basis follows from HBT

-Algorithm for producing G given F by Buchberger (1965), under supervision of his advisor Gröbner

-Hironaka developed something similar (standard bases) for his theorem on resolutions of singularites

Fundamental Thm of Algebra

Theorem (FTA): The number of zeroes $|V(I)|$ is the number of monomials not inside $\mathrm{in}_{<}(\mathcal{I})$

Example: $F = \{x_2^2 - x_1,\ x_2\}$. Using purely lex order, we have Grobner basis $G = \{x_1, x_2\}$ so $\mathrm{in}_{<}(\mathcal{I}) = \langle x_1, x_2 \rangle$ and thus $|V(\langle F \rangle)| = 1$.

Example: $(n = 1)$ $F = \{f(x)\}$. Then, $G = \{f\}$ is a Grobner basis for $I = \langle F \rangle$. Thus,

$$\mathrm{in}_{<}(\mathcal{I}) = \langle x^{\deg(f)} \rangle$$

and so there are $\deg(f)$ zeroes for f.

Computing Gröbner Bases

Fix a term order $<$. Given a set of polynomials G and a polynomial h, there is a way to divide h by G and produce a normal form, called the **division algorithm**

$$h = p_1 g_1 + \cdots + p_m g_m + r$$

Definition: Take g, g' in G and form the S-polynomial $m'g - mg'$ where m, m' are monomials of lowest degree s.t. $m' \cdot in_<(g) = m \cdot in_<(g')$

Theorem (Buchberger's Criterion): G is a Gröbner Basis iff every S-polynomial has normal form zero w.r.t. G

If G is a Gröbner basis, then $nf_G(h) = r$ is **unique**

Buchberger's Algorithm

Input: Finite list F of polynomials in $\mathbf{C}[x_1,\ldots,x_n]$
Output: Reduced Gröbner Basis G for F.

Step 1: Apply Buchberger's Criterion to check whether F is a GB.

Step 2: If "yes," then F is a GB. goto Step 4.

Step 3: If "no," we found $r = \mathrm{nf}_F(m'g\text{-}mg') \neq 0$. Set $F = F \cup \{r\}$ and goto step 1.

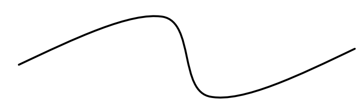
Step 4: Replace F by the reduced Gröbner Basis G and output G

-Terminates by Hilbert's Basis Theorem

Solving with Gröbner Bases

The Grobner basis G encodes more transparently the information about the ideal (and hence the variety)

Given a set $F = \{f_1,\ldots,f_m\}$, if one computes a Grobner Basis G, then one solves



dim = 1

(1) Deciding if there are any solutions

$$V(F) = \{\, v \mid f_1(v) = 0,\ f_2(v) = 0,\ \ldots\ ,\ f_m(v) = 0 \,\}$$

(2) Determining $|V(F)|$, $\dim(V(F))$, Hilbert Polynomials, ...

(3) Ideal membership: Is $h \in I$? (Check $nf_G(h) = 0$)

Elimination example

With appropriate term orders, one can use Grobner bases to eliminate indeterminates from equations

Example: Find the defining equation over the rationals for the algebraic number z defined as the solution to

$$p(z) = z^5 + \sqrt{2}\, z^3 - a^2z + a = 0$$

where a is a solution to $a^3 + a - 1 = 0$.

$F = \{x^2 - 2,\ a^3 + a - 1,\ z^5 + xz^3 - a^2z + a\}$, $<$ is lex with $a > x > z$. Compute a GB G. There will be an element of G only involving z. This is the answer.

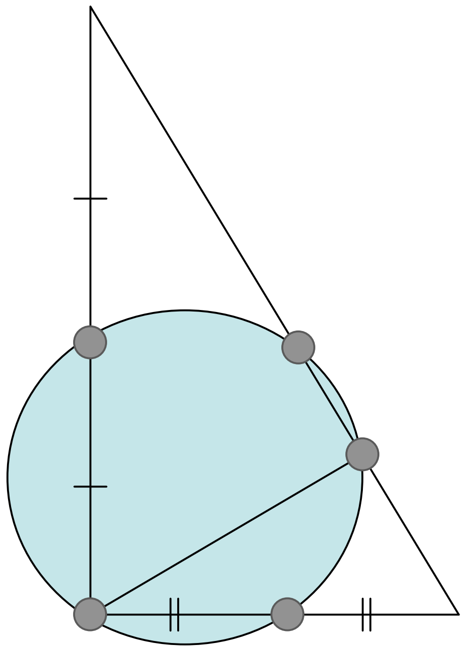
Automatic Theorem Proving

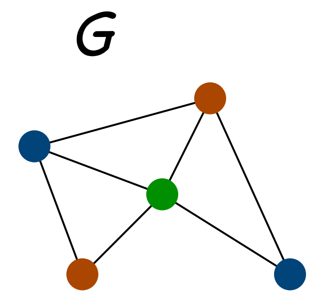
Theorem: The altitude and midpoints of a right triangle lie on a circle

proof: Write down the equations for the input (sides of triangle, midpoints, circle with altitude as chord, etc), compute a GB G, and then check that

$$\mathrm{nf}_G(h) = 0$$

for polynomials h that say the midpoints lie on the circle.





Graph Colorings

Let G be a simple graph $G = (V,E)$ with vertices $V = \{1,2,\ldots,n\}$, edges E

Definition: A *k*-coloring of G is an assignment of k colors to the vertices of G

Definition: A k-coloring is proper if adjacent vertices receive different colors

Definition: A graph is *k*-colorable if it has a proper k-coloring

Algebraic Colorability

Main Idea (implicit in work of Bayer, de Loera, Lovász):

colorings are points in varieties

$\Downarrow$

varieties are represented by ideals

$\Downarrow$

ideals can be manipulated with **Groebner Bases**

k-Colorings as Points in Varieties

Setup: F is an algebraically closed field, (char F) $\nmid k$

So F contains k distinct kth roots of unity. Let

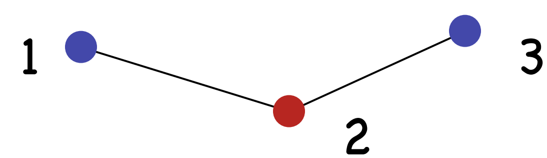
$$I_k = \langle x_1^k - 1,\ x_2^k - 1,\ \ldots,\ x_n^k - 1 \rangle \subset F[x_1,\ldots,x_n]$$

This ideal is radical, and $|V(I_k)| = k^n$

Can think of point $v = (v_1,\ldots,v_n)$ in $V(I_k)$ as assignment

$$v = (v_1,\ldots,v_n) \quad \Longleftrightarrow \quad \text{vertex } i \text{ gets color } v_i$$

Eg. If 1 = Blue, -1 = Red, then $v = (1,-1,1)$ is coloring



Proper k-Colorings of Graphs

We can also restrict to proper k-colorings of graph G

$$I_{G,k} = I_k + \langle x_i^{k-1} + x_i^{k-2}x_j + \cdots + x_j^{k-1} : (i,j) \in E \rangle$$

This ideal is radical, and $|V(I_{G,k})|$ = # proper k-colorings

---

Proof: (=>) If v in $V(I_{G,k})$, wts v proper. If $v_i = v_j$ for $(i,j) \in E$, then

$$0 = v_i^{k-1} + v_i^{k-2}v_j + \cdots + v_j^{k-1} = kv_i^{k-1}$$

(<=) If v proper, then $v_i \neq v_j$ and

$$(v_i - v_j) \cdot (v_i^{k-1} + \cdots + v_j^{k-1}) = v_i^k - v_j^k = 1 - 1 = 0$$

Thus, $v_i^{k-1} + \cdots + v_j^{k-1} = 0$ and v in $V(I_{G,k})$

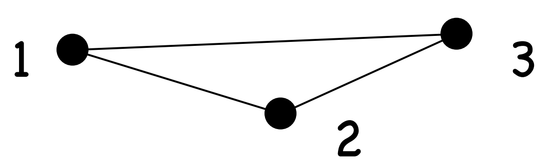
Algebraic Characterization

Notice that if $I_{G,k} = \langle 1 \rangle = F[x_1,\ldots,x_n]$ then

$$V(I_{G,k}) = \varnothing \quad \Rightarrow \quad G \text{ is not } k\text{-colorable}$$

Therefore, we have a test for k-colorability:

Algorithm: Compute a reduced Groebner basis B for $I_{G,k}$. Then, $B = \{1\}$ iff G is not k-colorable.



(k = 2)

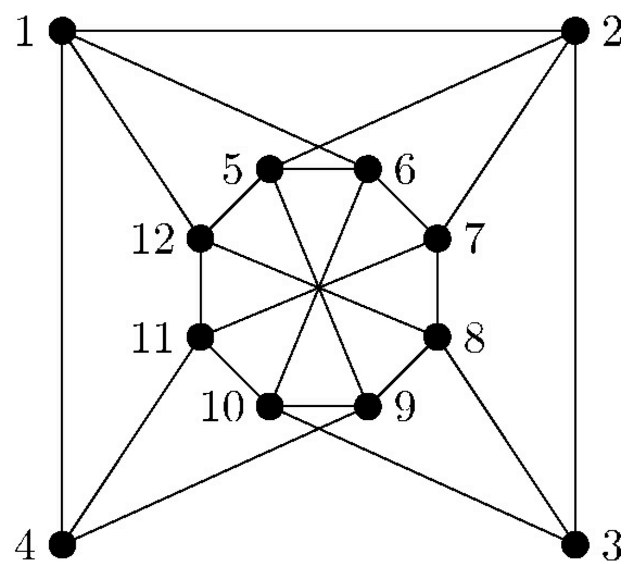
$$I_{G,k} = \langle x_1^2 - 1,\ x_2^2 - 1,\ x_3^2 - 1,\ x_1 + x_2,\ x_2 + x_3,\ x_1 + x_3 \rangle = \langle 1 \rangle$$

$$2x_1^2 = (x_1 - x_2)(x_1 + x_2) + (x_2 - x_3)(x_2 + x_3) + (x_1 - x_3)(x_1 + x_3)$$

Computer Proof

This leads to the following concrete application:

Theorem: There is an algorithm to decide *k*-colorability (and find the coloring) that is significatly better than pure search.



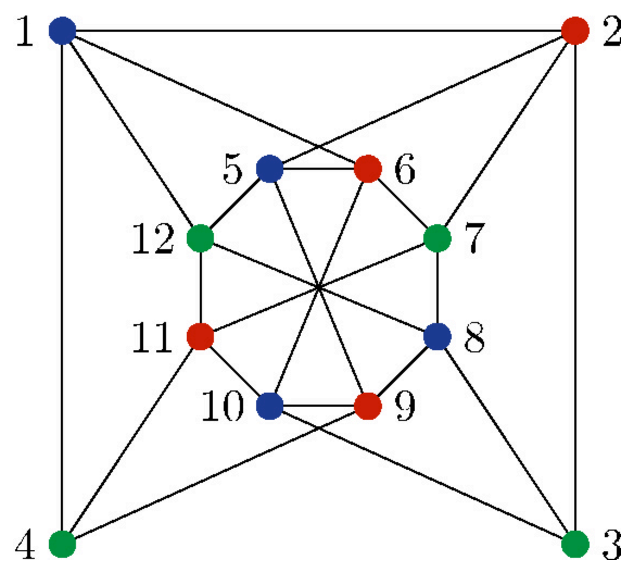
3-colorable?

Uniquely 3-colorable?

Computer Proof

This leads to the following concrete application:

Theorem: There is an algorithm to decide k-colorability (and find the coloring) that is significatly better than pure search.



3-colorable?

Uniquely 3-colorable?

Computer Proof

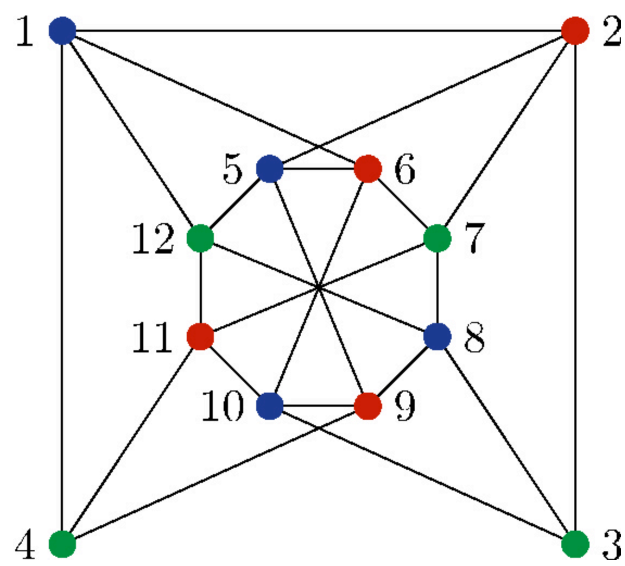
This leads to the following concrete application:

Theorem: There is an algorithm to decide k-colorability (and find the coloring) that is significatly better than pure search.

3-colorable?

Uniquely 3-colorable?

Y e s !



Integer Programming

Gröbner Bases: Transforms integer programming feasible sol'n using local moves into global optimum.

Minimize P+N+D+Q

Subject to P,N,D,Q $\geq$ 0 and P+5N+10D+25Q = 117

Integer solution: (P,N,D,Q) = (2,1,1,4)

Represent a collection C of coins by a polynomial $h = p^a n^b d^c q^d$ in p,n,d,q. (eg, 2 pennies, 4 dimes is $p^2 d^4$)

Input set $F = \{p^5-n,\ p^{10}-d,\ p^{25}-q\}$

Output set $G = \{p^5-n,\ n^2-d,\ d^2n-q,\ d^3-nq\}$

- Expresses a more useful set of replacement rules. Eg, the expression d^3-nq translates to: replace 3 dimes with a nickel and a quarter

Integer Programming

Given a collection C of coins, we use rules encoded by G to transform (in any order) C into a set of coins C' with equal monetary value but smaller number of elements.

Example (solving previous integer program):

$$p^{17}n^{10}d^5 \;\to\; p^{12}n^{11}d^5 \;\to \cdots \to\; p^2n^{13}d^5 \;\to$$
$$p^2n^{12}d^3q \;\to\; p^2n^{13}dq^2 \;\to \cdots \to\; p^2ndq^4$$

Computing $nf_G(h)$ with $G = \{p^5-n, n^2-d, d^2n-q, d^3-nq\}$

Great Reference: Cox, Little, O'Shea, *Ideals Varieties and Algorithms.*

The End

(of talk)