An introduction to computational complexity in algebraic geometry

Lily Silverstein

Cal Poly Pomona

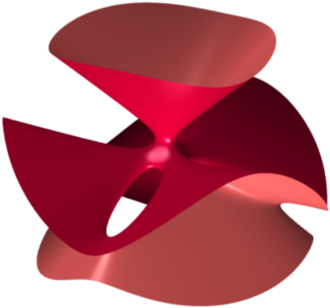
November 13, 2019

$$\begin{Bmatrix} x^5 + y^4 + z^3 = 1 \\ x^3 + y^3 + z^2 = 1 \end{Bmatrix}$$

$$\begin{Bmatrix} xy^3 + 3xyz - 5x - 2 = 0 \\ xy + 13z^9 - y^3 z + 18x = 0 \\ 17x^2 - 18y^2 + 5z^3 = 0 \end{Bmatrix}$$

$$\begin{Bmatrix} 3x + 7y - 5z - 35 = 0 \\ x^2 + y^2 + z^2 - 81 = 0 \end{Bmatrix}$$

multivariable
polynomial systems



algebraic varieties

Polynomial rings and ideals

$R = K[x_1, \ldots, x_n]$, a polynomial ring over some field K.

Ex. $R = \mathbb{Q}[x, y]$, polynomials in x and y with rational coefficients.

$I = \langle f_1, \ldots, f_k \rangle \subseteq R$, the ideal generated by $f_1, \ldots, f_k \in R$.

$I = \langle f_1, \ldots, f_k \rangle = \{a_1 f_1 + a_2 f_2 + \cdots + a_n f_n : a_i \in R\}$

"R-linear combinations of the f_i" or "linear combinations of the f_i with polynomial coefficients"

Ex. $I = \left\langle x^2 - y^3, xy^2 + x \right\rangle = \left\{ a(x^2 - y^3) + b(xy^2 + x) : a, b \in \mathbb{Q}[x, y] \right\}$

Corresponds to the system $\begin{Bmatrix} x^2 - y^3 = 0 \\ xy^2 + x = 0 \end{Bmatrix}$

Are the following two ideals equal?

$$\langle x^2 - y^3, xy^2 + x \rangle \qquad \text{and} \qquad \langle x^2 - y^3, xy^2 + x, x^5 + x \rangle$$

In other words, are the following two polynomial systems equivalent?

$$\begin{Bmatrix} x^2 - y^3 = 0 \\ xy^2 + x = 0 \end{Bmatrix} \qquad \text{and} \qquad \begin{Bmatrix} x^2 - y^3 = 0 \\ xy^2 + x = 0 \\ x^5 + x = 0 \end{Bmatrix}$$

Put a third way: is $x^5 + x \in \langle x^2 - y^3, xy^2 + x \rangle$?

Are the following two ideals equal?

$$\langle x^2 - y^3, xy^2 + x \rangle \qquad \text{and} \qquad \langle x^2 - y^3, xy^2 + x, x^5 + x \rangle$$

In other words, are the following two polynomial systems equivalent?

$$\left\{ \begin{aligned} x^2 - y^3 &= 0 \\ xy^2 + x &= 0 \end{aligned} \right\} \qquad \text{and} \qquad \left\{ \begin{aligned} x^2 - y^3 &= 0 \\ xy^2 + x &= 0 \\ x^5 + x &= 0 \end{aligned} \right\}$$

Put a third way: is $x^5 + x \in \langle x^2 - y^3, xy^2 + x \rangle$?

Today's talk: this problem is surprisingly hard!!

Definition.

A **decision problem** in computer science is a class of instances, or specific inputs, on which a true-or-false statement can be evaluated.

For example, the **subset sum problem**: given a set of integers, is there a subset of them which sums to zero?

A particular instance of this problem is:
Is there a subset of $\{1, -3, 8, -2, 4, -13, 5\}$ *that sums to zero?*

An **algorithm** for a decision problem is not the same thing as the problem itself.

For example, the “brute force” algorithm for the subset sum problem: iterate over every possible subset, sums the elements of the subset, and check if the sum is zero.

There are several ways to evaluate how efficient/practical an algorithm is, including

- **time complexity**: how much time does it take (how many steps or operations are required)
- **space complexity**: how much memory is used?

Both kinds of complexity are thought of as **functions of the input size**, and we usually focus on finding an upper bound for the **worst case**.

For example, let's evaluate the time complexity of the brute force algorithm for subset sum.

- Input size: n, the number of integers in the set.
- There are 2^n subsets of a set of n elements.
- In the worst case, we check all 2^n subsets.
- For each subset, we have to add at most n numbers.
- Total: no more than $n2^n$ additions
- Complexity of this algorithm is $\mathcal{O}(n2^n)$ ("grows no faster than a constant times $n2^n$")
- This is an *exponential-time* algorithm

For example, let's evaluate the time complexity of the brute force algorithm for subset sum.

- Input size: n, the number of integers in the set.
- There are 2^n subsets of a set of n elements.
- In the worst case, we check all 2^n subsets.
- For each subset, we have to add at most n numbers.
- Total: no more than $n2^n$ additions
- Complexity of this algorithm is $\mathcal{O}(n2^n)$ ("grows no faster than a constant times $n2^n$")
- This is an *exponential-time* algorithm

As a general principle, exponential-time/exponential-space algorithms are bad (impractical, don't work on large instances) while polynomial-time/polynomial-space algorithms are good.

Examples of polynomial complexity: $\mathcal{O}(n)$, $\mathcal{O}(n^2)$, $\mathcal{O}(n \log n)$.

Audience challenge: come up with a polynomial-time algorithm for the subset sum problem.

Reward: $1,000,000

Audience challenge: come up with a polynomial-time algorithm for the subset sum problem.

Reward: $1,000,000

Alternative audience challenge: prove there is no polynomial-time algorithm for the subset sum problem.

Reward: $1,000,000

P=NP?

P = class of all decision problems that admit a polynomial-time (in the input size) algorithm.

NP = class of all decision problems for which a *proposed* solution can be *verified* in polynomial time.

Example: subset sum problem is in **NP**. We don't know if it's in **P**.

Millennium Prize problem: is **P**$=$**NP**?
• **P**$\subseteq$**NP**.
• Most computer scientists "believe" that **P**$\neq$**NP**.
• To prove **P**$\neq$**NP**, just need to prove that some particular problem in **NP**, like subset sum, cannot have a polynomial-time algorithm.
• To prove **P**$=$**NP**, just need to find a polynomial-time algorithm for any of dozens of **NP**-complete problem.

P = class of all decision problems that admit a polynomial-time (in the input size) algorithm.

NP = class of all decision problems for which a *proposed* solution can be *verified* in polynomial time.

EXPTIME = class of all decision problems which have an exponential-time algorithm

EXPSPACE = class of all decision problems which have an exponential-space algorithm

P$\subseteq$**NP**$\subsetneq$ **EXPTIME**$\subseteq$**EXPSPACE**

The ideal membership problem

Instance

$R = \mathbb{Q}[x, y]$, polynomials in x and y with rational coefficients.

$I = \langle x^2 - y^3, xy^2 + x \rangle = \{a(x^2 - y^3) + b(xy^2 + x) : a, b \in R\}$

Is $x^5 + x$ an element of I?

General decision problem

$R = K[x_1, \ldots, x_n]$, a polynomial ring over some field K.

$I = \langle f_1, \ldots, f_k \rangle \subseteq R$, the ideal generated by $f_1, \ldots, f_k \in R$.

Given $f \in R$, does $f \in I$?

Let S be the subspace of $\mathbb{R}^3$ spanned by $\begin{bmatrix} 3 \\ -2 \\ 4 \end{bmatrix}$ and $\begin{bmatrix} 6 \\ 2 \\ -1 \end{bmatrix}$.

Is $\begin{bmatrix} -3 \\ -10 \\ 14 \end{bmatrix}$ an element of S?

Let S be the subspace of $\mathbb{R}^3$ spanned by $\begin{bmatrix} 3 \\ -2 \\ 4 \end{bmatrix}$ and $\begin{bmatrix} 6 \\ 2 \\ -1 \end{bmatrix}$.

Is $\begin{bmatrix} -3 \\ -10 \\ 14 \end{bmatrix}$ an element of S?

Gaussian elimination algorithm:

$$\left[\begin{array}{cc|c} 3 & 6 & -3 \\ -2 & 2 & -10 \\ 4 & -1 & 14 \end{array}\right] \to \left[\begin{array}{cc|c} 1 & 2 & -1 \\ -2 & 2 & -10 \\ 4 & -1 & 14 \end{array}\right] \to \left[\begin{array}{cc|c} 1 & 2 & -1 \\ 0 & 6 & -12 \\ 4 & -1 & 14 \end{array}\right]$$

$$\to \left[\begin{array}{cc|c} 1 & 2 & -1 \\ 0 & 6 & -12 \\ 0 & -9 & 18 \end{array}\right] \to \left[\begin{array}{cc|c} 1 & 2 & -1 \\ 0 & 1 & -2 \\ 0 & -9 & 18 \end{array}\right] \to \left[\begin{array}{cc|c} 1 & 0 & -3 \\ 0 & 1 & -2 \\ 0 & -9 & 18 \end{array}\right] \to \left[\begin{array}{cc|c} 1 & 0 & 3 \\ 0 & 1 & -2 \\ 0 & 0 & 0 \end{array}\right]$$

Let S be the subspace of $\mathbb{R}^3$ spanned by $\begin{bmatrix} 3 \\ -2 \\ 4 \end{bmatrix}$ and $\begin{bmatrix} 6 \\ 2 \\ -1 \end{bmatrix}$.

Is $\begin{bmatrix} -3 \\ -10 \\ 14 \end{bmatrix}$ an element of S?

Gaussian elimination algorithm:

$$\left[\begin{array}{rr|r} 3 & 6 & -3 \\ -2 & 2 & -10 \\ 4 & -1 & 14 \end{array}\right] \to \left[\begin{array}{rr|r} 1 & 0 & 3 \\ 0 & 1 & -2 \\ 0 & 0 & 0 \end{array}\right]$$

Let S be the subspace of $\mathbb{R}^3$ spanned by $\begin{bmatrix} 3 \\ -2 \\ 4 \end{bmatrix}$ and $\begin{bmatrix} 6 \\ 2 \\ -1 \end{bmatrix}$.

Is $\begin{bmatrix} -3 \\ -10 \\ 14 \end{bmatrix}$ an element of S?

Gaussian elimination algorithm:

$$\left[\begin{array}{cc|c} 3 & 6 & -3 \\ -2 & 2 & -10 \\ 4 & -1 & 14 \end{array}\right] \to \left[\begin{array}{cc|c} 1 & 0 & 3 \\ 0 & 1 & -2 \\ 0 & 0 & 0 \end{array}\right]$$

Yes, $\begin{bmatrix} -3 \\ -10 \\ 14 \end{bmatrix} \in S$, because $\begin{bmatrix} -3 \\ -10 \\ 14 \end{bmatrix} = 3 \begin{bmatrix} 3 \\ -2 \\ 4 \end{bmatrix} + (-2) \begin{bmatrix} 6 \\ 2 \\ -1 \end{bmatrix}$.

Complexity of Gaussian elimination

$$\left[\begin{array}{cc|c} 3 & 6 & -3 \\ -2 & 2 & -10 \\ 4 & -1 & 14 \end{array}\right] \to \left[\begin{array}{cc|c} 1 & 2 & -1 \\ -2 & 2 & -10 \\ 4 & -1 & 14 \end{array}\right] \to \left[\begin{array}{cc|c} 1 & 2 & -1 \\ 0 & 6 & -12 \\ 4 & -1 & 14 \end{array}\right]$$

$$\to \left[\begin{array}{cc|c} 1 & 2 & -1 \\ 0 & 6 & -12 \\ 0 & -9 & 18 \end{array}\right] \to \left[\begin{array}{cc|c} 1 & 2 & -1 \\ 0 & 1 & -2 \\ 0 & -9 & 18 \end{array}\right] \to \left[\begin{array}{cc|c} 1 & 0 & -3 \\ 0 & 1 & -2 \\ 0 & -9 & 18 \end{array}\right] \to \left[\begin{array}{cc|c} 1 & 0 & 3 \\ 0 & 1 & -2 \\ 0 & 0 & 0 \end{array}\right]$$

Input: m vectors in $\mathbb{R}^n$.

- m=number of columns
- n=number of rows
- Each time we reduce/normalize a row, we do m multiplications
- Each time we add a multiple of one row to another, we do m multiplications and m additions
- For each of the n rows, we normalize at most once, and then add a multiple of that row to at most $n-1$ other rows

Total: at most $n(m+(n-1)2m)$ operations

Complexity of Gaussian elimination

So we found that if the input is m vectors in $\mathbb{R}^n$, this algorithm takes at most $n(m + (n-1)2m) = 2n^2m - nm$ operations.

Time complexity of this Gaussian elimination algorithm is $\mathcal{O}\left(n^2m\right)$.

(grows no faster than a constant times n^2m)

Corollary: For n vectors in $\mathbb{R}^n$, the time complexity of Gaussian elimination is $\mathcal{O}\left(n^3\right)$.

The "subspace membership problem" is in **P**.

Consider the ideal $I = \langle x^2 + x - 2 \rangle$ in the ring $\mathbb{Q}[x]$.
Is $x^3 + 3x^2 + 5x + 4$ an element of I?

Consider the ideal $I = \langle x^2 + x - 2 \rangle$ in the ring $\mathbb{Q}[x]$.
Is $x^3 + 3x^2 + 5x + 4$ an element of I?

Algorithm: polynomial long division.

$$
\begin{array}{rrrrrrrrrrrrrr}
 & & & & & & x & + & 2 & & & & & \\
\cline{6-13}
x^2 & + & x & - & 2 & \big| & x^3 & + & 3x^2 & + & 5x & + & 4 \\
 & & & & & - & (x^3 & + & x^2 & - & 2x) & & \\
\cline{6-11}
 & & & & & & & & 2x^2 & + & 7x & + & 4 \\
 & & & & & & & - & (2x^2 & + & 2x & - & 4) \\
\cline{8-13}
 & & & & & & & & & & 5x & + & 8
\end{array}
$$

Consider the ideal $I = \langle x^2 + x - 2 \rangle$ in the ring $\mathbb{Q}[x]$.
Is $x^3 + 3x^2 + 5x + 4$ an element of I?

Algorithm: polynomial long division.

$$
\begin{array}{rrrrrrr|rrrrrrrrr}
 & & & & & & & & x & + & 2 & & & & & \\
\cline{8-16}
x^2 & + & x & - & 2 & & & & x^3 & + & 3x^2 & + & 5x & + & 4 \\
 & & & & & & & - & (x^3 & + & x^2 & - & 2x) & & \\
\cline{8-13}
 & & & & & & & & & & 2x^2 & + & 7x & + & 4 \\
 & & & & & & & & & - & (2x^2 & + & 2x & - & 4) \\
\cline{10-16}
 & & & & & & & & & & & & 5x & + & 8
\end{array}
$$

$$x^3 + 3x^2 + 5x + 4 \quad = \quad (x+2)(x^2 + x - 2) + (5x + 8)$$

Consider the ideal $I = \langle x^2 + x - 2 \rangle$ in the ring $\mathbb{Q}[x]$.
Is $x^3 + 3x^2 + 5x + 4$ an element of I?

Algorithm: polynomial long division.

$$
\begin{array}{r|rrrrrrrr}
 & & x & + & 2 & & & & \\
\hline
x^2 + x - 2 & & x^3 & + & 3x^2 & + & 5x & + & 4 \\
 & - & (x^3 & + & x^2 & - & 2x) & & \\
\cline{2-7}
 & & & & 2x^2 & + & 7x & + & 4 \\
 & & & - & (2x^2 & + & 2x & - & 4) \\
\cline{4-9}
 & & & & & & 5x & + & 8
\end{array}
$$

$$x^3 + 3x^2 + 5x + 4 \quad = \quad (x+2)(x^2+x-2) + (5x+8)$$

$$\implies \quad x^3 + 3x^2 + 5x + 4 \quad \notin \quad \langle x^2 + x - 2 \rangle$$

Complexity of this algorithm?

In this case, it makes sense to think of the input size as the **degree**.

$$
\begin{array}{rrrrrr|rrrrrrrrr}
 & & & & & & & & x & + & 1 & & & & \\
\cline{7-15}
x^2 & + & x & - & 2 & & & & x^3 & + & 3x^2 & + & 5x & + & 4 \\
 & & & & & & & - & (x^3 & + & x^2 & - & 2x) & & \\
\cline{8-13}
 & & & & & & & & & & 2x^2 & + & 7x & + & 4 \\
 & & & & & & & & & - & (2x^2 & + & 2x & - & 4) \\
\cline{10-15}
 & & & & & & & & & & & & 5x & + & 8
\end{array}
$$

Complexity of this algorithm?

In this case, it makes sense to think of the input size as the **degree**.

$$
\begin{array}{r|rrrrrrrr}
 & & x & + & 1 & & & & \\
\cline{2-9}
x^2 + x - 2 & & x^3 & + & 3x^2 & + & 5x & + & 4 \\
 & - & (x^3 & + & x^2 & - & 2x) & & \\
\cline{2-7}
 & & & & 2x^2 & + & 7x & + & 4 \\
 & & & - & (2x^2 & + & 2x & - & 4) \\
\cline{4-9}
 & & & & & & 5x & + & 8
\end{array}
$$

Polynomial long division in one variable is in **P**.

Goal: generalize the division algorithm so it works with polynomials in multiple variables.

The essential features that make the division algorithm work are:

- always knowing what the leading term of a polynomial is
- every time we subtract to get rid of the leading term, we are left with a polynomial of strictly smaller degree
- this process has to terminate because degrees are well-ordered

Definition.

Let $x^\alpha = x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_n^{\alpha_n}$ denote an arbitrary monomial where α is the vector of exponents. A *monomial order* on $R = k[x_1, \ldots, x_n]$ is a relation $>$ on the monomials of R such that

1. $>$ is a total ordering
2. $>$ is a well-ordering
3. if $x^\alpha > x^\beta$ then $x^\gamma x^\alpha > x^\gamma x^\beta$ for any x^γ (i.e., $>$ respects multiplication).

Example.

Lexicographic (lex) order is defined by $\alpha > \beta$ if the leftmost nonzero component of $\alpha - \beta$ is positive. For example, with lex order on $\mathbb{R}[x, y, z]$, $x > y > z$, $xy > y^4$, and $xz > y^2$.

Divide $x^5 + x$ by the generators $x^2 - y^3$ and $xy^2 + x$.

$$
\begin{array}{ccc|cccccccccccc}
 & & & q_1 : & x^3 & - & xy & & & & & & & & \\
 & & & q_2 : & x^2y & - & y^2 & + & 1 & & & & & & \\
\hline
x^2 & - & y^3 & & & & & & & & & & & & \\
xy^2 & + & x & & x^5 & + & x & & & & & & & & \\
 & & & - & (x^5 & - & x^3y^3) & & & & & & & & \\
 & & & & & & x^3y^3 & + & x & & & & & & \\
 & & & & & - & (x^3y^3 & + & x^3y) & & & & & & \\
 & & & & & & & & -x^3y & + & x & & & & \\
 & & & & & & & - & (-x^3y & + & xy^4) & & & & \\
 & & & & & & & & & & -xy^4 & + & x & & \\
 & & & & & & & & & - & (-xy^4 & - & xy^2) & & \\
 & & & & & & & & & & & & xy^2 & + & x \\
 & & & & & & & & & & & - & (xy^2 & + & x) \\
 & & & & & & & & & & & & & & 0
\end{array}
$$

Divide $x^5 + x$ by the generators $x^2 - y^3$ and $xy^2 + x$.

$$
\begin{array}{r|cccccccccccc}
 & & q_1: x^3 & - & xy & & & & & & & & \\
 & & q_2: x^2y & - & y^2 & + & 1 & & & & & & \\
\hline
x^2 - y^3 & & & & & & & & & & & & \\
xy^2 + x & & x^5 & + & x & & & & & & & & \\
 & - & (x^5 & - & x^3y^3) & & & & & & & & \\
\cline{2-7}
 & & & & x^3y^3 & + & x & & & & & & \\
 & & & - & (x^3y^3 & + & x^3y) & & & & & & \\
\cline{4-9}
 & & & & & & -x^3y & + & x & & & & \\
 & & & & & - & (-x^3y & + & xy^4) & & & & \\
\cline{6-10}
 & & & & & & & & -xy^4 & + & x & & \\
 & & & & & & & - & (-xy^4 & - & xy^2) & & \\
\cline{8-13}
 & & & & & & & & & & xy^2 & + & x \\
 & & & & & & & & & - & (xy^2 & + & x) \\
\cline{10-13}
 & & & & & & & & & & & & 0
\end{array}
$$

$$x^5 + x \quad = \quad (x^3 - xy)(x^2 - y^3) + (x^2y - y^2 + 1)(xy^2 + x)$$

Divide $x^5 + x$ by the generators $x^2 - y^3$ and $xy^2 + x$.

$$
\begin{array}{ccc|cccccccccccc}
 & & & q_1: & x^3 & - & xy & & & & & & & & \\
 & & & q_2: & x^2y & - & y^2 & + & 1 & & & & & & \\
\hline
x^2 & - & y^3 & & & & & & & & & & & & \\
xy^2 & + & x & & x^5 & + & x & & & & & & & & \\
 & & & - & (x^5 & - & x^3y^3) & & & & & & & & \\
\cline{4-9}
 & & & & & & x^3y^3 & + & x & & & & & & \\
 & & & & & - & (x^3y^3 & + & x^3y) & & & & & & \\
\cline{6-11}
 & & & & & & & & -x^3y & + & x & & & & \\
 & & & & & & & - & (-x^3y & + & xy^4) & & & & \\
\cline{8-13}
 & & & & & & & & & & -xy^4 & + & x & & \\
 & & & & & & & & & - & (-xy^4 & - & xy^2) & & \\
\cline{10-15}
 & & & & & & & & & & & & xy^2 & + & x \\
 & & & & & & & & & & & - & (xy^2 & + & x) \\
\cline{12-15}
 & & & & & & & & & & & & & & 0
\end{array}
$$

$$x^5 + x = (x^3 - xy)(x^2 - y^3) + (x^2y - y^2 + 1)(xy^2 + x)$$

$$\implies \quad x^5 + x \in \langle x^2 - y^3, xy^2 + x \rangle$$

Definition.

When F is a set of polynomials and dividing h by the $f_i \in F$ using the division algorithm leads to the remainder r, we write $h^F \to r$ and say h reduces to r.

Definition.

When F is a set of polynomials and dividing h by the $f_i \in F$ using the division algorithm leads to the remainder r, we write $h^F \to r$ and say h reduces to r.

Lemma.

If $h^F \to 0$ then h is in the ideal generated by F.

Definition.

When F is a set of polynomials and dividing h by the $f_i \in F$ using the division algorithm leads to the remainder r, we write $h^F \rightarrow r$ and say h reduces to r.

Lemma.

If $h^F \rightarrow 0$ then h is in the ideal generated by F.

Unfortunately, the converse is false.

Using the same ideal $I = \langle x^2 - y^3, xy^2 + x \rangle$, note that $(-y^2 - 1)(x^2 - y^3) + x(xy^2 + x) = y^5 + y^3$, so $y^5 + y^3 \in I$. However, long division produces the nonzero remainder $y^5 + y^3$.

Definition

After fixing a monomial order, every multivariate polynomial f has a well-defined leading term, $\text{LT}_>(f)$.
For an ideal I, we define $\text{LT}_>(I) = \langle \text{LT}_>(f) : f \in I \rangle$, the ideal generated by all leading terms of polynomials in I.

Definition

Given a monomial order, a *Gröbner basis* G of a nonzero ideal I is a subset $\{g_1, g_2, \ldots, g_s\} \subseteq I$ such that either of the following equivalent conditions hold:

(i) $f^G \to 0 \iff f \in I$

(ii) $\langle \text{LT}_>(g_1), \text{LT}_>(g_2), \ldots, \text{LT}_>(g_s) \rangle = \text{LT}_>(I)$

So to solve the ideal membership problem, we first need a Gröbner basis for our ideal.

- Good news: a finite Gröbner basis always exists.
- More good news: Buchberger's algorithm is guaranteed to correctly compute a Gröbner basis in finite time.

So to solve the ideal membership problem, we first need a Gröbner basis for our ideal.

- Good news: a finite Gröbner basis always exists.
- More good news: Buchberger's algorithm is guaranteed to correctly compute a Gröbner basis in finite time.

- Bad news: a finite Gröbner basis can be very, very large.
- More bad news: "finite time" can be a very, very long time!

So to solve the ideal membership problem, we first need a Gröbner basis for our ideal.

- Good news: a finite Gröbner basis always exists.
- More good news: Buchberger's algorithm is guaranteed to correctly compute a Gröbner basis in finite time.

- Bad news: a finite Gröbner basis can be very, very large.
- More bad news: "finite time" can be a very, very long time!

Let's see a small example. Let $R = \mathbb{Q}[x, y, z]$, using lex order, and let $I = \langle x^5 + y^4 + z^3 - 1, x^3 + y^3 + z^2 - 1 \rangle$.

The (reduced) Gröbner basis of I has 8 polynomials. One of these 8 polynomials is on the next slide.

$69984xyz^2 - 139968xyz + 69984xy - 44425xz^{20} - 327070xz^{19} - 1278214xz^{18} - 2698855xz^{17} - 2572042xz^{16} + 2619449xz^{15} +$
$10650408xz^{14} + 11493837xz^{13} - 2616810xz^{12} - 16744470xz^{11} - 12049440xz^{10} + 4801407xz^9 + 8854766xz^8 + 1892306xz^7 -$
$1980847xz^6 + 17496xz^5 - 34992xz^4 + 17496xz^3 - 69984xz^2 + 139968xz - 69984x - 44425y^{14}z^{11} + 339305y^{14}z^{10} +$
$1628711y^{14}z^9 + 3000105y^{14}z^8 + 2743338y^{14}z^7 + 437586y^{14}z^6 - 3228714y^{14}z^5 - 6067476y^{14}z^4 - 5393667y^{14}z^3 -$
$1569800y^{14}z^2 + 632812y^{14}z + 501226y^{14} + 444250y^{13}z^{11} + 1671400y^{13}z^{10} + 3140020y^{13}z^9 + 4046756y^{13}z^8 + 3960482y^{13}z^7 +$
$1782242y^{13}z^6 - 2836264y^{13}z^5 - 6324094y^{13}z^4 - 5404156y^{13}z^3 - 1661654y^{13}z^2 + 685300y^{13}z + 474982y^{13} +$
$266550y^{12}z^{12} + 718520y^{12}z^{11} + 910274y^{12}z^{10} + 1263518y^{12}z^9 + 3116408y^{12}z^8 + 5071808y^{12}z^7 + 3440132y^{12}z^6 -$
$2194496y^{12}z^5 - 6620078y^{12}z^4 - 5499938y^{12}z^3 - 1622288y^{12}z^2 + 632812y^{12}z + 501226y^{12} - 88850y^{11}z^{13} + 1744810y^{11}z^{12} +$
$7686377y^{11}z^{11} + 11626231y^{11}z^{10} + 4404103y^{11}z^9 - 11359143y^{11}z^8 - 25510554y^{11}z^7 - 28425462y^{11}z^6 - 9426528y^{11}z^5 +$
$21880364y^{11}z^4 + 29810057y^{11}z^3 + 10350756y^{11}z^2 - 3181556y^{11}z - 2497382y^{11} + 44425y^{10}z^{14} + 1881945y^{10}z^{13} +$
$6728289y^{10}z^{12} + 9990070y^{10}z^{11} + 7801347y^{10}z^{10} + 2153415y^{10}z^9 - 9140507y^{10}z^8 - 29133398y^{10}z^7 - 36482669y^{10}z^6 -$
$11662110y^{10}z^5 + 22936006y^{10}z^4 + 29956543y^{10}z^3 + 10775034y^{10}z^2 - 3478988y^{10}z - 2348666y^{10} + 888500y^9z^{14} +$
$1921200y^9z^{13} - 187950y^9z^{12} - 1596036y^9z^{11} + 7831314y^9z^{10} + 19135710y^9z^9 + 5385232y^9z^8 - 31118752y^9z^7 -$
$46554784y^9z^6 - 15507324y^9z^5 + 24599634y^9z^4 + 30284550y^9z^3 + 10578204y^9z^2 - 3111572y^9z - 2532374y^9 - 44425y^8z^{15} +$
$2915955y^8z^{14} + 11847046y^8z^{13} + 15235952y^8z^{12} - 1342215y^8z^{11} - 26096155y^8z^{10} - 40336258y^8z^9 - 38148698y^8z^8 -$
$1947773y^8z^7 + 58365386y^8z^6 + 63744949y^8z^5 + 662692y^8z^4 - 35221464y^8z^3 - 15349894y^8z^2 + 3269036y^8z + 2453642y^8 +$
$88850y^7z^{16} + 2697690y^7z^{15} + 9160898y^7z^{14} + 9782204y^7z^{13} - 505866y^7z^{12} - 8841150y^7z^{11} - 16474014y^7z^{10} -$
$39769140y^7z^9 - 41664378y^7z^8 + 21330064y^7z^7 + 86946000y^7z^6 + 61819454y^7z^5 - 20296984y^7z^4 - 53124800y^7z^3 -$
$20474824y^7z^2 + 5569880y^7z + 3756116y^7 - 44425y^6z^{17} + 783555y^6z^{16} + 456911y^6z^{15} - 7506655y^6z^{14} - 12668822y^6z^{13} +$
$10778914y^6z^{12} + 40955979y^6z^{11} + 11243399y^6z^{10} - 68036522y^6z^9 - 80668677y^6z^8 + 18392944y^6z^7 + 105699982y^6z^6 +$
$68420946y^6z^5 - 23355948y^6z^4 - 52987825y^6z^3 - 20457328y^6z^2 + 4905032y^6z + 4088540y^6 + 1954700y^5z^{16} +$
$7105380y^5z^{15} + 5800536y^5z^{14} - 10997536y^5z^{13} - 25975004y^5z^{12} - 24957052y^5z^{11} - 17808216y^5z^{10} + 12529572y^5z^9 +$
$73310048y^5z^8 + 73580532y^5z^7 - 21170564y^5z^6 - 74140892y^5z^5 - 25675184y^5z^4 + 18268092y^5z^3 + 10504900y^5z^2 -$
$1388096y^5z - 941216y^5 + 44425y^4z^{18} + 1526545y^4z^{17} + 4467129y^4z^{16} + 2647468y^4z^{15} - 3245086y^4z^{14} + 1090138y^4z^{13} +$
$899768y^4z^{12} - 36144372y^4z^{11} - 61462426y^4z^{10} + 7525711y^4z^9 + 103064435y^4z^8 + 82980083y^4z^7 - 28598633y^4z^6 -$
$75995106y^4z^5 - 25336908y^4z^4 + 18247517y^4z^3 + 10793584y^4z^2 - 1738016y^4z - 766256y^4 - 88850y^3z^{19} - 32190y^3z^{18} -$
$1842423y^3z^{17} - 9605029y^3z^{16} - 10602997y^3z^{15} + 20587543y^3z^{14} + 54430174y^3z^{13} + 13274582y^3z^{12} - 82735585y^3z^{11} -$
$89174777y^3z^{10} + 37559804y^3z^9 + 127272309y^3z^8 + 49867042y^3z^7 - 74430398y^3z^6 - 79475920y^3z^5 - 1372204y^3z^4 +$
$36291181y^3z^3 + 15564220y^3z^2 - 2796644y^3z - 2689838y^3 + 444250y^2z^{18} + 1227150y^2z^{17} - 752630y^2z^{16} -$
$7006014y^2z^{15} - 8783974y^2z^{14} - 1436450y^2z^{13} + 4950830y^2z^{12} + 13378064y^2z^{11} + 30957924y^2z^{10} + 21952328y^2z^9 -$
$30170622y^2z^8 - 52627432y^2z^7 - 9384858y^2z^6 + 26513908y^2z^5 + 15113990y^2z^4 - 2001554y^2z^3 - 2374910y^2z^2 +$
$266550yz^{19} + 451970yz^{18} - 1140996yz^{17} - 2972806yz^{16} + 1218640yz^{15} + 3837574yz^{14} - 11018460yz^{13} - 21334144yz^{12} +$
$12799086yz^{11} + 55234262yz^{10} + 29962348yz^9 - 39724286yz^8 - 56881602yz^7 - 8218528yz^6 + 26664768yz^5 + 15232088yz^4 -$
$2010302yz^3 - 2436146yz^2 + 139968yz - 69984y - 44425z^{21} - 193795z^{20} - 1274354z^{19} - 3527528z^{18} - 1109995z^{17} +$
$13565093z^{16} + 22302653z^{15} - 7954033z^{14} - 56030677z^{13} - 42908546z^{12} + 42041860z^{11} + 91874913z^{10} + 31327296z^9 -$
$57432520z^8 - 63266461z^7 - 5375344z^6 + 27268337z^5 + 14641598z^4 - 1214234z^3 - 2619854z^2 - 139968z + 69984$

Mayr and Meyer, 1982: The ideal membership problem is **EXPSPACE**-complete.

In particular, it is not in **P** and is not in **NP**.

Mayr and Meyer, 1982: The ideal membership problem is **EXPSPACE**-complete.

In particular, it is not in **P** and is not in **NP**.

Also Mayr-Meyer, 1982: The “degree complexity” of the ideal membership problem is double exponential in max(number of variables, degree of input polynomials).

Mayr and Meyer, 1982: The ideal membership problem is **EXPSPACE**-complete.

In particular, it is not in **P** and is not in **NP**.

Also Mayr-Meyer, 1982: The “degree complexity” of the ideal membership problem is double exponential in max(number of variables, degree of input polynomials).

Where do we go from here?

- Refine Gröbner basis algorithms
  - Faugère's F4 and F5 algorithms, FGLM
  - Specialized architecture for specific applications (e.g. Zuzana Kúkelová in computer vision)
  - Machine learning used to train a computer to pick S-pairs in an optimal way (Dylan Peifer and Mike Stillman)
- Beyond the worst case
  - Average case complexity of G.B. for polynomials with generic coefficients (Faugère et al)
  - Algorithms for polynomial systems with special combinatorial structure (e.g. Diego Cifuentes and Pablo Parrilo)
  - Probabilistic analysis of monomial ideals (Daniel Erman and Jay Yang, De Loera-Hoşten-Krone-Silverstein, De Loera-Petrović-Stasi-Silverstein-Wilburne, Silverstein-Yang-Wilburne)
- Ask different questions
  - e.g., find the dimension, projective dimension, regularity, Hilbert series, etc. of a variety rather than a complete description (all still **NP**-hard)
  - Machine learning used to train a computer to compute Hilbert series in an optimal way (De Loera-Krone-Silverstein-Zhao)

⋆ Huge acknowledgment to Dylan Peifer for letting me use a few of his slides (especially the long division ones!)

Definition

Let $S(f,g) = \frac{x^\gamma}{\mathrm{LT}_>(f)} f - \frac{x^\gamma}{\mathrm{LT}_>(g)} g$ where x^γ is the least common multiple of the leading terms of f and g. This is the S-polynomial of f and g, where S stands for syzygy.

Definition

Let $S(f,g) = \frac{x^\gamma}{\mathrm{LT}_>(f)} f - \frac{x^\gamma}{\mathrm{LT}_>(g)} g$ *where* x^γ *is the least common multiple of the leading terms of* f *and* g*. This is the* *S-polynomial* *of* f *and* g*, where S stands for syzygy.*

Example

$$\begin{aligned} S(x^2 - y^3, xy^2 + x) &= \frac{x^2y^2}{x^2}(x^2 - y^3) - \frac{x^2y^2}{xy^2}(xy^2 + x) \\ &= y^2(x^2 - y^3) - x(xy^2 + x) \\ &= -x^2 - y^5 \end{aligned}$$

Definition

Let $S(f,g) = \frac{x^\gamma}{\mathrm{LT}_>(f)} f - \frac{x^\gamma}{\mathrm{LT}_>(g)} g$ where x^γ is the least common multiple of the leading terms of f and g. This is the S-polynomial of f and g, where S stands for syzygy.

Example

$$\begin{aligned} S(x^2 - y^3, xy^2 + x) &= \frac{x^2y^2}{x^2}(x^2 - y^3) - \frac{x^2y^2}{xy^2}(xy^2 + x) \\ &= y^2(x^2 - y^3) - x(xy^2 + x) \\ &= -x^2 - y^5 \end{aligned}$$

Theorem (Buchberger's Criterion)

Let $G = \{g_1, g_2, \ldots, g_s\}$ generate some ideal I. If $\overline{S(g_i, g_j)}^G \to 0$ for all pairs g_i, g_j then G is a Gröbner basis of I.

Algorithm 1 Buchberger's Algorithm

input a set of polynomials $\{f_1, \ldots, f_k\}$
output a Gröbner basis G of $I = \langle f_1, \ldots, f_k \rangle$
procedure BUCHBERGER($\{f_1, \ldots, f_k\}$)
    $G \leftarrow \{f_1, \ldots, f_k\}$ ▷ the current basis
    $P \leftarrow \{(f_i, f_j) \mid 1 \leq i < j \leq k\}$ ▷ the remaining pairs
    while $|P| > 0$ **do**
        $(f_i, f_j) \leftarrow \mathrm{select}(P)$
        $P \leftarrow P \setminus \{(f_i, f_j)\}$
        $r \leftarrow S(f_i, f_j)^G$
        if $r \neq 0$ **then**
            $P \leftarrow P \cup \{(f, r) : f \in G\}$
            $G \leftarrow G \cup \{r\}$
        end if
    end while
    return G
end procedure

Example

$I = \langle x^2 - y^3, xy^2 + x \rangle$

Example

$I = \langle x^2 - y^3, xy^2 + x \rangle$

initialize G to $\{x^2 - y^3, xy^2 + x\}$
initialize P to $\{(x^2 - y^3, xy^2 + x)\}$

Example

$I = \langle x^2 - y^3, xy^2 + x\rangle$

initialize G to $\{x^2 - y^3, xy^2 + x\}$
initialize P to $\{(x^2 - y^3, xy^2 + x)\}$

select $(x^2 - y^3, xy^2 + x)$ *and compute* $S(x^2 - y^3, xy^2 + x)^G \to -y^5 - y^3$
update G to $\{x^2 - y^3, xy^2 + x, -y^5 - y^3\}$
update P to $\{(x^2 - y^3, -y^5 - y^3), (xy^2 + x, -y^5 - y^3)\}$

Example

$I = \langle x^2 - y^3, xy^2 + x \rangle$

initialize G to $\{x^2 - y^3, xy^2 + x\}$
initialize P to $\{(x^2 - y^3, xy^2 + x)\}$

select $(x^2 - y^3, xy^2 + x)$ *and compute* $S(x^2 - y^3, xy^2 + x)^G \to -y^5 - y^3$
update G to $\{x^2 - y^3, xy^2 + x, -y^5 - y^3\}$
update P to $\{(x^2 - y^3, -y^5 - y^3), (xy^2 + x, -y^5 - y^3)\}$

select $(x^2 - y^3, -y^5 - y^3)$ *and compute* $S(x^2 - y^3, -y^5 - y^3)^G \to 0$

Example

$I = \langle x^2 - y^3, xy^2 + x \rangle$

initialize G to $\{x^2 - y^3, xy^2 + x\}$
initialize P to $\{(x^2 - y^3, xy^2 + x)\}$

select $(x^2 - y^3, xy^2 + x)$ *and compute* $S(x^2 - y^3, xy^2 + x)^G \rightarrow -y^5 - y^3$
update G to $\{x^2 - y^3, xy^2 + x, -y^5 - y^3\}$
update P to $\{(x^2 - y^3, -y^5 - y^3), (xy^2 + x, -y^5 - y^3)\}$

select $(x^2 - y^3, -y^5 - y^3)$ *and compute* $S(x^2 - y^3, -y^5 - y^3)^G \rightarrow 0$

select $(xy^2 + x, -y^5 - y^3)$ *and compute* $S(xy^2 + x, -y^5 - y^3)^G \rightarrow 0$

Example

$I = \langle x^2 - y^3, xy^2 + x \rangle$

initialize G to $\{x^2 - y^3, xy^2 + x\}$
initialize P to $\{(x^2 - y^3, xy^2 + x)\}$

select $(x^2 - y^3, xy^2 + x)$ *and compute* $S(x^2 - y^3, xy^2 + x)^G \to -y^5 - y^3$
update G to $\{x^2 - y^3, xy^2 + x, -y^5 - y^3\}$
update P to $\{(x^2 - y^3, -y^5 - y^3), (xy^2 + x, -y^5 - y^3)\}$

select $(x^2 - y^3, -y^5 - y^3)$ *and compute* $S(x^2 - y^3, -y^5 - y^3)^G \to 0$

select $(xy^2 + x, -y^5 - y^3)$ *and compute* $S(xy^2 + x, -y^5 - y^3)^G \to 0$

return $G = \{x^2 - y^3, xy^2 + x, -y^5 - y^3\}$