Gröbner bases algorithms

Third year research project: M3R

Raphaël Pellegrin
Professor Tom Coates, Doctor Giuseppe Pitton

Imperial College, London

July 25, 2019

Overview

Gröbner bases: motivation

Gröbner bases: history

Monomial orderings

The division algorithm in $k[x_1, \ldots, x_n]$

Buchberger's algorithm

Faugère's F4 algorithm

Signature based algorithms and Faugère's F5 algorithm

Gröbner bases: motivation

The algebra of the polynomial rings $k[x_1, \ldots, x_n]$ and the geometry of affine algebraic varieties are linked. Gröbner bases allow us to solve problems about polynomial ideals in an algorithmic fashion [1].

Gröbner bases: motivation

Problems concerning the algebra of polynomial ideals and the geometry of affine varieties:

- The ideal membership problem: given $f \in k[x_1, ..., x_n]$ and an ideal $I = \langle f_1, \ldots, f_s \rangle$, determine if $f \in I$. Closely related to determining whether $\mathbf{V}(f_1, \ldots, f_s)$ lies on the variety $\mathbf{V}(f)$.
- The problem of solving polynomial equations: find all common solutions in k^n of a system of polynomial equations $f_1(x_1, \ldots, x_n) = \cdots = f_s(x_1, \ldots, x_n) = 0$. This is the same as asking for the points in the affine variety $\mathbf{V}(f_1, \ldots, f_s)$.

Gröbner bases: history

Gröbner bases were developed by Bruno Buchberger in 1965 in his PhD. thesis. He developed this theory throughout his career. He named these objects after his advisor Wolfgang Gröbner [2].

Monomial orderings

We need a way to order monomials. For example, in dividing $f(x) = x^5 - 3x^2 + 1$ by $g(x) = x^2 - 4x + 7$ by the Euclidean algorithm, we:

- Write the terms in the polynomials in decreasing order by degree in x.
- The leading term in f is $x^5 = x^3 \cdot$ (leading term in g). Thus, subtract $x^3 g(x)$ from f to cancel the leading term.
- Repeat the same process on $f(x) - x^3 \cdot g(x)$, etc., until we obtain a polynomial of degree less than 2.

Monomial orderings

For the division algorithm on polynomials in one variable, we are dealing with the degree ordering on the one-variable monomials:

$$\cdots > x^{m+1} > x^m > \cdots > x^2 > x > 1$$

The success of the algorithm depends on working systematically with the leading terms in f and g, and not removing terms "at random" from f using arbitrary terms from g.

Monomial orderings

A major component of any extension of division to arbitrary polynomials in several variables will be an ordering on the terms in polynomials in $k[x_1, ..., x_n]$. There are different ways to define orderings on monomials (or equivalently $\mathbb{Z}^n_{\geq 0}$).

Monomial orderings

Definition

A total ordering satisfies:

- the ordering is a partial ordering (transitive, antisymmetric, reflexive)
- for every pair of monomials x^α and x^β , exactly one of the three statements $x^\alpha > x^\beta$, $x^\alpha = x^\beta$, $x^\beta > x^\alpha$ should be true

Monomial orderings

We must take into account the effect of the sum and product operations on polynomials.

Definition (Monomial ordering)

A monomial ordering $>$ on $k[x_1, \ldots, x_n]$ is a relation $>$ on the set of monomials x^α, $\alpha \in \mathbb{Z}^n_{\geq 0}$, satisfying:

- $>$ is a total (or linear) ordering on $\mathbb{Z}^n_{\geq 0}$.
- If $\alpha > \beta$ and $\gamma \in \mathbb{Z}^n_{\geq 0}$, then $\alpha + \gamma > \beta + \gamma$.
- $>$ is a well-ordering on $\mathbb{Z}^n_{\geq 0}$. This means that every nonempty subset of $\mathbb{Z}^n_{\geq 0}$ has a smallest element under $>$.

Monomial orderings

Definition (Lexicographic Order)

Let $\alpha = (\alpha_1, \ldots, \alpha_n)$ and $\beta = (\beta_1, \ldots, \beta_n)$ be in $\mathbb{Z}^n_{\geq 0}$. We say $\alpha >_{lex} \beta$ if the leftmost nonzero entry of the vector difference $\alpha - \beta \in \mathbb{Z}^n$ is positive. We will write $x^\alpha >_{lex} x^\beta$ if $\alpha >_{lex} \beta$. This is a monomial ordering.

Monomial orderings

Definition (Graded Lex Order)

Let $\alpha, \beta \in \mathbb{Z}^n_{\geq 0}$. We say $\alpha >_{grlex} \beta$ if $|\alpha| = \sum_{i=1}^n \alpha_i > |\beta| = \sum_{i=1}^n \beta_i$ or $|\alpha| = |\beta|$ and $\alpha >_{lex} \beta$. This is a monomial ordering.

We see that grlex orders by total degree first, then "break ties" using lex order.

Monomial orderings

Examples:

- $(3, 2, 4) >_{lex} (3, 2, 1)$ since $\alpha - \beta = (0, 0, 3)$.
- $(1, 2, 3) >_{grlex} (3, 2, 0)$ since $|(1, 2, 3)| = 6 > |(3, 2, 0)| = 5$.
- $(1, 2, 4) >_{grlex} (1, 1, 5)$ since $|(1, 2, 4)| = |(1, 1, 5)|$ and $(1, 2, 4) >_{lex} (1, 1, 5)$.

Monomial orderings

Definition

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:

$$multideg(f) = \max\{\alpha \in \mathbb{Z}^n_{\geq 0} : a_\alpha \neq 0\}$$

  (the maximum is taken with respect to $>$).
- The leading coefficient of f is $\mathrm{LC}(f) = a_{multideg(f)} \in k$.
- The leading monomial of f is $\mathrm{LM}(f) = x^{multideg(f)}$ (with coefficient 1).
- The leading term of f is: $\mathrm{LT}(f) = \mathrm{LC}(f)\,\mathrm{LM}(f)$.

Monomial orderings

To illustrate, let $f = 4xy^2z + 4z^2 - 5x^3 + 7x^2z^2$ as before and let $>$ denote lex order. Then $multideg(f) = (3, 0, 0)$, $\mathrm{LC}(f) = -5$, $LM(f) = x^3$, $\mathrm{LT}(f) = -5x^3$.

The division algorithm in $k[x_1, \ldots, x_n]$

The goal is to divide $f \in k[x_1, \ldots, x_n]$ by $f_1, \ldots, f_s \in k[x_1, \ldots, x_n]$. As we will see, this means expressing f in the form $f = q_1 f_1 + \cdots + q_s f_s + r$, where the "quotients" $q_1, \ldots, q_s$ and remainder r lie in $k[x_1, \ldots, x_n]$. This is where we will use the monomial orderings introduced previously.

The division algorithm in $k[x_1, \ldots, x_n]$

The basic idea of the algorithm is the same as in the one-variable case:

We want to cancel the leading term of f by multiplying some f_i by an appropriate monomial and subtracting.

Let us first work through some examples to see what is involved.

The division algorithm in $k[x_1, \ldots, x_n]$

Let us divide $f = x^2y + xy^2 + y^2$ by $f_1 = xy - 1$ and $f_2 = y^2 - 1$, using the lex order with $x > y$. The first two give us the following partially completed division:

$$\begin{array}{r|l} x^2y + xy^2 + y^2 & xy - 1, y^2 - 1 \\ \hline xy^2 + x + y^2 & x \\ x + y^2 + y & x + y \end{array}$$

The division algorithm in $k[x_1, \ldots, x_n]$

$$
\begin{array}{r|l}
x^2y + xy^2 + y^2 & \underline{xy - 1, y^2 - 1} \\
xy^2 + x + y^2 & x \\
x + y^2 + y & x + y
\end{array}
$$

Note that neither $\mathrm{LT}(f_1) = xy$ nor $\mathrm{LT}(f_2) = y^2$ divides $\mathrm{LT}(x + y^2 + y) = x$. However, $x + y^2 + y$ is not the remainder since $\mathrm{LT}(f_2)$ divides y^2.

The division algorithm in $k[x_1, \ldots, x_n]$

$$\begin{array}{r|l c}
x^2y + xy^2 + y^2 & xy - 1, y^2 - 1 & \text{remainder} \\
\hline
y^2 + y & x + y & x \\
y + 1 & x + y, 1 & x \\
0 & x + y, 1 & x + y + 1
\end{array}$$

Thus, the remainder is $x + y + 1$, and we obtain

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

The remainder is a sum of monomials, none of which is divisible by the leading terms $\mathrm{LT}(f_1)$ or $\mathrm{LT}(f_2)$.

The division algorithm in $k[x_1, \ldots, x_n]$

The division algorithm is not a perfect generalisation of its univariate version.

In fact, the algorithm achieves its full potential only when coupled with the Gröbner bases [2].

The division algorithm in $k[x_1, \ldots, x_n]$

Important property of the division algorithm in $k[x]$: the remainder is uniquely determined.

This can fail when there is more than one variable. Let us divide $f = x^2y + xy^2 + y^2$ by $f_1 = y^2 - 1$ and $f_2 = xy$–1. We will use lex order with $x > y$. This is the same as the previous example, except that we have changed the order of the divisors.

The division algorithm in $k[x_1, \ldots, x_n]$

The remainder is different from what we got previously.

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

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

The remainder is not uniquely characterised by the requirement that none of its terms be divisible by $\mathrm{LT}(f_1), \ldots, \mathrm{LT}(f_s)$.

The division algorithm in $k[x_1, \ldots, x_n]$

One nice feature of the division algorithm in $k[x]$ is the way it solves the ideal membership problem.

Do we get something similar in the multivariate case?

The division algorithm in $k[x_1, \ldots, x_n]$

Let $f_1 = y^2 - 1$, $f_2 = xy + 1 \in k[x, y]$ with the lexicographic order. Dividing $f = x^2y + 2xy^2 + y$ by $F = (f_1, f_2)$, the result is

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

With $F = (f_2, f_1)$, however, we have

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

However:

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

The third calculation shows that $f \in \langle f_1, f_2 \rangle$. However, it is still possible to obtain a nonzero remainder on division by $F = (f_1, f_2)$ and $F' = (f_2, f_1)$.

Gröbner bases

Definition (Monomial ideal)

An ideal $I \subseteq k[x_1, \ldots, x_n]$ is a monomial ideal if there is a subset $A \subseteq \mathbb{Z}^n_{\geq 0}$ (possibly infinite) such that I consists of all polynomials which are finite sums of the form $\sum_{\alpha \in A} h_\alpha x^\alpha$, where $h_\alpha \in k[x_1, \ldots, x_n]$.

In this case, we write $I = \langle x^\alpha : \alpha \in A \rangle$.

Gröbner bases

Theorem

Let $I = \langle x^\alpha : \alpha \in A \rangle$ be a monomial ideal. Then a monomial x^β lies in I if and only if x^β is divisible by x^α for some $\alpha \in A$.

Gröbner bases

Theorem (Dickson's Lemma)

Let $I = \langle x^\alpha : \alpha \in A \rangle \subseteq k[x_1, \ldots, x_n]$ be a monomial ideal. Then I can be written in the form $I = \langle x^{\alpha(1)}, \ldots, x^{\alpha(s)} \rangle$, where $\alpha(1), \ldots, \alpha(s) \in A$. In particular, I has a finite basis.

Gröbner bases

Definition

Let $I \subseteq k[x_1, \ldots, x_n]$ be an ideal other than $\{0\}$, and fix a monomial ordering on $k[x_1, \ldots, x_n]$. Then:

- We denote by $\mathrm{LT}(I)$ the set of leading terms of nonzero elements of I. Thus,

$$\mathrm{LT}(I) = \{cx^\alpha : \text{ there exists } f \in I \setminus \{0\} \text{ with } \mathrm{LT}(f) = cx^\alpha\}$$

- We denote by $\langle \mathrm{LT}(I) \rangle$ the ideal generated by the elements of $\mathrm{LT}(I)$.

Gröbner bases

Theorem

Let $I \subseteq k[x_1, \ldots, x_n]$ *be an ideal different from* 0*.*

- $\langle \mathrm{LT}(I) \rangle$ *is a monomial ideal.*
- *There are* $g_1, \ldots, g_t \in I$ *such that* $\langle \mathrm{LT}(I) \rangle = \langle \mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_t) \rangle$*.*

Gröbner bases

Definition (Gröbner basis)

Fix a monomial order on the polynomial ring $k[x_1, \ldots, x_n]$. A finite subset $G = \{g_1, \ldots, g_t\}$ of an ideal $I \subseteq k[x_1, \ldots, x_n]$ different from $\{0\}$ is said to be a Gröbner basis (or standard basis) if $\langle \mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_t)\rangle = \langle \mathrm{LT}(I)\rangle$. Using the convention that $\langle \emptyset \rangle = \{0\}$, we define the empty set $\emptyset$ to be the Gröbner basis of the zero ideal $\{0\}$.

Equivalently, a set $\{g_1, \ldots, g_t\} \subseteq I$ is a Gröbner basis of I if and only if the leading term of any element of I is divisible by one of the $\mathrm{LT}(g_i)$.

Gröbner bases

Theorem (Division with Gröbner bases)

Let $I \subseteq k[x_1, \ldots, x_n]$ be an ideal and let $G = \{g_1, \ldots, g_t\}$ be a Gröbner basis for I. Then given $f \in k[x_1, \ldots, x_n]$, there is a unique $r \in k[x_1, \ldots, x_n]$ with the following two properties:

- *No term of r is divisible by any of $\mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_t)$.*
- *There is $g \in I$ such that $f = g + r$.*

In particular, r is the remainder on division of f by G no matter how the elements of G are listed when using the division algorithm.

Gröbner bases

Definition

We will write $\overline{f}^F$ for the remainder on division of f by the ordered s-tuple $F = (f_1, \ldots, f_s)$.

If F is a Gröbner basis for $\langle f_1, \ldots, f_s \rangle$, then we can regard F as a set (without any particular order) by our previous results.

For instance, with $F = (x^2y - y^2, x^4y^2 - y^2) \subseteq k[x, y]$, using the lex order, we have $\overline{x^5y}^F = xy^3$ since the division algorithm yields $x^5y = (x^3 + xy)(x^2y - y^2) + 0 \cdot (x^4y^2 - y^2) + xy^3$.

Gröbner bases

To study cancellation phenomenons, we introduce the following special combinations.

Definition

Let $f, g \in k[x_1, \dots, x_n]$ be nonzero polynomials.

- If $multideg(f) = \alpha$ and $multideg(g) = \beta$, then let $\gamma = (\gamma_1, \dots, \gamma_n)$, where $\gamma_i = \max(\alpha_i, \beta_i)$ for each i. We call x^γ the least common multiple of $\mathrm{LM}(f)$ and $\mathrm{LM}(g)$, written $x^\gamma = \mathrm{lcm}(\mathrm{LM}(f), \mathrm{LM}(g))$.
- The S-polynomial of f and g is defined to be the combination

$$S(f, g) = \frac{x^\gamma}{\mathrm{LT}(f)} \cdot f - \frac{x^\gamma}{\mathrm{LT}(g)} \cdot g$$

Gröbner bases

The S-polynomial $S(f, g)$ has leading term that is guaranteed to be strictly less than $\mathrm{lcm}(\mathrm{LM}(f), \mathrm{LM}(g))$.

Gröbner bases

For example,let $f = x^3y^2 - x^2y^3 + x$ and $g = 3x^4y + y^2$ in $\mathbb{R}[x, y]$ with the grlex order.

Then $\gamma = (4, 2)$ and

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

Gröbner bases

Theorem (Buchberger's Criterion)

Let I be a polynomial ideal. Then a basis $G = \{g_1, \ldots, g_t\}$ of I is a Gröbner basis of I if and only if for all pairs $i \neq j$, the remainder on division of $S(g_i, g_j)$ by G (listed in some order) is zero.

Buchberger's algorithm

Theorem (Buchberger's Algorithm)

Let $I = \langle f_1, \ldots, f_s \rangle \neq 0$ be a polynomial ideal. Then a Gröbner basis for I can be constructed in a finite number of steps by the following algorithm:

Input : $F = (f_1, \ldots, f_s)$
Output : a Gröbner basis $G = (g_1, \ldots, g_t)$ *for* I, *with* $F \subseteq G$
$G := F$
REPEAT
    $G' := G$
    FOR each pair $\{p, q\}$, $p \neq q$ *in* G' *DO*
        $r := \overline{S(p, q)}^{G'}$
        IF $r \neq 0$ *THEN* $G := G \cup \{r\}$
UNTIL $G = G'$
RETURN G

Refinement of Buchberger's criterion and first improved algorithm

We have a more general criterion to the one we presented before.

Theorem

A basis $G = \{g_1, \ldots, g_t\}$ for an ideal I is a Gröbner basis if and only if $S(g_i, g_j) \to_G 0$ for all $i \neq j$.

f reduces to zero modulo G, written $f \to_G 0$, if f has a standard representation $f = A_1 g_1 + \cdots + A_t g_t$, $A_{\in} k[x_1, \ldots, x_n]$, which means that whenever $A_i g_i \neq 0$, we have $multideg(f) \geq multideg(A_i g_i)$.

Refinement of Buchberger's criterion and first improved algorithm

Theorem

Given a finite set $G \subseteq k[x_1, \ldots, x_n]$, suppose that we have f, $g \in G$ such that the leading monomials of f and g are relatively prime. Then $S(f, g) \to_G 0$.

Faugère's F4 algorithm

The information generated by several S-polynomial remainder computations can be obtained simultaneously via row operations on a suitable matrix - this was first noted by Daniel Lazard in the 80s. This connection with linear algebra is the basis for Jean-Charles Faugère's F4 algorithm, in which the goal is to compute S-pairs and to reduce them simultaneously using linear algebra [3].

Faugère's F4 algorithm

The matrix in question is usually (very) sparse and we can use fast reduction algorithm, such as GBLA (Gröbner Bases Linear Algebra), from Faugère and Sylvian Lachartre.

Signature based algorithms and Faugère's F5 algorithm

One of the features of the signature-based family of Gröbner basis algorithms is the systematic use of information indicating how the polynomials generated in the course of the computation depend on the original input polynomials $f_1, \ldots, f_s$. The goal is to eliminate unnecessary S-polynomial remainder calculations as much as possible by exploiting relations between the f_i [4].

Signature based algorithms and Faugère's F5 algorithm

Idea:

If $I = \langle f_1, \ldots, f_s \rangle$ is any collection of polynomials, then the S-polynomials and remainders produced in the course of a Gröbner basis computation can all be written as

$$(a_1, \ldots, a_s) \cdot (f_1, \ldots, f_s) = a_1 f_1 + \cdots + a_s f_s$$

for certain $a = (a_1, \ldots, a_s)$ in $k[x_1, \ldots, x_n]^s$. We will see that there are key features of the vectors a corresponding to some S-polynomials that make computing the S-polynomial remainder unnecessary. Those key features can be recognised directly from the largest term in the vector and other information known to the algorithm. In particular, it is not necessary to compute the combination $a_1 f_1 + \cdots + a_s f_s$ to recognise that a key feature is present.

Signature based algorithms and Faugère's F5 algorithm

Definition (Signature)

Let $\mathbf{g} = (g_1, \ldots, g_s) \in R^s$. Then the signature of $\mathbf{g}$, denoted $\mathfrak{S}(\mathbf{g})$, is the term appearing in $\mathbf{g}$ that is largest in the $>_{POT}$ order.

POT order extending the order $>$ on R:

$$x^\alpha \mathbf{e}_i >_{POT} x^\beta \mathbf{e}_j \Leftrightarrow i > j, \text{ or } i = j \text{ and } x^\alpha > x^\beta$$

Signature based algorithms and Faugère's F5 algorithm

Consider $f_1 = x^2 + xy$ and $f_2 = x^2 + y$ in $\mathbb{Q}[x, y]$, using the grevlex order with $x > y$.

$$S(f_1, f_2) = (1, -1) \cdot (f_1, f_2) = xy - y$$

Since that does not reduce to zero under $\{f_1, f_2\}$, we would include $f_3 = \overline{S(f_1, f_2)}^{\{f_1, f_2\}} = xy - y$ as a new Gröbner basis element.

Signature based algorithms and Faugère's F5 algorithm

$$S(f_1, f_3) = yf_1 - xf_3 = yf_1 - x(f_1 - f_2) = (y - x)f_1 + xf_2$$

$$\overline{S(f_1, f_3)}^{\{f_1, f_2, f_3\}} = y^2 + y$$

This gives another Gröbner basis element. Similarly:

$$S(f_2, f_3) = yf_2 - xf_3 = yf_2 - x(f_1 - f_2) = -xf_1 + (x + y)f_2$$

$$\overline{S(f_2, f_3)}^{\{f_1, f_2, f_3\}} = y^2 + y$$

Signature based algorithms and Faugère's F5 algorithm

These two remainder calculations have led to precisely the same result!

We could have predicted this.

$$S(f_1, f_3) = (y - x)f_1 + xf_2 = \mathbf{a} \cdot (f_1, f_2)$$

$$S(f_2, f_3) = -xf_1 + (x + y)f_2 = \mathbf{b} \cdot (f_1, f_2)$$

The largest terms in the POT order are the same for **a** and **b**—in both vectors, the largest term is the $x\mathbf{e}_2$.

References

1 Fayssal M, Renault G, Albrecht MR. Faugère-Lachartre Parallel Gaussian Elimination for Gröbner Bases Computations Over Finite Fields. Master's thesis, Pierre and Marie Curie University; 2012.

2 Cox DA, Little J, O'Shea D. Ideals, Varieties, and Algorithms: An Introduction to Computational Algebraic Geometry and Commutative Algebra, 3rd edition (Undergraduate Texts in Mathematics). Berlin, Heidelberg: Springer-Verlag; 2007.

References

3 Faugère JC. A new efficient algorithm for computing Gröbner bases (F4). Journal of Pure and Applied Algebra. 1999;139(1):61 - 88. Available from: http://www.sciencedirect.com/science/article/pii/S0022404999000055.

4 Faugère JC. A new efficient algorithm for computing Gröbner bases with out reduction to zero (F5). In: Proceedings of the 2002 international symposium on Symbolic and algebraic computation; 2002. p. 75–83.

Thank you for listening!

Thank you for your attention!

Staircases

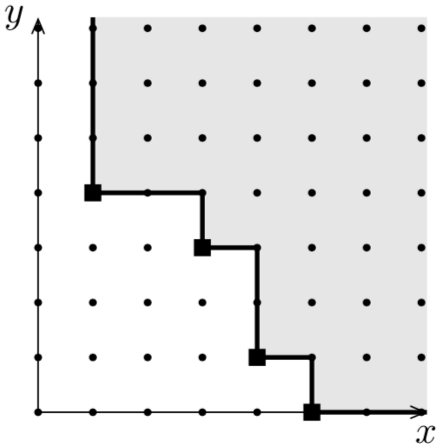

Figure 1: The ideal $I = \langle xy^4, x^3y^3, x^4y, x^5 \rangle$

Staircases

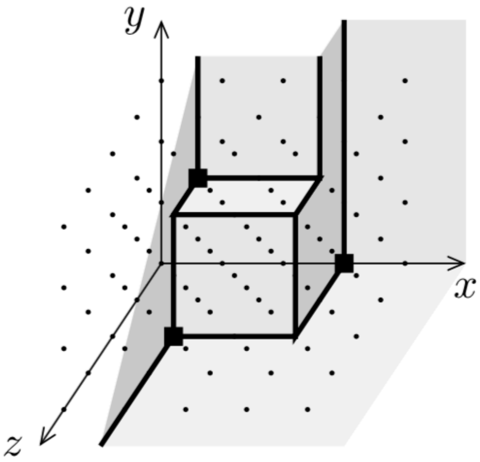

Figure 2: The ideal $I = \langle x^3, xy^2z, xz^2 \rangle$

Staircases

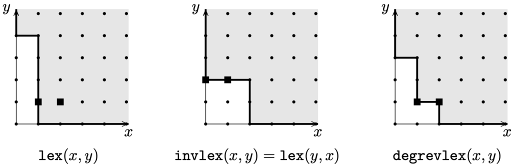

Figure 3: The ideal $I = \langle xy + x + y^2 + 1, x^2y + xy^2 + 1\rangle$

$$
\begin{aligned}
G_1 &= \{x - \frac{1}{2}y^3 + y^2 + \frac{3}{2}, y^4 - y^3 - 3y - 1\} \\
G_2 &= \{y^2 + xy + x + 1, x^2 + x - 1\} \\
G_3 &= \{y^3 - 2y^2 - 2x - 3, x^2 + x - 1, xy + y^2 + x + 1\}
\end{aligned}
$$

Gröbner basis

The coefficients of the elements of Gröbner basis can be significantly messier than the coefficients of the original generating set. For example, for $I = \langle x^2 + y^2 + z^2 - xy, x^2y^2z + z, x^2y + y^2z + z\rangle$, a Gröbner basis (with graded lexicographic order) is:

$$G = \left\{ \begin{array}{l} y^3z^2 + yz^2 - z, \\ z^5 - \frac{3}{5}xyz + \frac{6}{5}xz^2 - \frac{1}{5}y^2z - yz^2 - \frac{4}{5}z^3 + \frac{1}{5}z, \\ xyz^2 - \frac{1}{4}y^3z - \frac{3}{4}y^2z^2 - \frac{5}{4}z^4 - \frac{1}{2}xz + \frac{1}{4}yz, \\ xz^3 + \frac{1}{2}y^3z - \frac{1}{2}y^2z^2 - \frac{1}{2}z^4 - xz + \frac{1}{2}yz - z^2, \\ y^4 - \frac{3}{4}y^3z + \frac{11}{4}y^2z^2 + \frac{5}{4}z^4 + \frac{1}{2}xz - \frac{5}{4}yz + 2z^2, \\ yz^3 + xz - yz + z^2, \\ xy^2 - y^3 + y^2z - yz^2 + z, \\ x^2 - xy + y^2 + z^2 \end{array} \right\}$$

F4

F4 ALGORITHM
Input: $F = (f_1, \dots, f_s)$
Output: a Gröbner basis G for $I = \langle f_1, \dots, f_s \rangle$

```
G := F
k := s
B := {(i, j) : 1 ≤ i < j ≤ k}
WHILE B ≠ 0 DO
   B' := select(B)
   B := B\B'
   G' := REDUCTION(B', G)
   FOR h in G' DO
      G := G ∪ {h}
      k := k + 1
      B := B ∪ {(i, k) : 1 ≤ i < k}
return G
```

F4

REDUCTION

Input: a set of pairs B' and a current basis G

Output: a set G' of new basis elements

$L :=$ SYMBOLICPREPROCESSING(B', G)

$M :=$ matrix with rows the polynomials in L

$M' :=$ reduced row echelon form of M

$L' :=$ polynomials corresponding to the rows of M'

$G' := \{f \in L' : \mathrm{LM}(f) \neq \mathrm{LM}(g) \text{ for any } g \in L\}$

RETURN G'

F4

SYMBOLICPREPROCESSING
Input: a set of pairs B' and a current basis G
Output: a set L of polynomials

Left $:= \{\mathrm{lcm}(\mathrm{LM}(G_i), \mathrm{LM}(G_j))/\,\mathrm{LT}(G_i) \cdot G_i : (i,j) \in B'\}$
Right $:= \{\mathrm{lcm}(\mathrm{LM}(G_i), \mathrm{LM}(G_j))/\,\mathrm{LT}(G_j) \cdot G_j : (i,j) \in B'\}$
$L :=$ Left $\cup$ Right
done $:= \{\mathrm{LM}(f) : f \in L\}$
WHILE done $\neq \mathrm{Mon}(L)$ DO
  $m :=$ largest monomial in $(\mathrm{Mon}(L) \setminus$ done$)$
  done $:=$ done $\cup \{m\}$
  IF $\mathrm{LM}(g)$ divides m for some g in G THEN
    $f :=$ choose g such that $\mathrm{LM}(g)$ divides m
    $L := L \cup \{m/\,\mathrm{LM}(f) \cdot f\}$
RETURN L

POT order

If $\mathbf{g} = (x^3, y, x + z^2)$ in $\mathbb{Q}[x, y, z]^3$, with $>_{POT}$ extending the grevlex order with $x > y > z$, then $\mathfrak{S}(\mathbf{g}) = z^2\mathbf{e}_3$.