WHAT IS...

a Gröbner Basis?

Bernd Sturmfels

A *Gröbner basis* is a set of multivariate polynomials that has desirable algorithmic properties. Every set of polynomials can be transformed into a Gröbner basis. This process generalizes three familiar techniques: *Gaussian elimination* for solving linear systems of equations, the *Euclidean algorithm* for computing the greatest common divisor of two univariate polynomials, and the *Simplex Algorithm* for linear programming; see [3]. For example, the input for Gaussian elimination is a collection of linear forms such as

$$\mathcal{F} = \Big\{ 2x + 3y + 4z - 5, 3x + 4y + 5z - 2 \Big\},$$

and the algorithm transforms $\mathcal{F}$ into the Gröbner basis

$$\mathcal{G} = \Big\{ \underline{x} - z + 14, \ \underline{y} + 2z - 11 \Big\}.$$

Let K be any field, such as the real numbers $K = \mathbb{R}$, the complex numbers $K = \mathbb{C}$, the rational numbers $K = \mathbb{Q}$, or a finite field $K = \mathbb{F}_p$. We write $K[x_1, \ldots, x_n]$ for the ring of polynomials in n variables x_i with coefficients in the field K. If $\mathcal{F}$ is any set of polynomials, then the *ideal generated* by $\mathcal{F}$ is the set $\langle \mathcal{F} \rangle$ consisting of all polynomial linear combinations:

$$\langle \mathcal{F} \rangle = \Big\{ p_1 f_1 + \cdots + p_r f_r \ : f_1, \ldots, f_r \in \mathcal{F} \quad \text{and} \quad p_1, \ldots, p_r \in K[x_1, \ldots, x_n] \Big\}.$$

In our example the set $\mathcal{F}$ and its Gröbner basis $\mathcal{G}$ generate the same ideal: $\langle \mathcal{G} \rangle = \langle \mathcal{F} \rangle$. By *Hilbert's Basis Theorem*, every ideal I in $K[x_1, \ldots, x_n]$ has the form $I = \langle \mathcal{F} \rangle$; i.e., it is generated by some finite set $\mathcal{F}$ of polynomials.

A *term order* on $K[x_1, \ldots, x_n]$ is a total order $\prec$ on the set of all monomials $x^a = x_1^{a_1} \cdots x_n^{a_n}$ which has the following two properties:

(1) It is multiplicative; i.e., $x^a \prec x^b$ implies $x^{a+c} \prec x^{b+c}$ for all $a, b, c \in \mathbb{N}^n$.

(2) The constant monomial is the smallest; i.e., $1 \prec x^a$ for all $a \in \mathbb{N}^n \backslash \{0\}$.

An example of a term order (for $n = 2$) is the *degree lexicographic order*

$$1 \prec x_1 \prec x_2 \prec x_1^2 \prec x_1 x_2 \prec x_2^2 \prec x_1^3 \prec x_1^2 x_2 \prec \cdots .$$

If we fix a term order $\prec$, then every polynomial f has a unique *initial term* $in_\prec(f) = x^a$. This is the $\prec$-largest monomial x^a which occurs with nonzero coefficient in the expansion of f. We write the terms of f in $\prec$-decreasing order, and we often underline the initial term. For instance, a quadratic polynomial is written

$$f = \underline{3x_2^2} + 5x_1 x_2 + 7x_1^2 + 11x_1 + 13x_2 + 17.$$

Suppose now that I is an ideal in $K[x_1, \ldots, x_n]$. Then its *initial ideal* $in_\prec(I)$ is the ideal generated by the initial terms of all the polynomials in I:

$$in_\prec(I) = \langle \, in_\prec(f) : f \in I \rangle.$$

A finite subset $\mathcal{G}$ of I is a *Gröbner basis* with respect to the term order $\prec$ if the initial terms of the elements in $\mathcal{G}$ suffice to generate the initial ideal:

$$in_\prec(I) = \langle \, in_\prec(g) \, : \, g \in \mathcal{G} \, \rangle.$$

There is no minimality requirement for being a Gröbner basis. If $\mathcal{G}$ is a Gröbner basis for I, then any finite subset of I that contains $\mathcal{G}$ is also a Gröbner basis. To remedy this nonminimality, we say that $\mathcal{G}$ is a *reduced Gröbner basis* if

(1) for each $g \in \mathcal{G}$, the coefficient of $in_\prec(g)$ in g is 1,

(2) the set $\{ in_\prec(g) : g \in \mathcal{G} \}$ minimally generates $in_\prec(I)$, and

(3) no trailing term of any $g \in \mathcal{G}$ lies in $in_\prec(I)$.

With this definition, we have the following theorem: If the term order $\prec$ is fixed, then every ideal I in $K[x_1, \ldots, x_n]$ has a unique reduced Gröbner basis.

The reduced Gröbner basis $\mathcal{G}$ can be computed from any generating set of I by a method that was introduced in Bruno Buchberger's 1965 dissertation. Buchberger named his method after his advisor, Wolfgang Gröbner. With hindsight, the idea of Gröbner bases can be traced back to earlier sources, including a paper written in 1900 by the invariant theorist Paul Gordan. But Buchberger was the first to give an algorithm for computing Gröbner bases.

Bernd Sturmfels is a professor of mathematics and computer science at the University of California at Berkeley. His email address is `bernd@math.berkeley.edu`.

Gröbner bases are very useful for solving systems of polynomial equations. Suppose $K \subseteq \mathbb{C}$, and let $\mathcal{F}$ be a finite set of polynomials in $K[x_1,\dots,x_n]$. The *variety* of $\mathcal{F}$ is the set of all common complex zeros:

$$\mathcal{V}(\mathcal{F}) = \Big\{ (z_1,\dots,z_n) \in \mathbb{C}^n : f(z_1,\dots,z_n) = 0 \quad \text{for all} \quad f \in \mathcal{F} \Big\}.$$

The variety does not change if we replace $\mathcal{F}$ by another set of polynomials that generates the same ideal in $K[x_1,\dots,x_n]$. In particular, the reduced Gröbner basis $\mathcal{G}$ for the ideal $\langle \mathcal{F} \rangle$ specifies the same variety:

$$\mathcal{V}(\mathcal{F}) = \mathcal{V}(\langle \mathcal{F} \rangle) = \mathcal{V}(\langle \mathcal{G} \rangle) = \mathcal{V}(\mathcal{G}).$$

The advantage of $\mathcal{G}$ is that it reveals geometric properties of the variety that are not visible from $\mathcal{F}$. The first question that one might ask about a variety $\mathcal{V}(\mathcal{F})$ is whether it is empty. *Hilbert's Nullstellensatz* implies that

$$\text{the variety } \mathcal{V}(\mathcal{F}) \text{ is empty if and only if } \mathcal{G} \text{ equals } \{1\}.$$

How can one count the number of zeros of a given system of equations? To answer this, we need one more definition. Given a fixed ideal I in $K[x_1,\dots,x_n]$ and a term order $\prec$, a monomial $x^a = x_1^{a_1} \cdots x_n^{a_n}$ is called *standard* if it is not in the initial ideal $in_\prec(I)$. The number of standard monomials is finite if and only if every variable x_i appears to some power in the initial ideal. For example, if $in_\prec(I) = \langle x_1^3, x_2^4, x_3^5 \rangle$, then there are sixty standard monomials, but if $in_\prec(I) = \langle x_1^3, x_2^4, x_1 x_3^4 \rangle$, then the set of standard monomials is infinite.

The variety $\mathcal{V}(I)$ is finite if and only if the set of standard monomials is finite, and the number of standard monomials equals the cardinality of $\mathcal{V}(I)$, when zeros are counted with multiplicity. For $n = 1$ this is the *Fundamental Theorem of Algebra*, which states that the variety $\mathcal{V}(f)$ of a univariate polynomial $f \in K[x]$ of degree d consists of d complex numbers. Here the singleton $\{f\}$ is a Gröbner basis, and the standard monomials are $1, x, x^2, \dots, x^{d-1}$.

Our criterion for deciding whether a variety is finite generalizes to the following formula for the *dimension of a variety*. Consider a subset S of the variables $\{x_1,\dots,x_n\}$ such that no monomial in the variables in S appears in $in_\prec(I)$, and suppose that S has maximal cardinality among all subsets with this property. That maximal cardinality $|S|$ equals the dimension of $\mathcal{V}(I)$.

The set of standard monomials is a K-vector-space basis for the *residue ring* $K[x_1,\dots,x_n]/I$. The image of a polynomial p modulo I can be expressed uniquely as a K-linear combination of standard monomials. This expression is the *normal form* of p. The process of computing the normal form is the *division algorithm*. In the familar case of only one variable x, where $I = \langle f \rangle$ and f has degree d, the division algorithm writes any polynomial $p \in K[x]$ as a K-linear combination of $1, x, x^2, \dots, x^{d-1}$. But the division algorithm works relative to any Gröbner basis $\mathcal{G}$ in any number of variables.

How can we test whether a given set of polynomials $\mathcal{G}$ is a Gröbner basis or not? Consider any two polynomials g and g' in $\mathcal{G}$, and form their *S-polynomial* $m'g - mg'$. Here m and m' are monomials of smallest possible degree such that $m' \cdot in_\prec(g) = m \cdot in_\prec(g')$. The S-polynomial $m'g - mg'$ lies in the ideal $\langle \mathcal{G} \rangle$. We apply the division algorithm with respect to the tentative Gröbner basis $\mathcal{G}$ to $m'g - mg'$. The resulting normal form is a K-linear combination of monomials none of which is divisible by an initial monomial from $\mathcal{G}$. A necessary condition for $\mathcal{G}$ to be a Gröbner basis is

$$\text{normalform}_{\mathcal{G}}(m'g - mg') = 0 \quad \text{for all } g, g' \in \mathcal{G}.$$

Buchberger's Criterion states that this necessary condition is sufficient: a set $\mathcal{G}$ of polynomials is a Gröbner basis if and only if all its S-polynomials have normal form zero. From this criterion, one derives *Buchberger's Algorithm* [1] for computing the reduced Gröbner basis $\mathcal{G}$ from any given input set $\mathcal{F}$.

In summary, Gröbner bases and the Buchberger Algorithm for finding them are fundamental notions in algebra. They furnish the engine for more advanced computations in algebraic geometry, such as elimination theory, computing cohomology, resolving singularities, etc. Given that polynomial models are ubiquitous across the sciences and engineering, Gröbner bases have been used by researchers in optimization, coding, robotics, control theory, statistics, molecular biology, and many other fields. We invite the reader to experiment with one of the many implementations of Buchberger's algorithm (e.g., in `CoCoA`, `Macaulay2`, `Magma`, `Maple`, `Mathematica`, or `Singular`).

References

[1] David Cox, John Little, and Donal O' Shea, *Ideals, Varieties and Algorithms. An Introduction to Computational Algebraic Geometry and Commutative Algebra*, second ed., Undergraduate Texts in Mathematics, Springer-Verlag, New York, 1997.

[2] Niels Lauritzen, *Concrete Abstract Algebra: From Numbers to Gröbner Bases*, Cambridge University Press, 2003.

[3] Bernd Sturmfels, *Two Lectures on Gröbner Bases*, New Horizons in Undergraduate Mathematics, VMath Lecture Series, Mathematical Sciences Research Institute, Berkeley, California, 2005, `http://www.msri.org/communications/vmath/special_productions/`.