Last updated: 28 January 2023

2 *Gröbner Bases*

Gröbner basis provide a crucial computational tool for solving systems of polynomial equations and computing the Zariski closure of images of algebraic varieties under rational maps.

2.0 Noetherian rings

Which affine subvarieties are defined by finitely many polynomials?

2.0.0 Theorem (Hilbert basis)**.** *Let n be nonnegative integer. Every ideal in the polynomial ring $S := \mathbb{K}[x_1, x_2, \ldots, x_n]$ is finitely generated.*

David Hilbert's original proof in 1888 was nonconstructive. It is reported that when Paul Gordan first saw Hilbert's proof, he said, "This is not mathematics, but theology!" However, when Gordan published his proof of the Hilbert basis theorem in 1899, he said, "I have convinced myself that theology also has it advantages."

Proof by Gordon. Fix a monomial order $>$ on S and let I be an ideal in S. By definition, the leading term ideal $\mathrm{LT}(I)$ is generated by the monomials $\mathrm{LM}(f)$ for all $f \in I$. The Dickson Lemma 1.1.4 implies that monomial ideal $\mathrm{LT}(I)$ is finitely generated. Hence, there exists $g_1, g_2, \ldots, g_m \in I$ such that $\mathrm{LT}(I) = \langle \mathrm{LM}(g_1), \mathrm{LM}(g_2), \ldots, \mathrm{LM}(g_m) \rangle$. It suffices to show that $I = \langle g_1, g_2, \ldots, g_m \rangle$.

Clearly, we have $\langle g_1, g_2, \ldots, g_m \rangle \subseteq I$. For the converse, suppose that $f \in I$. Applying the Division Algorithm 1.2.2, we obtain

$$f = q_1 g_1 + q_2 g_2 + \cdots + q_m g_m + r$$

where none of the monomials in the remainder r belong to $\mathrm{LT}(I)$. When $r \neq 0$, the equation $r = f - q_1 g_1 - q_2 g_2 - \cdots - q_m g_m \in I$ implies that $\mathrm{LT}(r) \in \mathrm{LT}(I)$. It follows that $\mathrm{LT}(r)$ is divisible by some $\mathrm{LT}(g_i)$, which is a contradiction. Consequently, we must have $r = 0$, $f \in \langle g_1, g_2, \ldots, g_m \rangle$, and $I \subseteq \langle g_1, g_2, \ldots, g_m \rangle \subseteq I$. □

The contemporary form of the Hilbert basis theorem allows for coefficients in more general commutative rings. Before explaining this variant, we need an additional concept.

2.0.1 Theorem. *A commutative ring R is* noetherian *if it satisfies the following three equivalent conditions.*

(a) *Every ascending chain of ideals in the ring R becomes stationary: for any nested sequence $I_0 \subseteq I_1 \subseteq I_3 \subseteq \cdots$ of ideals in R, there exists a nonnegative integer m such that $I_m = I_{m+1} = I_{m+2} = \cdots$.*

(b) *Every nonempty set of ideals in R, partially ordered by inclusion, has a maximal element.*

(c) *Every ideal in R is finitely generated.*

Emmy Noether introduced the ascending chain condition in 1921.

All principal ideal domains, including fields, $\mathbb{Z}$, and $\mathbb{K}[x]$, are noetherian.

Proof.

(a) ⇒ (b): Suppose that $\mathcal{I}$ be a nonempty family of ideals in R having no maximal element. Choose $I_1 \in \mathcal{I}$. Since I_1 is not maximal, there exists $I_2 \in \mathcal{I}$ such that $I_1 \subset I_2$. The ideal I_2 is not maximal, so there is $I_3 \in \mathcal{I}$ with $I_2 \subset I_3$. Continuing in this way, we would construct a non-stationary ascending chain of ideals in R, contradicting the ascending chain condition.

(b) ⇒ (c): Let I be an ideal in R and define $\mathcal{I}$ to be the family of all the finitely generated ideals contained in I. This family is nonempty, because it contains the zero ideal. By hypothesis, there exists a maximal $M \in \mathcal{I}$. We have $M \subseteq I$ because $M \in \mathcal{I}$. If $M \subset I$, then there exists $f \in I$ such that $f \notin M$. The ideal

$$J := \{g + rf \mid g \in M \text{ and } r \in R\} = M + \langle f \rangle \subseteq I$$

is finitely generated, so $J \in \mathcal{I}$ and $M \subset J$ contradicting the maximality of M. We deduce that $M = I$ and the ideal I is finitely generated.

(c) ⇒ (a): Assume that every ideal in R is finitely generated and let $I_0 \subseteq I_1 \subseteq \cdots \subseteq I_j \subseteq \cdots$ be an ascending chain of ideals in R. The union $J := \bigcup_{j \in \mathbb{N}} I_j$ is an ideal. By hypothesis, there exists $g_1, g_2, \ldots, g_k \in J$ such that $J = \langle g_1, g_2, \ldots, g_k \rangle$. For each $i \in \mathbb{N}$, the element g_i belongs to J by being in I_{j_i} for some j_i. Setting m to be the largest j_i, we see that $I_{j_i} \subseteq I_m$ for all i. It follows that $g_i \in I_m$ for all i, so $J = \langle g_1, g_2, \ldots, g_k \rangle \subseteq I_m \subseteq J$. We deduce that, for all $j \geqslant m$, we have $J = I_m \subseteq I_j \subseteq J$ and $I_m = J$. Therefore, the ascending chain stops and the ring R satisfies the ascending chain condition. □

Let R be the ring of all real-valued functions on the reals under pointwise operations. For any $n \in \mathbb{N}$, the set

$$I_n := \{f \colon \mathbb{R} \to \mathbb{R} \mid f(x) = 0 \text{ for all } x \geqslant n\}$$

is an ideal in R and $I_n \subset I_{n+1}$. Thus, the ring R is not noetherian.

2.0.2 Theorem. *For any noetherian ring R, $R[x]$ is also noetherian.*

Proof. Let I be an ideal in $R[x]$. Suppose that I is not finitely generated. Choose a sequence $f_0, f_1, f_2, \ldots$ in I such that f_{i+1} has minimal degree in the set $I \setminus \langle f_0, f_1, \ldots, f_i \rangle$. For all $i \in \mathbb{N}$, set $a_i := \operatorname{LC}(f_i)$ and let $J := \langle a_0, a_1, a_2, \ldots \rangle$ be the ideal in R. As R is noetherian, there is $m \in \mathbb{N}$ such that $J = \langle a_0, a_1, \ldots, a_m \rangle$. For some $b_j \in R$ with $0 \leqslant j \leqslant m$, we have $a_{m+1} = b_0\, a_0 + b_1\, a_1 + \cdots + b_m\, a_m$. Consider the polynomial

$$g := b_0\, f_0\, x^{d_0} + b_1\, f_1\, x^{d_1} + \cdots + b_m\, f_m\, x^{d_m}$$

where $d_j := \deg(f_{m+1}) - \deg(f_i)$. Because $\deg(g) = \deg(f_{m+1})$ and the leading coefficient of g and f_{m+1} agree, the difference $f_{m+1} - g$ has degree strictly less than the degree of f_{m+1}, contradicting the choice of f_{m+1}. Therefore, the ideal I is finitely generated. □

2.0.3 Corollary. *Let R be a noetherian ring. For all nonnegative integers n, the polynomial ring $R[x_1, x_2, \ldots, x_n]$ is also noetherian.*

Proof. We proceed by induction on n. The base case $n = 0$ is vacuous. Assuming that $R[x_1, x_2, \dots, x_{n-1}]$ is noetherian, Theorem 2.0.2 shows that $(R[x_1, x_2, \dots, x_{n-1}])[x_n] = R[x_1, x_2, \dots, x_n]$ is noetherian. □

2.1 Remainders

How do Gröbner basis effect division?

2.1.0 Proposition. *Fix a monomial order on $S := \mathbb{K}[x_1, x_2, \dots, x_n]$ and assume that $g_1, g_2, \dots, g_m \in S$ form a Gröbner basis for an ideal I in S. For any $f \in S$, there exists a unique polynomial $r \in S$ such that*

- *none of monomials in r are divisible by monomials of $\operatorname{LT}(I)$, and*
- *there is an element $g \in I$ such that $f = g + r$.*

When $g_1, g_2, \dots, g_m$ is a Gröbner basis, the remainder f on division by vector $[g_1 \;\; g_2 \;\; \cdots \;\; g_m]^{\mathsf{T}}$ is independent of the order of the entries.

Proof. Set $\mathbf{G} := [g_1 \;\; g_2 \;\; \cdots \;\; g_m]^{\mathsf{T}}$. The Division Algorithm 1.2.2 demonstrates that $f = q_1 g_1 + q_2 g_2 + \cdots + q_m g_m + r$ for some $q_1, q_2, \dots, q_m, r \in S$ where none of the monomials in r are divisible by a monomial in $\operatorname{LT}(I)$. Setting $g = q_1 g_1 + q_2 g_2 + \cdots + q_m g_m$, we see that there exists a polynomial r with the desired properties.

Given two expressions $f = g + r$ and $f = g' + r'$, it follows that $r - r' = g' - g \in I$. If $r \neq r'$, then we have $\operatorname{LT}(r - r') \in \operatorname{LT}(I)$, so some monomial in r or r' is divisible by an element of $\operatorname{LT}(I)$. As this contradicts the properties of r and r', we must have $r = r'$. □

2.1.1 Corollary. *Let $g_1, g_2, \dots, g_m$ be a Gröbner basis for the ideal I in S. A polynomial $f \in S$ belongs to the ideal I if and only if its remainder on division by $[g_1 \;\; g_2 \;\; \cdots \;\; g_m]^{\mathsf{T}}$ is zero.*

By constructing a Gröbner basis for any ideal in S, we obtain a solution to the ideal membership problem [1.0.1].

Proof. Having the remainder being zero means that

$$f = q_1 g_1 + q_2 g_2 + \cdots + q_m g_m$$

which implies $f \in \langle g_1, g_2, \dots, g_m \rangle = I$. Conversely, for any $f \in I$, the expression $f + 0$ satisfies the conditions in Proposition 2.1.0. It follows that 0 is the remainder. □

2.2 Gröbner basics

How can we recognize a Gröbner basis? To answer this question, we exploit some auxiliary polynomials.

2.2.0 Definition. For two polynomials f and g in $S := \mathbb{K}[x_1, x_2, \dots, x_n]$, the *S-polynomial* is

$$\operatorname{spoly}(f, g) := \frac{\operatorname{lcm}\big(\operatorname{LM}(f), \operatorname{LM}(g)\big)}{\operatorname{LT}(f)} f - \frac{\operatorname{lcm}\big(\operatorname{LM}(f), \operatorname{LM}(g)\big)}{\operatorname{LT}(g)} g .$$

By design, the leading terms of f and g cancel in their S-polynomial. The "S" apparently refers to either "subtraction" or "syzygy".

2.2.1 Example. Choose a monomial order on $\mathbb{Q}[x,y]$ such that $x > y$. When $f := 2xy - x$ and $g := 3x^3 - y$, we have

$$\begin{aligned}\operatorname{spoly}(f,g) &= \frac{\operatorname{lcm}(xy,x^3)}{2xy} f - \frac{\operatorname{lcm}(xy,x^3)}{3x^3} g \\ &= \frac{x^2}{2}(2xy - x) - \frac{y}{3}(3x^3 - y) = -\frac{1}{2}x^3 + \frac{1}{3}y^2 . \end{aligned} \qquad \diamond$$

2.2.2 Theorem (Buchberger criterion). *The polynomials $g_1, g_2, \ldots, g_m$ in the ring S form a Gröbner basis if and only if, for all $1 \leqslant i < j \leqslant m$, the remainder of $\operatorname{spoly}(g_i, g_j)$ on division by $\mathbf{G} := [g_1 \;\; g_2 \;\; \cdots \;\; g_m]^{\mathsf{T}}$ is zero.*

In 1965, Bruno Buchberger introduced this criterion in his PhD thesis supervised by Wolfgang Gröbner.

Proof. Set $I := \langle g_1, g_2, \ldots, g_m \rangle$.

$\Rightarrow$: Assuming that $g_1, g_2, \cdots, g_m$ form a Gröbner basis, it follows that $\operatorname{spoly}(g_i, g_j) \in I$, so $\operatorname{spoly}(g_i, g_j) \,\%\, \mathbf{G} = 0$ for all $1 \leqslant i < j \leqslant m$.

$\Leftarrow$: Suppose that the remainder of each S-polynomial is zero. When $g_1, g_2, \ldots, g_m$ do not form a Gröbner basis, some $f \in I$ does not have its leading term in the ideal $\langle \operatorname{LT}(g_1), \operatorname{LT}(g_2), \cdots, \operatorname{LT}(g_m) \rangle$. Choose $f_1, f_2, \ldots, f_m \in S$ such that $f = f_1 g_1 + f_2 g_2 + \cdots + f_m g_m$ and two minimality assumptions hold:

- the monomial $x^u = \max_j \{\operatorname{LM}(f_j g_j)\}$ is minimal, and
- the number of indices j realizing the maximum is minimal.

After reindexing the g_j's, we may assume that

$$\operatorname{LM}(f_1 g_1) = \operatorname{LM}(f_2 g_2) = \cdots = \operatorname{LM}(f_k g_k) = x^u$$

and, for all $j > k$, we also have $\operatorname{LM}(f_j g_j) < x^u$. We observe that $k \geqslant 2$, because the x^u-terms cancel. Since $\operatorname{spoly}(g_1, g_2) \,\%\, \mathbf{G} = 0$, there exists polynomials $h_1, h_2, \ldots, h_m \in S$ such that

$$\operatorname{spoly}(g_1, g_2) = h_1 g_1 + h_2 g_2 + \cdots + h_m g_m$$

and, for all $1 \leqslant j \leqslant m$, we have $\operatorname{LM}\big(\operatorname{spoly}(g_1, g_2)\big) \geqslant \operatorname{LM}(h_j g_j)$. The definition of an S-polynomial gives

$$\frac{\operatorname{lcm}\big(\operatorname{LM}(g_1), \operatorname{LM}(g_2)\big)}{\operatorname{LT}(g_1)} g_1 - \frac{\operatorname{lcm}\big(\operatorname{LM}(g_1), \operatorname{LM}(g_2)\big)}{\operatorname{LT}(g_2)} g_2 - h_1 g_1 - h_2 g_2 - \cdots - h_m g_m = 0 . \tag{‡}$$

The least common multiple of the two monomials $\operatorname{LM}(g_1)$ and $\operatorname{LM}(g_2)$ divides x^u because $\operatorname{LM}(f_1 g_1) = x^u = \operatorname{LM}(f_2 g_2)$. Hence, there is a monomial $q \in S$ such that

$$q \cdot \operatorname{lcm}\big(\operatorname{LM}(g_1), \operatorname{LM}(g_2)\big) = \operatorname{LT}(f_1) \operatorname{LT}(g_1) .$$

Subtracting q times (‡) from chosen expression for f, we obtain $f = \widetilde{f}_1 g_1 + \widetilde{f}_2 g_2 + \cdots + \widetilde{f}_m g_m$ such that $x^u \geqslant \operatorname{LM}(\widetilde{f}_j g_j)$ with strict inequality from $j > k$ and $j = 1$. This contradicts the minimality assumption in our chosen expression for f. $\square$

2.2.3 Problem. Fix a monomial order $>$ on $\mathbb{Q}[x,y]$ such that $x > y$. Show that polynomials $x^2 - y, xy - x, y^2 - y$ form a Gröbner basis for the ideal $I := \langle x^2 - y, xy - x, y^2 - y \rangle$.

Solution. Since

$$\begin{aligned}
\operatorname{spoly}(x^2 - y, xy - x) &= y(x^2 - y) - x(xy - x) \\
&= y^2 - y \in I \\
\operatorname{spoly}(x^2 - y, y^2 - y) &= y^2(x^2 - y) - x^2(y^2 - y) \\
&= x^2 y - y^3 = y(x^2 - y) - y(y^2 - y) \in I \\
\operatorname{spoly}(xy - x, y^2 - y) &= y(xy - x) - x(y^2 - y) \\
&= 0 \in I\,,
\end{aligned}$$

the Buchberger criterion establishes that the three polynomials are a Gröbner basis. □

2.2.4 Proposition (Buchberger second criterion)**.** *For any two polynomials g_1 and g_2 in the ring S such that* $\gcd\big(\operatorname{LM}(g_1), \operatorname{LM}(g_2)\big) = 1$*, we have*

$$\operatorname{spoly}(g_1, g_2) \,\%\, [g_1 \;\; g_2]^{\mathsf{T}} = 0\,.$$

Proof. For all $1 \leqslant j \leqslant 2$, set $\widetilde{g}_j := g_j - \operatorname{LT}(g_j)$. It follows that

$$\begin{aligned}
&\operatorname{spoly}(g_1, g_2) \\
&= \frac{\operatorname{lcm}\big(\operatorname{LM}(g_1), \operatorname{LM}(g_2)\big)}{\operatorname{LT}(g_1)} g_1 - \frac{\operatorname{lcm}\big(\operatorname{LM}(g_1), \operatorname{LM}(g_2)\big)}{\operatorname{LT}(g_2)} g_2 \\
&= \frac{\operatorname{LM}(g_2)}{\operatorname{LC}(g_1)\gcd\big(\operatorname{LM}(g_1), \operatorname{LM}(g_2)\big)} g_1 - \frac{\operatorname{LM}(g_1)}{\operatorname{LC}(g_2)\gcd\big(\operatorname{LM}(g_1), \operatorname{LM}(g_2)\big)} g_2 \\
&= \frac{1}{\operatorname{LC}(g_1)} \operatorname{LM}(g_2)\, g_1 - \frac{1}{\operatorname{LC}(g_2)} \operatorname{LM}(g_1)\, g_2 \\
&= \frac{1}{\operatorname{LC}(g_1)\operatorname{LC}(g_2)} \big((g_2 - \widetilde{g}_2) g_1 - (g_1 - \widetilde{g}_1) g_2\big) \\
&= \frac{1}{\operatorname{LC}(g_1)\operatorname{LC}(g_2)} (\widetilde{g}_1\, g_2 - \widetilde{g}_2\, g_1) \in \langle g_1, g_2 \rangle\,.
\end{aligned}$$

□

Observe that

$$\gcd(x^u, x^v) \operatorname{lcm}(x^u, x^v) = x^u\, x^v\,.$$