

GRÖBNER BASES

AMBAREESH SHYAM SUNDAR

ABSTRACT. We introduce Gröbner bases as a tool for solving systems of polynomial equations, motivated by the idea of generalizing Gaussian elimination. Along the way, we provide various applications of Gaussian elimination to abstract algebra and computational algebraic geometry.

1. INTRODUCTION

Let K be an algebraically closed field, and let $f_1, \dots, f_k \in R = K[x_1, \dots, x_n]$. Recall that the set of roots of $\{f_1, f_2, \dots, f_k\}$ is the affine variety $V(I) = V(\langle f_1, f_2, \dots, f_k \rangle)$. While affine varieties are a central object of study in algebraic geometry, they are not always easy to visualize and deal with computationally, as solving systems of polynomials is not a particularly simple task. However, it turns out that there is an efficient (polynomial-time) algorithm for solving such systems.

To observe how such an algorithm might arise, let us first consider the simpler case in which the f_i are linear polynomials. The standard method to compute $V(I)$ is Gaussian elimination. Writing each f_i as $c_{i,1}x_{i,1} + c_{i,2}x_{i,2} + \dots + c_{i,n}x_{i,n}$, we can write the system as

$$\begin{pmatrix} c_{1,1} & c_{1,2} & \cdots & c_{1,n} \\ c_{2,1} & c_{2,2} & \cdots & c_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ c_{k,1} & c_{k,2} & \cdots & c_{k,n} \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$$

Using elementary row operations, we can convert the coefficient matrix $C = (c_{i,j})$ into reduced row-echelon form. This row-reduced matrix encodes an equivalent set of relations (in other words, a canonical set of generators for I). For any $m \geq 1$, looking at the last m rows of this row-reduced matrix gives a unique solution for the last m variables. We obtain this solution by back-substituting row k into row $k - 1$, then back-substituting the resulting relations into row $k - 2$, and so on. Note that we have implicitly chosen an ordering of the monomials based on the order in which we back-substitute them – in this case, $x_n < x_{n-1} < \dots < x_1$.

Wishful thinking might lead one to consider a similar approach when the f_i are not linear (say, of maximum degree $d \geq 2$) – fix some ordering on the monomials of degree at most d , write the coefficient matrix $(c_{i,j})$, where $c_{i,j}$ is the coefficient of monomial j in f_i , row reduce, and back-substitute. Unfortunately, this fails to account for the fact that in degree 2 and higher, there exist relations between monomials that must be satisfied. For example, we must always have that

$$\frac{(x_1^2 x_2)(x_1 x_2^2)}{(x_1 x_2)^3},$$

but the values computed by row-reduction may not satisfy this. Therefore, we need an alternative to row-reduction that can produce a canonical generating set for I that takes these relations into account.

2. DEFINITIONS

For notational convenience, write $R = K[x_1, \dots, x_n]$, and let M_R be the set of monomials in R . Our first order of business is to fix an ordering on M_R that satisfies some useful properties.

Definition 2.1. A *monomial order* is a total order $\leq$ on M_R that satisfies the following properties:

(M1) For any $m \in M_R$, $1 \leq m$.

(M2) If $m_1, m_2 \in M_R$ and $m_1 \leq m_2$, then for any $m_3 \in M_R$, $m_1 m_3 \leq m_2 m_3$.

The following combinatorial result due to L. E. Dickson [1], which we state without proof, will be instrumental in the study of monomial orders.

Theorem 2.2. (*Dickson's lemma.*) Let $\preceq$ be a partial order on $\mathbb{N}^n$, where $(a_1, \dots, a_n) \preceq (b_1, \dots, b_n)$ if and only if $a_i \leq b_i$ for all $i \in [n]$. Then $\mathbb{N}^n$ has finitely many minimal elements with respect to $\preceq$.

There is a natural bijection $\text{ev} : M_R \rightarrow \mathbb{N}^n$: the monomial $\prod_{i=1}^n x_i^{a_i}$ maps to the tuple $(a_1, \dots, a_n)$. (Here, ev stands for “exponent vector”.) For any $p, q \in M_R$, $p \mid q$ if and only if $\text{ev}(p) \preceq \text{ev}(q)$. Then by Dickson's lemma, M_R (thought of as a poset ordered by divisibility) contains only finitely many minimal elements.

Armed with Dickson's lemma, we can now prove a desirable property of monomial orderings.

Theorem 2.3. Let $\leq$ be a monomial order. Any descending chain in M_R under $\leq$ stabilizes.

Proof. Let $m_1 \geq m_2 \geq \dots$ be a descending chain in M_R . Let $m_{i_1}, \dots, m_{i_r}$ be the minimal elements of the set $\{m_1, m_2, \dots\}$ ordered by divisibility. Then for any $j > i_r$, there exists some $k \in [r]$ for which $m_{i_k} \mid m_j$. If $m_{i_k} \mid m_j$, then m_j/m_{i_k} is a monomial in R . By property (M1), $1 \leq m_j/m_{i_k}$; then by property (M2), $m_{i_k} \leq (m_j/m_{i_k}) \cdot m_{i_k} = m_j$. But since $j > i_r$, we must have $j > i_k$, and so $m_{i_k} \geq m_j$. It follows that $m_{i_k} = m_j$. Therefore, for any $j_1, j_2 \geq i_r$, $m_{j_1} = m_{j_2}$. $\square$

To make the discussion of monomial orders more tangible, we introduce a standard monomial order known as the *pure lexicographic order*.

Definition 2.4. Let $p = \prod_{i=1}^n x_i^{a_i}$ and $q = \prod_{i=1}^n x_i^{b_i}$ be two monomials in M_R . Let j be the smallest index i such that $a_i \neq b_i$. Under the *pure lexicographic order*, $p < q$ if and only if $a_j < b_j$.

Equivalently, $p < q$ if and only if the tuple $(a_1, \dots, a_n)$ appears before $(b_1, \dots, b_n)$ in dictionary order.

For the remainder of this section, $\leq$ refers to the pure lexicographic order.

Given a polynomial $f \in R$, we define the *leading term* of f , written $\text{lt}(f)$, as the additive term with the largest monomial with respect to $\leq$. The *leading coefficient* $\text{lc}(f)$ and *leading monomial* $\text{lm}(f)$ are defined analogously. For example, if $f = 2x_1^3x_2^2 + x_1^2x_2^4 + x_1x_3$, we would have

$$\text{lt}(f) = 2x_1^3x_2^2, \quad \text{lc}(f) = 2, \quad \text{lm}(f) = x_1^3x_2^2.$$

In particular, $\text{lt}(f) = \text{lc}(f) \cdot \text{lm}(f)$.

Fix an ideal $I = \langle f_1, \dots, f_k \rangle \subseteq R$. We can define the *initial ideal* I^{in} as the ideal generated by all leading terms of polynomials in I ; that is,

$$I^{\text{in}} = \langle \text{lt}(f) : f \in I \rangle.$$

Since K is a field, $\langle \text{lt}(f) : f \in I \rangle = \langle \text{lm}(f) : f \in I \rangle$.

Definition 2.5. A *Gröbner basis* of I is a set of polynomials $g_1, \dots, g_m \in I$ such that $\langle g_1, \dots, g_m \rangle = I^{\text{in}}$.

We begin with some elementary observations about Gröbner bases. As in Section 1, consider the case in which I is generated by linear polynomials with coefficient matrix C . Let C' be the reduced row-echelon form of C . Then the linear polynomials encoded by C' form a Gröbner basis for I : since elementary row operations on C correspond to addition and scalar multiplication in $K[x_1, \dots, x_n]$, the pivots columns correspond exactly to the monomials that can occur in the leading terms of polynomials in I .

As an easy consequence of Dickson's lemma, we get the following general result:

Theorem 2.6. *Let $I \in R$. Then I has a Gröbner basis.*

Proof. Let $S = \{\text{lt}(f) : f \in I\}$. By Dickson's lemma, S (partially ordered by divisibility) has finitely many minimal elements $g_1, \dots, g_m$. Then $\langle g_1, \dots, g_m \rangle$ contains S , and therefore contains I^{in} . $\square$

Even in the linear case, one cannot obtain a Gröbner basis for I simply by taking the initial terms of all the generators of I . For example, let $I = \langle x_1, x_1 + x_2 \rangle$. Then I contains both x_1 and x_2 , and so does I^{in} ; but $\langle \text{lm}(x_1), \text{lm}(x_1 + x_2) \rangle = \langle x_1 \rangle$. The converse, however, is true:

Theorem 2.7. *Let $I \subseteq K[x_1, \dots, x_n]$ be an ideal and $g_1, \dots, g_m$ a Gröbner basis of I . Then $\langle g_1, \dots, g_m \rangle = I$.*

Proof. By definition, $\langle g_1, \dots, g_m \rangle \subseteq I$. To prove the reverse inclusion, choose an arbitrary $f \in I$. Then $\text{lt}(f) \in I^{\text{in}}$; in particular, there exists some monomial u and an integer $j \in [m]$ such that $u \cdot \text{lt}(g_j) = \text{lt}(f)$.

We wish to show that $f \in \langle g_1, \dots, g_m \rangle$. We proceed by induction. We can write a polynomial h that satisfies $\text{lm}(h) < \text{lm}(f)$ as follows:

$$h = f - \text{lc}(f) \cdot \text{lc}(g_j)^{-1} \cdot u g_j$$

By construction, the coefficient of $\text{lm}(f)$ in h is 0, so $\text{lm}(h) < \text{lm}(f)$.

The base case is when $h = 0$; then $f = \text{lc}(f) \cdot \text{lc}(g_j)^{-1} \cdot u g_j$, which means $f \in \langle g_1, \dots, g_m \rangle$.

For the inductive step, assume that for all $f' \in R$ that satisfy $\text{lm}(f') < \text{lm}(f)$, $f' \in \langle g_1, \dots, g_m \rangle$. Then by this hypothesis, $h \in \langle g_1, \dots, g_m \rangle$. Since $f = h + \text{lc}(f) \cdot \text{lc}(g_j)^{-1} \cdot u g_j$, $f \in \langle g_1, \dots, g_m \rangle$ as well. $\square$

The combination of Theorem 2.6 and Theorem 2.7 suffices to prove Hilbert's basis theorem for fields:

Theorem 2.8. (*Hilbert's basis theorem.*) *Let K be a field. Then $K[x_1, \dots, x_n]$ is Noetherian.*

Proof. A ring is Noetherian if and only if every ideal is finitely generated. Let $I \subseteq K[x_1, \dots, x_n]$ be an ideal. By Theorem 2.6, I has a Gröbner basis, which is finite by definition. By Theorem 2.7, the Gröbner basis generates I . Therefore I is finitely generated. $\square$

3. BUCHBERGER'S ALGORITHM

While Theorem 2.6 guarantees the existence of a Gröbner basis for every ideal, it does not provide a method by which one can compute a Gröbner basis for a given ideal. Such an algorithm would be desirable not only for the purposes of

computational algebraic geometry, but also as a constructive proof of Hilbert's basis theorem. In this section, we discuss Buchberger's algorithm, which solves the aforementioned problem.

Let $I = \langle f_1, f_2 \rangle$. We know that $\{f_1, f_2\}$ is not necessarily a Gröbner basis of I ; however, any element of I^{in} not in $\langle \text{lt}(f_1), \text{lt}(f_2) \rangle$ must be the initial term of a linear combination of f_1 and f_2 that kills the leading term of both generators.

The S -polynomial of f_1 and f_2 is a canonical example of this. Define

$$S(f_1, f_2) = \frac{\text{lcm}(\text{lm}(f_1), \text{lm}(f_2))}{\text{lt}(f_1)} f_1 - \frac{\text{lcm}(\text{lm}(f_1), \text{lm}(f_2))}{\text{lt}(f_2)} f_2.$$

Intuitively, if $S(f_1, f_2)$ can be expressed as a linear combination of polynomials $g_1, \dots, g_m$, then $g_1, \dots, g_m$ is, in some sense, close to being a Gröbner basis of I . To formalize this idea, we introduce the concept of *reductions* of multivariate polynomials.

Whereas a univariate polynomial ring $K[x]$ is a Euclidean domain and therefore admits a division algorithm, $K[x_1, \dots, x_n]$ is not a Euclidean domain for $n \geq 2$. Therefore, there is no canonical multivariate polynomial division algorithm. However, we may define a generalization of Euclidean division as follows:

Definition 3.1. Let $f, g \in K[x_1, \dots, x_n]$. We say f is *reducible* by g if some monomial m of f is divisible by $\text{lm}(g)$. Let c be the coefficient of m in f . Then the reduction of f by g is defined as

$$\text{red}(f, g) = f - \frac{cm}{\text{lt}(g)} \cdot g.$$

If $G = \{g_1, \dots, g_m\}$, then the reduction of f by G is computed by reducing f by g_1 as much as possible, then by g_2 , and so on, until g_m . This produces a sequence of polynomials $h_1, \dots, h_m$ and a *remainder* polynomial r such that

$$f = h_1 g_1 + \dots + h_m g_m + r.$$

Two important properties of polynomial reduction must be noted. First, reducibility is defined only with respect to a given monomial order, and therefore changing the monomial order can change the value of $\text{red}(f, g)$. Second, even with some fixed monomial order, the reduction of f by G depends on the order of the polynomials $g_1, \dots, g_m$. For example, let $f = x_1 x_2 + x_2^2$, $g_1 = x_1 + x_2$, and $g_2 = x_1$. Then reducing by g_1 and then g_2 gives $f = x_2 \cdot g_1$, but reducing by g_2 and then g_1 gives $f = x_2 \cdot g_2 + x_2^2$.

A central motivating result in the study of Gröbner bases is that there is no such ordering requirement when reducing by a Gröbner basis.

Theorem 3.2. Let $g_1, \dots, g_m$ be a Gröbner basis for $I \subseteq K[x_1, \dots, x_n]$. Let $f \in K[x_1, \dots, x_n]$. Then the remainder of the reduction of f by $\{g_1, \dots, g_m\}$ is independent of the order of the $g_1, \dots, g_m$.

Proof. We proceed by contradiction. Assume f can be written in two different ways as a linear combination of g_i plus a remainder; that is,

$$f = r + \sum_{i=1}^m h_i g_i = r' + \sum_{i=1}^m h'_i g_i,$$

where $r \neq r'$ and r and r' are not reducible by any g_i . Then $r - r' \in I$, so $\text{lt}(r - r') \in I^{\text{in}}$. Since $\text{lt}(g_i)$ generate I^{in} , we have that some $\text{lt}(g_i)$ divides $\text{lt}(r - r')$. But this means $\text{lt}(g_i)$ divides a term of $r - r'$, which means it divides a term of r or

r' . This contradicts the assumption that r and r' are not reducible by any g_i . Therefore we must have $r = r'$. $\square$

Now that we have a well-defined notion of what it means for a polynomial to be reducible by a Gröbner basis, we can state Buchberger's criterion [1].

Theorem 3.3. *Let $I = \langle g_1, \dots, g_m \rangle \subseteq K[x_1, \dots, x_n]$. Then $G = \{g_1, \dots, g_m\}$ is a Gröbner basis of I if and only if, for all $i < j$, the remainder of the reduction of $S(g_i, g_j)$ with respect to G is 0.*

For the sake of brevity, we omit the proof of this theorem, as is long and fairly computational.

Buchberger's criterion allows us to formulate an algorithm to compute a Gröbner basis of an ideal $I = \langle f_1, \dots, f_k \rangle$. We start with the set $G = \{f_1, \dots, f_k\}$. At each step, we compute the S -polynomials $S(f, f')$ for each $f, f' \in G$. If they all reduce to 0 with respect to G , then G is a Gröbner basis; otherwise, we add to G one of the S -polynomials that does not reduce to 0.

To see that this algorithm terminates, note that the ideal generated by $\{\text{lt}(g) : g \in G\}$ is always a subset of I^{in} , and furthermore, adding to G an S -polynomial that does not reduce to 0 makes the ideal strictly larger. Since $K[x_1, \dots, x_n]$ is Noetherian, it satisfies the ascending chain condition: every infinite ascending chain of ideals stabilizes. Therefore, there must be a step at which adding an S -polynomial with nonzero remainder to G would violate the ascending chain condition, so at this step, every S -polynomial must reduce to 0.

While Buchberger's algorithm is guaranteed to produce a Gröbner basis, it has the unfortunate downside that the basis produced need not be unique. For example, the basis can change depending on the choice of S -polynomial at each step; similarly, adding extra polynomials in I to an existing Gröbner basis produces yet another Gröbner basis. To obtain a single canonical Gröbner basis for a given ideal (analogous to reduced row-echelon form for linear systems), it is necessary to perform one more reduction step.

Definition 3.4. Let I be an ideal and $G = \{g_1, \dots, g_m\}$ be a Gröbner basis of I . G is a *reduced Gröbner basis* if $\text{lc}(g) = 1$ for all $g \in G$, and for all $g_i, g_j \in G$, g_i is not reducible by g_j .

Theorem 3.5. *Every ideal $I \subseteq K[x_1, \dots, x_n]$ has a unique reduced Gröbner basis [1].*

We describe (without proof) a method to convert an arbitrary Gröbner basis into a reduced Gröbner basis. First, we convert the Gröbner basis $G = \{g_1, \dots, g_m\}$ into a *minimal* Gröbner basis by iteratively removing any polynomial $g \in G$ for which there exists a $g' \in G$ such that $\text{lm}(g') \mid \text{lm}(g)$. Then, for each i in 1 to m , we reduce g_i by $G \setminus \{g_i\}$ to obtain a remainder r_i , then replace g_i by r_i in G . The resulting set is a reduced Gröbner basis for I .

4. APPLICATIONS

We conclude our discussion of Gröbner bases by presenting a few applications to computational algebraic geometry.

4.1. Ideal membership.

Gröbner bases provide us a convenient algorithm to determine whether a given $f \in K[x_1, \dots, x_n]$ lies within an ideal $I \subseteq K[x_1, \dots, x_n]$.

Theorem 4.1.1. *If $G = \{g_1, \dots, g_m\}$ is a Gröbner basis of I , then $f \in I$ if and only if the remainder of the reduction of f with respect to G is 0.*

Proof. If the remainder is 0, then f is a linear combination of g_i , so by Theorem 2.7, $f \in I$. Conversely, if $f \in I$, then f can be written as a linear combination of g_i , and so reduces to 0 for some ordering of the g_i ; then by Theorem 3.2, it must reduce to 0 regardless of the order of the g_i . $\square$

Therefore, given any Gröbner basis G of I , we can determine whether $f \in I$ by ordering the elements of G arbitrarily and reducing f by each element in sequence, and comparing the remainder of this reduction to 0.

4.2. Intersection of ideals.

If I and J are arbitrary ideals in $K[x_1, \dots, x_n]$, then $I \cap J$ and $I + J = \{f + g : f \in I, g \in J\}$ are ideals in $K[x_1, \dots, x_n]$ as well. While it is straightforward to compute a generating set for $I + J$ (simply take the union of the generating sets of I and J), the same cannot be said for $I \cap J$. Fortunately, Gröbner bases prove quite useful in this scenario.

Let t be an indeterminate, and consider the polynomial ring $K[t, x_1, \dots, x_n]$. Let $M = tI + (1 - t)J \subseteq K[t, x_1, \dots, x_n]$.

Theorem 4.2.2. $I \cap J = M \cap K[x_1, \dots, x_n]$.

Proof. Let $f \in I \cap J$. Then clearly $f \in K[x_1, \dots, x_n]$. Also, since $f \in I$, we have that $tf \in tI$, and similarly $(1 - t)f \in (1 - t)J$; then

$$f = tf + (1 - t)f \in tI + (1 - t)J = M.$$

It follows that $f \in M \cap K[x_1, \dots, x_n]$, so $I \cap J \subseteq M \cap K[x_1, \dots, x_n]$.

Now let $f \in M \cap K[x_1, \dots, x_n]$. Since $f \in M$, write $f = tg + (1 - t)h$, where $g \in I$ and $h \in J$. Since $f \in K[x_1, \dots, x_n]$, f does not depend on the value of t . This means

$$f = f|_{t=0} = h \in J$$

$$f = f|_{t=1} = g \in I$$

so $f \in I \cap J$. Then $M \cap K[x_1, \dots, x_n] \subseteq I \cap J$.

Therefore $I \cap J = M \cap K[t, x_1, \dots, x_n]$, as desired. $\square$

Let G be a Gröbner basis of M with respect to the pure lexicographical order (with $t > x_1 > \dots > x_n$). The following *elimination theorem* tells us that we can just delete the basis elements with t terms to obtain a generating set for $I \cap J$.

Theorem 4.2.3. *If G is a Gröbner basis of $M \subseteq K[t, x_1, \dots, x_n]$, then $G' := G \cap K[x_1, \dots, x_n]$ is a Gröbner basis of $M' := M \cap K[x_1, \dots, x_n]$.*

Proof. We know that the ideal generated by G' is a subset of M' , so the ideal generated by $\{\text{lt}(g) : g \in G'\}$ is a subset of $(M')^{\text{in}}$. It remains only to prove the reverse inclusion. Let $f \in M'$. We wish to show that $\text{lt}(f)$ is contained in the ideal generated by G' . Note that $\text{lm}(f)$ must be divisible by $\text{lm}(g)$ for some $g \in G$. Since $\text{lm}(f)$ is a monomial in $K[x_1, \dots, x_n]$, $\text{lm}(g)$ must be as well. But if the leading monomial of g does not contain t as a factor, then neither does any term of g , as t appears before any other variable in the lexicographical order chosen. Therefore $g \in M'$. $\square$

4.3. Solving systems of polynomial equations.

Applying Theorem 4.2.3 inductively tells us that we can eliminate any number of variables after fixing a variable ordering. We can use this to solve systems of polynomial equations.

Consider the system

$$\begin{cases} -y + x - 1 = 0 \\ y^2 + x^2 - 5 = 0 \end{cases}$$

with the lexicographical order using $y > x$. Using Buchberger's algorithm (or with the help of software like SageMath), we can determine that the ideal $I = \langle y^2 + x^2 - 5, -y + x - 1 \rangle$ has Gröbner basis $\{y^2 + y - 2, -y + x - 1\}$. Similar to Gaussian elimination, we can solve this system using the Gröbner basis by back-substitution. With y isolated, we obtain $y \in \{-2, 1\}$; substituting this back into the second generator, we get that $(x, y) \in \{(-1, -2), (2, 1)\}$.

5. CONCLUSION

We hope this has served as a useful introduction to the study of Gröbner bases and their applications. For a much more in-depth treatment of Gröbner basis theory, and a variety of deep applications in algebra, algebraic geometry, and combinatorics, the interested reader is encouraged to look at [1].

REFERENCES

1. Ene, V., Herzog, J.: Grobner bases in commutative algebra. American Mathematical Soc. (2011)
2. Ottem, J.: intersection of ideals in a commutative ring vs their product, <https://mathoverflow.net/q/49271>
3. Adamchik, V.: Gröbner bases, <https://www.andrew.cmu.edu/course/15-355/lectures/lecture11.pdf>
4. Hines, R.: Groebner bases and applications, https://math.colorado.edu/~rohi1040/expository/groebner_bases.pdf
5. Wikipedia contributors: Gröbner basis — Wikipedia, The Free Encyclopedia, https://en.wikipedia.org/w/index.php?title=Gr%C3%B6bner_basis&oldid=1307890806