Gröbner Bases

Joey Huang

July 6, 2020

1 Summary

In Hilbert's Nullstellensatz, we derive a bijection between the radical ideals of a ring and the algebraic varieties on an affine space. However, given an arbitrary polynomial $h \in R[x_1, \dots, x_n]$ and an ideal $I = (f) \subseteq R[x_1, \dots, x_n]$, a problem that often comes up is whether or not $h \in I$. In the case of $n = 1$, we can use Euclidean polynomial division and check to see if the remainder of $\frac{h}{f}$ is the zero polynomial, but in higher dimensions, this becomes exponentially harder. Therefore, we would like to see if there is another way of representing the ideal I by writing $I = (g)$ with g being easier to work with computationally. We call g the *Gröbner basis* for f.

To define the Gröbner basis, we first have to look at monomial term orders, namely lexicographic ordering and graded lexicographic ordering. Given a term order, we can specify a way to write the polynomial in further calculations. We can also find the initial ideal of a polynomial given a term order, denoted by $in_\prec(f)$, as well as the initial ideal $in_\prec(I) = (in_\prec(f) : f \in I)$.

A finite subset $G \subset I$ is a Gröbener basis if $in_\prec(I) = (in_\prec(g) : g \in G)$, but there is only a single *reduced Gröbner basis* for each ideal I. Buchberger's Criterion tells us that if the normal form of the S-polynomials of a set G is zero, then it's a reduced Gröbner basis; stemming from this, we have Buchberger's Algorithm which can be used to compute the reduced Gröbner basis for any given ideal $I = (f)$.

While Gröbner bases have many important applications in solving systems of multivariate polynomial equations, geometric theorem proving, and graph coloring, it can be effectively used to find solutions to integer programming problems.

2 Motivation for Gröbner Bases

In many cases, we wish to solve systems of polynomial equations. Given polynomials $f_1(x_1, \ldots, x_n), f_2(x_1, \ldots, x_n), \ldots, f_m(x_1, \ldots, x_n) \in \mathbb{C}[x_1, \ldots, x_n]$, we would like to find, *if any*, $(a_1, \ldots, a_n) \in \mathbb{A}^n_{\mathbb{C}}$ such that

$$f_1(a_1, \ldots, a_n) = f_2(a_1, \ldots, a_n) = \cdots = f_m(a_1, \ldots, a_n) = 0$$

Example. Let $f_1 = x_1 + x_2 - 1$ and $f_2 = x_1 - x_2 + 2$. Since there are two variables and two equations, we can solve for the roots of f_1 and f_2. We could use heuristics and see that adding f_1 and f_2 eliminates the x_2 term, but the most usual way to solve systems of linear equations is through *Gaussian elimination*, where we use the term x_1 in f_1 as a pivot to get $f_2 \coloneqq f_2 - f_1 = -2x_2 + 3$. We then use this new term $f_2 = -2x_2 + 3$ as a pivot, $f_1 \coloneqq f_1 + \frac{1}{2} f_2 = x_1 + \frac{1}{2}$. Hence, we can also write the original system of equations by the equivalent system $f_1 = x_1 + \frac{1}{2}$ and $f_2 = -2x_2 + 3$. We shall see in a later section that they are, in fact, Gröbner bases.

3 Monomial Term Orders

In the last section, we solved a system of linear polynomials using Gaussian elimination, which, put into linear algebra terms, are equivalent to finding a reduce row echelon form of $(A|B)$ where A is LHS of the system of linear polynomials and B is the RHS vector. The key to this method was choosing pivot variables for each step, but when we go beyond linearity, this becomes harder to intuitively see. For example, x_1^2 and $x_1 x_2$, which should be used as a pivot first?

Thus, we introduce the notion of *monomial term orders*.

Definition 3.1. A *term order* is a total order $\prec$ on a set of monomials $x_a = x_1^{a_1} x_2^{a_2} \cdots x_n^{a_n}$ such that $x^a \prec x_b \to x^{a+c} \prec x^{b+c}$ (multiplicative) and $1 \prec x^a$ for all $x^a \neq 1$.

Definition 3.2. A **lexicographic order** is the order $\prec$ such that $x^a \prec x^b$ exactly when the first non-zero entry in $b - a$ is positive.
A **graded lexicogrphic order** is the order $\prec$ such that $x^a \prec x^b$ if $\deg x^a < \deg x^b$ or $\deg x^a = \deg x^b$ and the last non-zero entry of $b - a$ is negative.

Example. For $R = k[x_1, x_2, x_3]$ and degree 2, we have the lexicographic order $1 \prec x_1 \prec x_1^2 \prec x_2 \prec \cdots \prec x_3^2$ and the graded lexicogrphic order $1 \prec x_1 \prec x_2 \prec x_3 \prec x_1^2 \prec x_1 x_2 \prec \cdots \prec x_2 x_3$.

Definition 3.3. Given a polynomial f on R and a term order $\prec$, there exists an initial term denoted by $in_{\prec}(f)$ given by the monomial with the "largest" exponent. We also define $in_{\prec}(0) = 0$.

Definition 3.4. Given an ideal $I \subset R$ and a term order $\prec$, the ideal of the initial terms is $in_{\prec}(I) = \{in_{\prec}(f) | f \in I\}$.

Definition 3.5. A finite subset G of an ideal I is a Gröbner basis if $in_{\prec}(I) = \{in_{\prec}(g) | g \in G\}$. A Gröbner basis is called *minimal* if the elements in G minimally generates I.

Example. Let $F = \{x_2^2 - x_1, x_2\}$ and a lexicographic order. F is not a Gröbner basis because $x_1 = x_2 * x_2 - (x_2^2 - x^1) \in in_{\prec}I$, but $x_1 \notin F$.

Lemma 3.6. ***Dickson's Lemma*** *Let S be a set of monomials in $k[x_1, \ldots, x_n]$. Under the order $x^a \prec x^b$ and if $x^a | x^b$, there are only finitely many minimal elements of S.*

Corollary 3.7. *Every monimial ideal in $k[x_1, \ldots, x_n]$ is finitely generated.*

4 Calculating Gröbner bases

Gröbner bases are extremely useful in computational algebraic geometry, because finding the Gröbner basis for a polynomial or an ideal can help us solve algebraic systems of equations, represent polynomials in terms of other polynomials, and construct nonlinear cryptosystems.

Example. Let's try and find the Gröbner basis for the ideal $I = (x^2, xy + y^2)$ with a graded lexicographic order $y \prec x$. We see immediately that $in_{\prec}(I)$ contains x^2 and xy, but what about other elements?We first cancel the lead terms $y(x^2) - x(xy + y^2) = xy^2$, but this is divisible by xy. We then use the term xy^2 to cancel out $xy^2 - y(xy - y^2) = y^3 \in I$, so y^3 is in the Gröbner bais. Using Buchberger's Criterion, we can check that these are the only elements, so $G = \{x^2, xy + y^2, y^3\}$.

4.1 Buchberger's Criterion

Definition 4.1. Let there be two non-zero polynomials p and q where $in(p) = c_1 x^a$ and $in(q) = c_2 x^b$, the S-polynomial

$$S(p, q) = c_2 x^c p - c_1 x^d q$$

where $x^c x^a = x^d x^b$ and $\gcd(x^c, x^d) = 1$.

Theorem 4.2. *[**Buchberger's Criterion**] Let $I \subset R$ be an ideal, and let $G \subset I$ be a finite subset of nonzero polynomials. Then G is a Gröbner basis iff every pair of elements $p, q \in G$, $R_G(S(p, q)) = 0$.*

4.2 Buchberger's Algorithm

From this criterion, we can derive a comprehensive algorithm for finding the Gröbner basis for any polynomial f or ideal I.

Algorithm 1: Buchberger's Algorithm

```
input  : A set $\{f_1, \ldots, f_n\} \subset R$
output: A Gröbner basis G of the ideal generated by $\{f_1, \ldots, f_n\}$
G := $\{f_1, \ldots, f_n\}$;
Pairs := $\{(\mathrm{f}_i, f_j)\ |1 \leq i < j \leq n\}$;
while Pairs $\neq \varnothing$ do
    $(g_i, g_j)$ := remove an element from Pairs;
    $S$ :=$S(g_i, g_j)$;
    $h$ :=$R_G(S)$;
    if $h \neq 0$ then
        Pairs := Pairs $\cup \{(h, g) | g \in G\}$;
        $G := G \cup \{h\}$;
    end
end
return $G$
```

In the last example, we have $p = x^2$ and $q = xy + y^2$. $in(p) = x^2$ and $in(q) = xy$. The S-polynomial $S(x^2, xy + y^2) = y(x^2) - x(xy + y^2) = -xy^2$. $S(xy^2, xy + y^2) = xy^2 - y(xy + y^2) = -y^3$. So the Gröbner basis is $\{x^2, xy + y^2, y^3\}$

5 Linear Programming Applications

Gröbner bases are incredibly useful in problems in operations research, as there are many linear programming equations that can be easily solved using this method.

Example. Given a collection of coins, we can use Gröbner bases to find a minimal combination of coins of the same monetary value. For example, we will try to find a minimal integer solution to

$$P + 5N + 10D + 25Q = 117$$

subject to $P, N, D, Q \geq 0$. We can represent this sum as a product: $f = P^a N^b D^c Q^d$ where P^a represents a pennies.

Since we also have several equivalence equations for the different coins, we can use an ideal to represent all the possible monetary values. Let $F = \{P^5 - N, P^10 - D, P^25 - Q\}$. Using Buchberger's algorithm as described in section 4.2, we find the Gröbner basis to be $G = \{P^5 - N, N^2 - D, D^2 N - Q, D^3 - NQ\}$. In other words, this gives a new set of equivalence relations: always replace two dimes and a nickel with a quarter and 3 dimes with a nickel and a quarter. Since the Gröbner basis is exhaustive, we are sure that there are no simpler solutions. Hence, we can start with 117 pennies and repeatedly use the substitutions to find the minimal set: $P^2 DNQ^4$.