Gröbner Bases on Multivariable Equations and Parabolic Envelopes

Ankita Pednekar

Euler Circle

July 15, 2024

Introduction

Current multi-variable linear equations are solved by Row-Reduction (Gaussian elimination)

$$\begin{aligned} 2x + y + 2z &= 0 \\ x + 3y + z &= 0 \\ 2x + y + z &= 1 \end{aligned} \quad \rightarrow \quad \begin{bmatrix} 2 & 1 & 2 & 0 \\ 1 & 3 & 1 & 0 \\ 2 & 1 & 1 & 1 \end{bmatrix} \quad \rightarrow \quad \begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & -1 \end{bmatrix} \quad \rightarrow \quad \boxed{(1, 0, -1)}$$

Gröbner bases allow for the computation of nonlinear multivariable equations, and was introduced by Bruno Buchberger in his thesis (along with the Buchberger Algorithm). Furthermore, it can be applied to other calculations in mathematics, including finding the parabolic equation for an envelope (as in my paper) to joint mechanics.

Preliminaries: Rings and Ideals

- Rings: a set that is abelian under addition, associative under multiplication, contains its multiplicative identity, and has it's multiplication distributive over addition.
- Ideals: I is a subgroup of R such that for all $r \in R$ and $m \in I$, $mr \in I$.
- A generating set of an ideal means that that every element in the ideal can be written as a linear combination of the elements of the generating set, as below where $f_i \in I$, $a_i \in R$ and $g_i \in G$,

$$f_i = a_1 g_1 + a_2 g_2 + \dots.$$

A special kind of generating set will then be the Gröbner basis!

For the integer ring $\mathbb{Z}$, the ideal will contain all multiples of n. The generator of this set will just be n.

Preliminaries: Ascending Chain Condition

Ascending Chain Condition

Polynomial rings (and Noetherian Rings) satisfies the fact that an initial ideal can be broken up into smaller ideals such that the sequence

$$I_1 \subseteq I_2 \subseteq I_3 \subseteq \ldots$$

will be finite.

For the integer ring (additionally a Noetherian Ring), a possible example ideal will thus be

$$\{\text{multiples of } 8\} \subseteq \{\text{multiples of } 4\} \subseteq \{\text{multiples of } 2\} \subseteq \mathbb{Z},$$

which ends at the maximal ideal, where the ideal is generated by the prime numbers (p).

Preliminaries: Admissible Ordering

Ordering x^n and x^m is easy, but it becomes tricky when ordering multivariable product terms. Admissible ordering orders the terms of the polynomial in these cases.

- Lexicographic ordering: An admissible ordering such that if $x > y$ and $n < n'$ then $x^n y^m < x^{n'} y^{m'}$.
- Leading monomials, denoted as LM, are the greatest monomial found in the lexicographic ordering.

Gröbner Bases

A Gröbner basis can be defined as a set of polynomials when for all $g_i \in G$ and all $f_j \in I$, G denoting the Gröbner basis and I denoting the ideal,

$$LM(g_i) | LM(f_j).$$

As such, each of the leading monomials for the polynomials in the Gröbner basis form linear combinations to generate the ideal.

S-Polynomials

The calculation for a Gröbner basis is dependent on the S-Polynomial:

$$S(f,g) = f \cdot \frac{\text{LCM(LM(f),LM(g))}}{\text{LT(f)}} - g \cdot \frac{\text{LCM(LM(f),LM(g))}}{\text{LT(g)}}.$$

This calculation is repeated for each pair $f, g \in I$ until no further polynomials can be added to the Gröbner basis. Buchberger's Algorithm repeatedly does the S-Polynomial calculation and checks for the remainders of this calculation. If $r \neq 0$, then r is added to G.

Elimination Theorem

Elimination Theorem

If $I \subseteq R[x_1, ..., x_n]$, then the Gröbner basis of the k-th elimination ideal I_k is

$$G_k = G \subseteq R[x_{k+1}, ..., x_n].$$

In the process of solving for the solutions of an equation, the Elimination Theorem limits the variables in the Gröbner basis so that singular variable polynomials in the Gröbner basis can be achieved.

Extension Theorem

Extension Theorem (with the k-th elimination ideal)

If $I = \langle f_1, ..., f_n \rangle \subseteq \mathbb{C}[x_1, ..., x_n]$, each f can be expressed as

$$f_i = c_i(x_{k+1}, ..., x_n)x_k^{N_i}$$

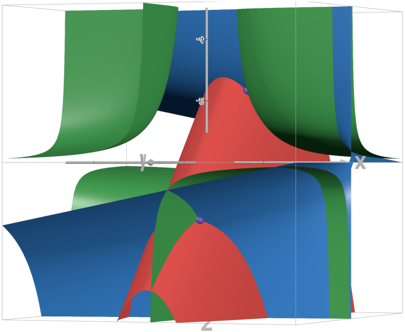
such that $c_i \in \mathbb{C}[x_1, ..., x_n]$ and I_k is the k-th elimination ideal of I. If we have the partial solution $(a_{k+1}, ..., a_n) \in \mathbf{V}(I_k)$ but $(a_{k+1}, ..., a_n) \notin \mathbf{V}(c_1, ..., c_n)$, then there exists such $a_k \in R$ where $(a_1, ..., a_n) \in \mathbf{V}(I)$.

The Extension Theorem then allows for a solution in the smaller elimination ideal, or the Gröbner basis, to be extended into the ideal as a whole.

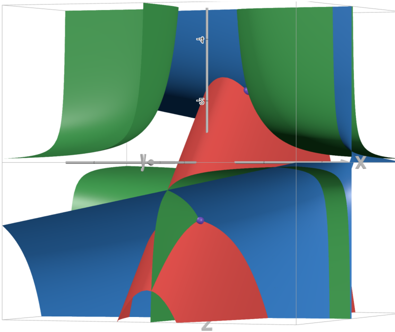
Example

- We have:
  $x^2 + y - z = 1, x + zy = 5,$
  and $xyz = 3$.
- The ideal: $I = \langle x^2+y-z-1, x+zy-5, xyz-3\rangle$
- Calculating the Gröbner bases will then lead to

$$g_1 = z^4 - 17z^3 - 14z^2 + 75z + 3$$
$$g_2 = 104y + 25z^3 - 420z^2 - 434z + 1809$$
$$g_3 = 104x - 5z^3 + 84z^2 + 66z - 445.$$



- The Elimination Theorem turns the initial equations into manageable singular variable polynomial equations
- Set each of the polynomials in the Gröbner basis equal to zero, and then solve. By the Extension Theorem, the solutions for the polynomials in the Gröbner basis will be the solution for the initial equations.
- The solutions then become: $(0.6972, -1.8332, -2.3471)$, $(4.3028, -17.5536, -0.0397)$, $(0.6972, 2.3471, 1.833)$, and $(4.3028, 0.0397, 17.5536)$.



Thank you for listening!