GRÖBNER BASIS

ÖMER FARUK BİTİKÇİOĞLU

161044010

What is Gröbner Basis?

A Gröbner basis is a set of multivariate nonlinear polynomials enjoying certain properties that allow simple algorithmic solutions for many fundamental problems in mathematics and natural and technical sciences.

Examples of such problems are the solution of algebraic systems of equations, the representability of polynomials in terms of other polynomials, the analysis and construction of nonlinear cryptosystems, the closed form summation and integration of expressions involving special functions, the closed form solution of linear boundary value problems (differential equations). Amazingly, also problems that seem to be far away from algebra as, for example, the automated proof and discovery of geometrical theorems, the construction of graph colorings and the solution of Sudoku games can be reduced to Gröbner bases computations. Examples of problems in natural and technical sciences that have recently been solved by the Gröbner bases methodology are intelligent control of oil platforms, reverse engineering of software, finding genetic relationship between species, and solving the inverse robotic kinematics.

Here is a typical example of a Gröbner basis consisting of three polynomials in three variables:

{x3−x2+2, y−2x2+1, z−3x+5}.

In this example, we see one of the advantageous properties of Gröbner bases: The equation system

x3 −x^2 +2 =0

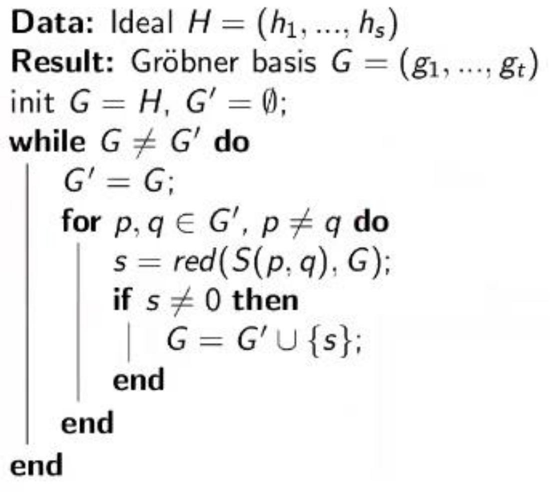
y −2x^2 +1 =0

z −3x +5 =0

in this Gröbner basis form can be easily solved. Namely, one first will find the three possible solutions x of the first equation and then substitute each of these solutions into the second and third equation to determine the corresponding y and z, respectively.

The fundamental insight and contribution of Gröbner bases theory is that every polynomial system, no matter how complicated, can be transformed by an algorithm (Buchberger's algorithm) into Gröbner basis form.

Buchberger's algorithm



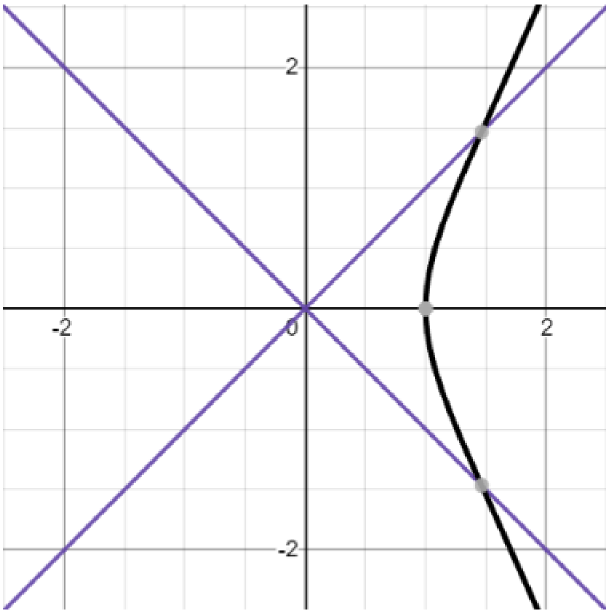
```
Data: Ideal $H = (h_1, \dots, h_s)$
Result: Gröbner basis $G = (g_1, \dots, g_t)$
init $G = H$, $G' = \emptyset$;
while $G \neq G'$ do
    $G' = G$;
    for $p, q \in G'$, $p \neq q$ do
        $s = red(S(p, q), G)$;
        if $s \neq 0$ then
            $G = G' \cup \{s\}$;
        end
    end
end
```

Example

For instance, let’s assume that we have a polynomial system like this:

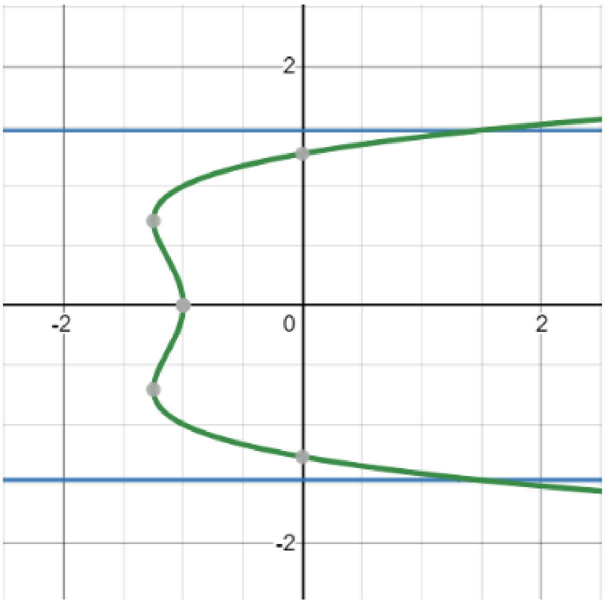
{x^2 -y^2 =0, x^3 -y^2 -1 =0}

It is actually very hard to find their intersecting points in this shape of equations.



But, by using Buchberger’s algorithm we find the Gröbner basis of these equation system and solve them easily. Since corresponding Gröbner basis equations are intersecting at the same points.

G = {y^6 –y^4 -2y^2 -1, x -y^4 +y^2 +1)



Gröbner bases are primarily defined for ideals in a polynomial ring over a field K. Although the theory works for any field, most Gröbner basis computations are done either when K is the field of rationals or the integers modulo a prime number.

A Gröbner basis G of an ideal I in a polynomial ring R over a field is a generating set of I characterized by any one of the following properties, stated relative to some monomial order:

- The ideal generated by the leading terms of polynomials in I equals the ideal generated by the leading terms of G;
- The leading term of any polynomial in I is divisible by the leading term of some polynomial in G;
- The multivariate division of any polynomial in the polynomial ring R by G gives a unique remainder;
- the multivariate division by G of any polynomial in the ideal I gives the remainder 0.

All these properties are equivalent; different authors use different definitions depending on the topic they choose. The last two properties allow calculations in the factor ring R/I with the same facility as modular arithmetic. It is a significant fact of commutative algebra that Gröbner bases always exist and can be effectively computed for any ideal given by a finite generating subset.

Multivariate division requires a monomial ordering, the basis depends on the monomial ordering chosen, and different orderings can give rise to radically different Gröbner bases. Two of the most used orderings are lexicographic ordering, and degree reverse lexicographic order (also called graded reverse lexicographic order or simply total degree order). Lexicographic order eliminates variables, however the resulting Gröbner bases are often very large and expensive to compute. Degree reverse lexicographic order typically provides for the fastest Gröbner basis computations. In this order monomials are compared first by total degree, with ties broken by taking the smallest monomial with respect to lexicographic ordering with the variables reversed.

In most cases (polynomials in finitely many variables with complex coefficients or, more generally, coefficients over any field, for example), Gröbner bases exist for any monomial ordering. Buchberger's algorithm is the oldest and most well-known method for computing them. Other methods are the Faugère's F4 and F5 algorithms, based on the same mathematics as the Buchberger algorithm, and involutive approaches, based on ideas from differential algebra. There are also three algorithms for converting a Gröbner basis with respect to one monomial order to a Gröbner basis with respect to a different monomial order: the FGLM algorithm, the Hilbert-driven algorithm and the Gröbner walk algorithm. These algorithms are often employed to compute (difficult) lexicographic Gröbner bases from (easier) total degree Gröbner bases.

A Gröbner basis is termed reduced if the leading coefficient of each element of the basis is 1 and no monomial in any element of the basis is in the ideal generated by the leading terms of the other elements of the basis. In the worst case, computation of a Gröbner basis may require time that is exponential or even doubly exponential in the number of solutions of the polynomial system (for degree reverse lexicographic order and lexicographic order, respectively). Despite these complexity bounds, both standard and reduced Gröbner bases are often computable in practice, and most computer algebra systems contain routines to do so.