

Abstract

Gröbner bases are a very powerful tool in polynomial algebra and algebraic geometry. Given a Gröbner basis, one can e.g. efficiently solve the ideal membership problem. Significant drawbacks are the big effort needed to compute Gröbner bases and the huge sizes of the Gröbner bases compared to other ideal generators. For many complexity considerations it is necessary to bound the degree of polynomials in a Gröbner basis. My thesis presents the upper bound obtained by Thomas W. Dubé in [2] and also mentions a lower bound.

Polynomial Algebra

In polynomial algebra the object of study is the noetherian ring $K[x_1, \dots, x_n]$ of polynomials in n variables. Especially **ideals** in this ring, i.e. subrings $I \subset K[x_1, \dots, x_n]$ with $I \cdot K[x_1, \dots, x_n] \subset I$, are investigated. A finite generating subset of an ideal is called **basis**.

For the following one needs a **monomial ordering**. This is a total well-ordering of the monomials of $K[x_1, \dots, x_n]$ that respects multiplication.

A simple example is the **lexicographic ordering**. For this purpose we write the monomials as x^α, x^β with multiindices α, β and say that

$$x^\alpha \succ x^\beta \Leftrightarrow \text{The first non-zero entry of } \alpha - \beta \text{ is positive.}$$

Then we call the greatest term of a polynomial (with respect to the monomial ordering) the **leading term**. Additionally we call $|\alpha| = \sum_{i=1}^n \alpha_i$ the **degree** of a polynomial. Of course there can be many different bases of the same ideal. Specially interesting are the so-called **Gröbner bases**. If G is a Gröbner basis of the ideal I , then for every polynomial in I the leading term is a multiple of the leading term of one of the polynomials in G . This definition immediately implies that Gröbner bases depend on the monomial ordering. Especially the computation effort and the size of a Gröbner basis may vary with the monomial ordering.

Gröbner bases have very nice properties. They imply an easy membership algorithm that tests whether a given polynomial is contained in an ideal. With a little effort one can derive a unique representation for an ideal and therefore gets an equality test for ideals. With the so-called Rabinovic trick one can also test whether an arbitrary power of a polynomial is contained in an ideal. This is also called radical membership test.

The problem about Gröbner bases is that they can be very big and that the computation can be very expensive. Since also matching lower bounds are known, the investigation of special subclasses of ideals is suggested.

Results

The main part of my thesis presents the results of Thomas W. Dubé published in [2]. He proves an upper bounds for the degrees of elements in the (reduced) Gröbner basis G of an ideal. This bound depends on the maximum degree d of the generators of the ideal and on the dimension n of the ring. Finally the following theorem is proven.

Theorem. Let G be a reduced Gröbner basis of an ideal $I = \langle f_1, \dots, f_r \rangle$. Let $d = \max \{ \deg(f_1), \dots, \deg(f_r) \}$. Then

$$\max \{ \deg(g) : g \in G \} \leq 2 \left(\frac{d^2}{2} + d \right)^{2^{n-1}}$$

This (or similar) bounds can be used to bound the complexity of the Buchberger algorithm that computes a Gröbner basis for a given ideal.

Sketch of Proof

The most important tool in the proof is the cone decomposition. A **cone** is a translated coordinate subring, i.e. given a monomial m , $m \cdot K[x_{i_1}, \dots, x_{i_s}]$ is a cone. We shortly say degree of the cone for the degree of the monomial m . Then a **cone decomposition** of some subspace is a direct sum of cones that equals the subspace. The aim is now to construct cone decompositions of the given ideal and its normal forms (this is the subspace of the monomials that are not element of the ideal). By giving a construction algorithm for cone decompositions one can now bound the degree of a Gröbner basis by the degrees of the cones in the appropriate cone decomposition.

But this alone is not very useful. The next idea is to use the Hilbert function (the dimension of the homogeneous subspace of degree z) and some combinatorial arguments to bound the degrees of the cone in the decomposition. Since the direct sum of an ideal I and its normal forms N_I is the whole ring, their Hilbert functions sum to the Hilbert function of the whole ring, which is given by a simple formula.

This leads to a formula like this (with φ_T denoting the Hilbert function of T):

$$(1) \quad \varphi_{K[x_1, \dots, x_n]}(z) = \varphi_I(z) + \varphi_{N_I}(z)$$

Also the Hilbert function of cones is very simple. So one could simply write the Hilbert function of the ideal and of the normal forms as sum of the Hilbert functions of the cones in the appropriate cone decompositions.

But for arbitrary cone decompositions one does not know which cones they contain. Therefore special cone decompositions are introduced. For these the Hilbert function can be written as functions of integral parameters.

These parameters are mainly special degree bounds of the cones in the decomposition. Now one can use equation (1) to get upper bounds on these parameters and thus also an upper bound for the Gröbner basis.

Applications

There are different fields of applications.

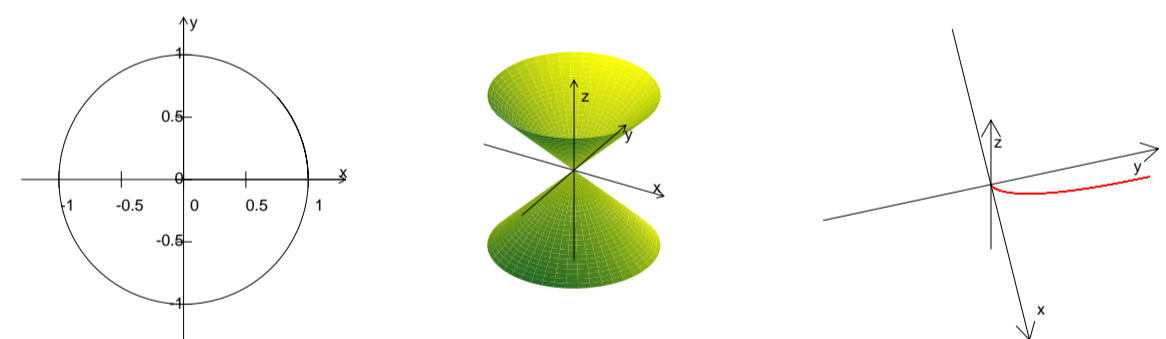
Elimination Theory

Elimination theory deals with solving a set of polynomial equations. As a first easy step variables are eliminated. From an ideal viewpoint this means to intersect an ideal with the subring $K[x_{k+1}, \dots, x_n]$. This can be accomplished by computing a Gröbner basis with respect to the lexicographic monomial ordering and intersecting the basis with the subring.

Another important step is the extension of a solution. Here one has a partial solution in the subring (variables x_{k+1}, \dots, x_n) and wants to know whether one can extend this to a full solution x_1, \dots, x_n that satisfies all polynomials. In many cases this can be guaranteed (though not easily computed).

Algebraic Geometry

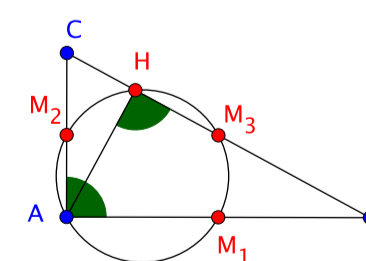
In algebraic geometry one studies the common zeros of a set of polynomials, called **varieties**.



These geometric objects can be combined by operations like intersection, union, set-difference and others. On the other hand one can model these operations algebraically as operations on the ideals generated by the set of defining polynomials. Some of these operations use Gröbner bases as tools. For example, the question whether a polynomial vanishes on a variety reduces to the radical membership test. Also methods of elimination theory apply here in various situations.

Automatic Theorem Proving

Automatic theorem proving in geometry can also often be done with the help of Gröbner bases. The basic idea is to formulate the conditions as polynomial equations in the coordinates of the objects. Then one does the same with the statement to prove. So basically the proof of the statement reduces to the question, whether the statement polynomial is member of the ideal of the condition polynomials. For example one can use this method to prove the circle theorem of Apollonius.



References

- [1] COX, D.A. ; LITTLE, J.B. ; O'SHEA, D.: *Ideals, Varieties, and Algorithms*. Springer New York, 1992
- [2] DUBÉ, T.W.: The Structure of Polynomial Ideals and Gröbner Bases. In: *SIAM Journal on Computing* 19 (1990), p. 750