

Introduction

A polynomial ideal I is a subset of a polynomial ring $k[x_1, \dots, x_n]$ with the properties

- $f, g \in I \Rightarrow f + g \in I$
- $f \in I \Rightarrow h \cdot f \in I \forall h \in k[x_1, \dots, x_n]$

Polynomial ideals are usually specified by giving their generators:

$$(f_1, \dots, f_s) = \left\{ \sum_{i=1}^s h_i f_i : h_i \in k[x_1, \dots, x_n] \right\}$$

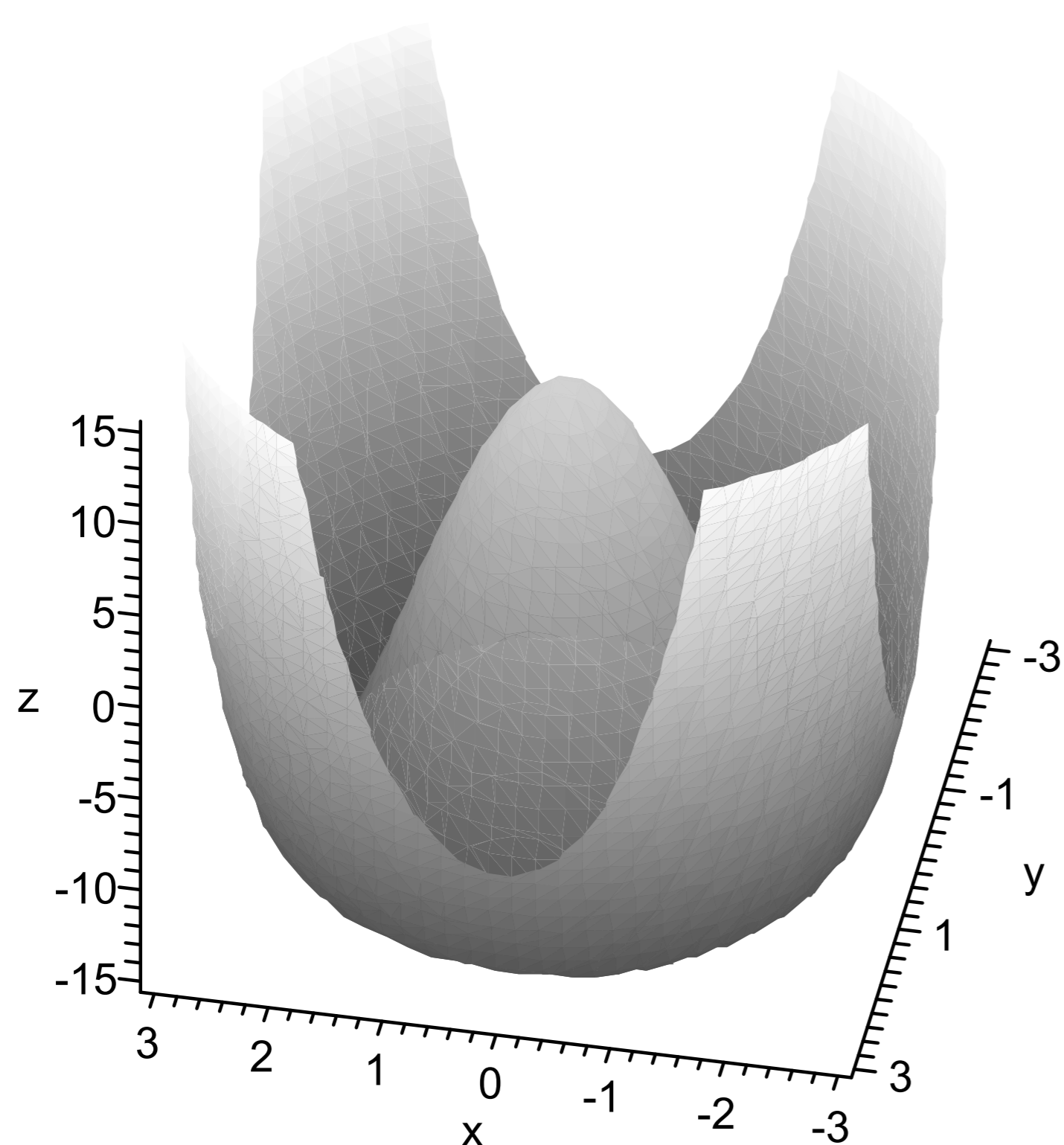
We will consider the *variety* $\mathbf{V}(I)$ of an ideal $I = (f_1, \dots, f_s)$, the subset of k^n on which all polynomials in I vanish. Note that

$$f(x) = 0 \forall f \in I \Leftrightarrow f_i(x) = 0 \forall i = 1, \dots, s.$$

This means that $\mathbf{V}(I)$ is the set of solutions of the system of polynomial equations

$$f_i(x_1, \dots, x_n) = 0 \forall i = 1, \dots, s$$

Example



The solution set of $.7 * (x^2 + y^2)^2 - 8 * (x^2 + y^2) + 8 - z = 0$

Objective

It is already possible to solve many problems involving polynomial ideals by using Gröbner bases. However the computing a Gröbner basis is very expensive, i.e. exponential space complete ([1]).

Our goal is to find specialized algorithms that compute only some specific properties of a polynomial ideal but require less space.

Dimension of a polynomial ideal

Intuitively the dimension of a polynomial is the geometrical dimension of its variety. The rigorous algebraic definition states that:

The dimension of an ideal I is the maximal number of independent variables modulo I , where variables x_{i_1}, \dots, x_{i_r} are called independent modulo I if the ideal I contains no non-zero polynomial involving only these variables. We call such polynomials *witness polynomials*.

Computing the dimension

The dimension can now be computed by checking whether the ideal contains such witness polynomials, i.e. whether the equation

$$g - \sum_{i=1}^s g_i f_i = 0,$$

where g, g_i are unknown polynomials has solutions such that g is non-zero and contains only certain variables. By comparison of coefficients we obtain a system of linear equations of the form

$$g_t - \sum_{i=1}^s \sum_{uv=t} f_{i,u} g_{i,v} = 0,$$

where $f_{i,u}$ is the coefficient of the monomial u in f_i etc. However there are a priori infinitely many monomials that may occur, yielding infinitely many equations in infinitely many unknowns. A result by Bronawell ([2]) can be used to show that if there are witness polynomials at all, one can be found within a certain degree bound. This reduces the number of equations and unknowns to finitely many and allows us to write the system in standard matrix form. By using algorithms for calculating the rank of a matrix in low parallel time and applying the Parallel Computation Thesis [3] we obtain from it an algorithm which computes the dimension of a polynomial ideal with $k = \mathbb{Q}$ in working space polynomial in the input size.

References

- [1] Ernst W. Mayr. Membership in polynomial ideals over \mathbb{Q} is exponential space complete. In B. Monien and R. Cori, editors, *Proceedings of the 6th Annual Symposium on Theoretical Aspects of Computer Science (Paderborn, FRG, February 1989)*, volume 349 of *Lecture Notes in Computer Science*, pages 400-406. GI, afcet, Springer-Verlag, 1989.
- [2] W. Dale Brownawell. Bounds for the degrees in the Nullstellensatz. *Ann. of Math*, 126:577-591, 1987.
- [3] S. Fortune and J. Wyllie. Parallelism in random access machines. In *Proceedings of the 10th Ann. ACM Symposium on Theory of Computing (San Diego, CA)*, pages 114-118, New York, 1978. ACM, ACM Press.