Abstract

One of the main problems in real algebraic geometry is root counting. Given a polynomial, we want to count the number of roots that satisfies constraints expressed as polynomial inequalities. A naive way is to compute an exponential number of time consuming quantities, called Tarski Queries. In this paper, we formalize an algorithm which allows to compute a linear number of them. We formally build a linear system, and we prove in Coq that the system is of small size. The proof that the solutions of this system are the numbers of roots satisfying the constraints is still ongoing.

Introduction

One of the main algorithms in real algebraic geometry is the cylindrical algebraic decomposition [4]. The purpose of such an algorithm is to give a precise representation of a partitioning of the space described by polynomial equations.

Many algorithms that are connected to the task of finding such a decomposition are described in a book by Basu, Pollack and Roy [1], which we use as a reference on algorithms in real algebraic geometry. In this talk we focus on the formalization one of the sign determination algorithms described in this book. The purpose of this algorithm is to count the number of roots of a given polynomial, that satisfy polynomial constraints. The standard way to compute such quantities is by linear combinations of Tarski Queries. The Tarski Query of two polynomials is an integer that can be computed using the coefficients of the numerator and denominator of the fraction.

Tarski queries and counting roots

Given a polynomial $P$ we consider the roots of, and a polynomial $Q$ which expresses sign constraints on the roots of $P$, the Tarski Query can be defined as follows:

$$\text{TaQ}(P, Q) = \sum_{x \in \text{roots}(P)} \text{sign}(Q(x)).$$

Although there is an algorithmic way to compute this quantity using the coefficients of $P$ and $Q$, we do not explain this here for the sake of readability. One can find detailed explanation on how to do so in [1, 3, 2].

The number of roots of $P$ such that $Q$ has sign $\sigma \in \{-1, 0, +1\}$ can be expressed as:

$$\text{cnt}(P, Q, \sigma) = \sum_{x \in \text{roots}(P) \atop \text{sign}(Q(x)) = \sigma} 1.$$
Hence, one can express Tarski Queries in terms of the number of roots in the following way:

\[
(TaQ(P, 1) \quad TaQ(P, Q) \quad TaQ(P, Q^2)) = \begin{pmatrix}
\text{cnt}(P, Q, 0) & \text{cnt}(P, Q, +1) & \text{cnt}(P, Q, -1)
\end{pmatrix} \cdot \begin{pmatrix}
1 & 0 & 0 \\
1 & 1 & 1 \\
1 & -1 & 1
\end{pmatrix}
\]

More generally, given a family \( Q \) of \( n \) polynomials \( Q_1, \ldots, Q_n \), and a family of sign constrains \( \sigma \in \{-1, 0, 1\}^n \) one can express the Tarski Query \( TaQ(P, Q^\alpha) \), in terms of \( \text{cnt}(P, Q, \sigma) \) using a linear transformation, where \( \alpha \in \{0, 1, 2\}^n \),

\[
Q^\alpha = \prod_i Q_i^{\alpha_i},
\]

and

\[
\text{cnt}(P, Q, \sigma) = \sum_{x \in \text{roots}(P)} 1, \quad \forall i, \text{sign}(Q_i(x)) = \sigma_i.
\]

We formalize the linear transformation as a matrix in Coq/SSReflect and we prove that the size of this matrix has the required bounds. The proof that this matrix is invertible is still in progress, but we influenced the writing of the paper proof in the process of writing the formal proof.

The formalization we describe here is intended as a replacement for a piece of code used in a previous work of the first author [3, 2]. Indeed, in this previous work, we use a naive sign determination algorithm were we have to invert a \( 3^n \) square matrix and compute \( 3^n \) Tarski Queries, where \( n \) is the number of polynomials. In fact we know in advance that at most \( r \) quantities of the form \( \text{cnt}(P, Q, \sigma) \) will be nonzero, since \( P \) has at most \( r \) roots, and we can build a square matrix of size \( r \) and compute at most \( 3n \) Tarski Queries.

The use of a proof assistant such as Coq in the formalization of these algorithms led us to write algorithms and conduct our proofs in a slightly different way than the one described in our reference [1]. The authors of the book then adopted some of our reformulations to modify their book, in order to make the description more precise or concise and to provide more detailed justifications.

Acknowledgment

We thank Marie-Françoise Roy for the numerous discussions we had together that enlightened us with her expertise of the subject.

References


