The Quadratic Form Method for Counting Real Zeros

Hoon Hong and Wolfgang Stöcher

June 19, 1995

Abstract

When solving equational constraints it is often required to quickly check whether there exist solutions at all and to compute the number of solutions.

In this report we describe our experiences with implementing an algorithm for counting the common real roots of a given polynomial system. Our approach is based on multivariate Sturm Theory (based on Pederson's results) and the Involution method for computing Gröbner bases.

1 Introduction

When dealing with geometric objects or when confronted with several equational constraints one often is at first hand only interested whether the objects intersect or the constraints can be met, respectively, rather than what the coordinates of the intersection points look like or how exactly to fulfill the constraints. Mathematically this can often be represented by a system of polynomial equations over the rationals in several variables, where we are only interested in the existence of real solutions.

We combine two methods: For fast computations involving ideals we use Gröbner bases. More specifically, Gröbner bases computed by the involution approach as described in [Zharkov, Blinkov 93]. The number of real roots we compute following [P. Pederson 92].

First an introduction to the mathematical foundations is given. Then the algorithm for computing the number of real roots is described.

2 Problem Statement

2.1 Examples

For example 1 we intersect a 'tacnode' with a circle:

$$f_1(x, y) = 2x^4 + y^4 - 3x^2y - 2y^3 + y^2,$$

$$f_2(x,y) = x^2 + y^2 - \frac{3}{2}.$$

Example 2 shows the intersection of a 'tacnode' with itself in rotated position:

$$f_1(x,y) = 2x^4 + y^4 - 3x^2y^1 - 2y^3 + y^2,$$

$$f_2(x,y) = 3x^4 - 4x^3y^1 + 8x^2y^2 - 4x^1y^3 + 3y^4 - 5x^3 - 3x^2y^1 - 3x^1y^2 - 5y^3 + x^2 + 2x^1y^1 + y^2 - 1.$$

These examples have 4 common zeros each.

2.2 Formal Description

More generally we can consider the given polynomials over an extension of an ordered field K.

given: $\{f_1, \ldots f_n\}, f_i \in K[\bar{x}]$,
the system $f_1 = \ldots = f_n = 0$ has finitely many solutions

find: number of real (and complex) solutions

The restriction to finitely many solutions is obviously necessary for counting the roots. It can be checked in advance, also automatically.

3 Mathematical Foundation

3.1 Counting Real Roots

We follow [P. Pederson 92]. Let K be an ordered field. The main idea is, given $f_1, \ldots f_n \in K[x_1, \ldots x_n] = K[\bar{x}]$ with finitely many common zeroes, to compute the *associated quadratic form*. Rank and signature of this quadratic form will give us the number of complex and real roots, respectively.

Let us go into more detail. The ideal generated by $f_1, \ldots f_n$ we denote by $I := <f_1, \ldots f_n>$. In the quotient ring $A := K[\bar{x}]/I$ the following functions shall be defined:

- $m_g : A \to A, \qquad m_g(h) = g \cdot h.$
- $B : A \times A \to K, \qquad B(g,h) = \mathrm{Trace}(m_g \circ m_h).$

Now the associated quadratic form can be defined as follows:

$$Q : A \to K, \qquad Q(g) = B(g,g).$$

The following theorem gives us the intended result.

Theorem 3.1 *Let $f_1, \ldots f_n \in \mathbf{Q}[\bar{x}]$ have only finitely many common zeroes and let Q be the associated quadratic form. Then the rank and signature of Q give the number of complex and real roots, respectively.*

3.2 Representation

For efficient computation we have to think about a good internal representation. To distinguish between an object and its representation we will mark the representation with an asterisk (*). For computations within the quotient ring A we need a basis. Here we make use of the following theorems.

Theorem 3.2 *Let $I \subset K$ be an ideal. Let $<LT(I)>$ denote the ideal generated by the leading terms in I and $\bar{x}^\alpha$ shall be an abbreviation for $x_1^{a_1} \dots x_n^{a_n}$. Then $K[\bar{x}]/I$ is isomorphic as a K-vector space to $S = \mathrm{Span}(\bar{x}^\alpha : \bar{x}^\alpha \notin <LT(I)>)$.*

Theorem 3.3 *The number of common roots of the system $f_1 = \dots = f_n = 0$ is finite in the algebraic closure $\mathbf{C}$ of K if and only if the quotient ring $K[\bar{x}]/I$ regarded as a $\mathbf{C}$-vector space is finite-dimensional.*

The following theorem tells us how to compute such a basis $V = \{v_1, \dots v_d\}$ of $K[\bar{x}]/I$.

Theorem 3.4 *Fix a monomial ordering on $K[\bar{x}]$ and let $I \subset K[\bar{x}]$ be an ideal. $<LT(I)>$ denotes the ideal generated by the leading terms in I.*

1. *Every $f \in K[\bar{x}]$ is congruent modulo I to a unique polynomial r which is a k-linear combination of the monomials in the complement of $<LT(I)>$.*

2. *The elements of $\{\bar{x}^\alpha : \bar{x}^\alpha \notin <LT(I)>\}$ are linearly independent modulo I.*

Hence $V := \{[\bar{x}^\alpha] : \bar{x}^\alpha \notin <LT(I)>\}$ is a finite basis of $K[\bar{x}]/I$. Therefore the equivalence classes in $K[\bar{x}]/I$ can be represented by K-tuples with dimension d (the order of V). The representation of a polynomial g by its coefficients with respect to the basis V will be denoted by g^*.

Now in order to compute V, we have to decide whether a monomial $\bar{x}^\alpha$ is in $<LT(I)>$ or not. Here we make use of the definition of a *Gröbner basis* (see for instance [D. Cox, et al. 92], p. 76).

Definition 3.1 *Fix a monomial order. A finite subset $G = \{g_1, \dots g_t\}$ of an ideal I is called a* Gröbner basis *or* standard basis *if*

$$<LT(g_1), \dots LT(g_t)> = <LT(I)> \ .$$

Then V can be constructed by simple divisible checks.

Having fixed the basis V the quadratic form Q can be represented by

$$Q(g)^* = {g^*}^T Q^* g^*,$$

where $Q^* = (q_{ij})$ is a symmetric square matrix. Tedious computation gives us

$$q_{ij} = \sum_{1 \le l,s \le d} w_{i,l,s} w_{j,l,s},$$

where $w_{i,j,k}, 1 \leq k \leq d$, arise as coefficients in

$$v_i v_j = \sum_{1 \leq k \leq d} w_{i,j,k} v_k.$$

From the symmetric matrix Q^* rank and signature can be computed by extracting the signs of the trace elements in the diagonalized form. The number of positive and negative elements on the diagonal gives the rank, where as the difference between positive and negative elements on the diagonal gives the signature, i. e. the number of common real roots of the given polynomials $f_1, \ldots f_n$.

4 The Algorithm

First we give the specification of the algorithm:

Inputs: polynomials $\{f_1, \ldots f_n\}$ over $\mathbf{Q}$ in several variables; the number of common (complex) roots is finite

Outputs: number of real (and complex) solutions

The algorithm proceeds in the following steps:

1. Compute the Gröbner Basis GB of the ideal $I := <f_1, \ldots f_n>$ generated by the polynomials of the input. This is done using the Involution Method.
2. Construct Basis $V = \{v_1, \ldots v_d\}$ of $A = K[\bar{x}]/I$. This is done using theorem 3.4.
3. Compute with respect to the basis V the pairwise products $[v_i][v_j] = \sum_k w_{i,j,k}[v_k]$. This again is done by reduction with the involutive basis.
4. Compute the associated quadratic form $Q = (q_{ij})_{1 \leq i,j \leq d}$ by $q_{ij} := \sum_l \sum_s w_{i,l,s} w_{j,s,l}$.
5. Compute rank and signature of Q by diagonalizing (based on Gaussian elimination); this gives the number of complex and real solutions, resp. This is done using fast interval arithmetic giving exact bounds, which mostly suffice for computing the sign, especially when given a system of full rank. A discussion of this approach is in preparation.

5 Future Work

For computing Gröbner basis it would be interesting to compare the involution approach also with other methods, as they might be faster for the application in the Quadratic forms method. Further speedups can be expected from parallelization where further work is under progress.

References

[D. Cox, et al. 92] D. Cox, J. Little, D. O'Shea *Ideals, Varieties and Algorithms - An Introduction to Computational Algebraic Geometry and Commutative Algebra*, Springer New York (1992)

[H. Hong, et al. 94] Hong, H. and Neubacher, A. and Stahl, V. *The STURM Library Manual.* RISC-Linz Report Series No. 94-30, RISC Linz, Johannes Kepler University, 4040 Linz, Austria, 1994.

[H. Hong, W. Stöcher 94] Hong, H. and Stöcher, W. *Exact Division applied to Diagonalizing Symmetric Matrices* RISC-Linz Report Series No. 94-34, RISC Linz, Johannes Kepler University, 4040 Linz, Austria, 1994.

[P. Pederson 92] P. Pederson *Counting Real Zeros*, Thesis at Courant Institute, New York (1991)

[Zharkov, Blinkov 93] Zharkov, Yu.A. and Blinkov, A.Yu. *Involution Approach to Solving Systems of Algebraic Equations.* Proceedings of IMACS'93, 1993.

[Zharkov, Blinkov 94] Zharkov, Yu.A. and Blinkov, A.Yu. *Involutive Bases of Zero-Dimensional Ideals.* to appear, 1994.