Algebraic algorithms and applications to geometry

Elias P. Tsigaridas[*]

Department of Informatics and Telecommunications
National Kapodistrian University of Athens, HELLAS
et@di.uoa.gr

Abstract. Real algebraic numbers are the real numbers that are real roots of univariate polynomials with integer coefficients. We study exact algorithms, from a theoretical and an implementation point of view, that are based on integer arithmetic of arbitrary precision, for computations with real algebraic numbers and applications of these algorithms on problems and algorithms in non linear computational geometry.

In order to construct a real algebraic number we must solve in the reals a univariate polynomial with integer coefficients. We unify and simplify the theory behind the subdivision-based methods for real root isolation and we improve the complexity of the algorithm that is based on the continued fraction expansion of the real roots. The based known complexity bound up today, namely $\widetilde{\mathcal{O}}_B(d^4\tau^2)$, where d is the degree of the polynomial and τ the maximum coefficient bit size. is achieved using new techniques. Moreover, we prove that the bound holds for non square-free polynomials and that in the same complexity bound we can compute the multiplicities of the real roots. We prove a new bound, namely $\widetilde{\mathcal{O}}_B(d^4\tau^2)$, for the expected complexity of the algorithm based on continued fractions. We generalize the real root isolation algorithms to bivariate polynomial systems, where we present a complexity bound of $\widetilde{\mathcal{O}}_B(d^{10}\tau^2)$ that improves the previously known by four factors. Our experimental analysis proves the effectiveness of our methods.

The algorithms that we consider for computations with real algebraic numbers are construction, comparison, sign evaluation and quantifier elimination. If the degree of the polynomial is small, i.e. ≤ 4 in the univariate case and ≤ 2 in the bivariate case, we propose special purpose algorithms that have constant arithmetic complexity. For all the algorithm we present a `C++` implementation and experimental analysis.

In computational geometry we study the predicates needed by the algorithms for the arrangement of elliptic arcs in the plane and computation of the Voronoi diagram of ellipses, also in the plane. Finally, given a convex lattice polygon we study algorithm for decomposing it to two other convex lattice polygons, such that their Minkowski sum is the original polygon. This problem is closely related to the factorization of bivariate polynomials.

[*] Supervisor: Prof. Ioannis Z. Emiris

1 Introduction

My PhD dissertation focuses on exact algorithms for real root isolation of integer polynomials of small and arbitrary degree, computations with real algebraic numbers using Sturm-Habicht sequences, real solving of bivariate polynomial systems and applications of these algorithms to non-linear computational geometry as well as efficient C++ implementations following the generic programming paradigm.

We have to mention that the stated references do not represent in any way the related work on the problems that we consider. We were not able to provide a detailed bibliography in this abstract due to reasons of space. We encourage the interested reader to refer to the thesis for a more complete description of related work.

In what follows, the notation $\mathcal{O}_B$ refers to bit (Boolean) complexity and $\widetilde{\mathcal{O}}_B$ means that we are ignoring logarithmic factors.

2 Algebraic algorithms

We focus on algorithms for real solving univariate integer polynomials and bivariate polynomial systems and on computations involving one and two real algebraic numbers. We have implemented our algorithms in C++ and most of our implementations are part of the SYNAPS [1] [23] library, which is an open-source C++ library for symbolic-numeric computations for polynomials and polynomial systems. For a detailed description of our implementation approach and experimental results, we encourage the reader to refer to the thesis.

2.1 Real solving arbitrary degree polynomials

Consider the polynomial

$$f(x) = a_d\, x^d + \cdots + a_1\, x + a_0,$$

where the coefficients are known exactly, i.e. they are rational numbers. We consider only exact algorithms, i.e algorithms that involve computations with rational numbers of arbitrary precision. Let d be the degree of f and $\tau = 1 + \max_{i \leq d}\{\lg |a_i|\}$ be the maximum bit size of the coefficients.

Real root isolation consists of computing disjoint intervals with rational endpoints that contains one and only one real root of f and every real root is contained in some interval. In addition we may also need to report the multiplicities of the real roots.

For the problem of real root isolation of a univariate polynomial, we consider the general concept of a subdivision solver, that mimics the binary search algorithm. The algorithms, that follow this concept, consider an initial interval that contains all the real roots of the polynomial and then repeatedly subdivide

[1] www-sop.inria.fr/galaad/synaps

it until the tested interval contains 0 or 1 real root. The subdivision algorithms differ in the way that they count the real roots of a polynomial in an interval. The most well-known subdivision-based algorithms are STURM, DESCARTES, and BERNSTEIN (e.g. [25,4]). However, they count differently the number of real roots of a polynomial in an interval. To be more specific, STURM counts exactly the number of real roots, based on Sturm's theorem and on the evaluation of polynomial remainder sequences. On the other hand DESCARTES and BENRSTEIN provide an overestimation, based on Descartes' rule of sign. Exploiting the fact that Descartes' rule of sign can not overestimate the number of real roots more than the degree of the polynomial, all the algorithms can be put under the general concept of the subdivision solver. Using exactly the same arguments we can prove that they perform the same number of steps, that is $\mathcal{O}(d\tau + d \lg d)$. The analysis that we present unifies and simplifies significantly the previous approaches, (e.g [3,6,5,25]).

For all the subdivision-based algorithms we prove that we can isolate the real roots of a polynomial f, not necessarily square-free, in $\widetilde{\mathcal{O}}_B(d^4\tau^2)$ and that in the same complexity bound we can also compute the multiplicities of the real roots.

The continued fraction algorithm, CF, differs from the subdivision-based algorithms in that instead of bisecting a given initial interval it computes the continued fraction expansion of the real roots of the polynomial. The previous known bound for this algorithm was $\widetilde{\mathcal{O}}_B(d^5\tau^3)$ [1]. Using results from the metric theory of continued fractions, we proved that the number of steps of CF is $\widetilde{\mathcal{O}}(d\tau)$, and that its expected complexity is $\widetilde{\mathcal{O}}_B(d^4\tau^2)$. This holds for non square-free polynomials and covers the cost of computing the multiplicities. As a byproduct of our work in the CF algorithms we proved some results concerning bounds on roots of a polynomial, that are interested on their own.

Part of our work in univariate real root isolation appeared in [27,9].

2.2 Real algebraic numbers and bivariate polynomial systems

A real algebraic number is a real root of an integer polynomial.

In order to represent real algebraic numbers we use a square-free polynomial and an isolating interval. Evidently the unique real root of the polynomial in the interval is the real algebraic number of interest. This representation is called *isolating interval representation*, e.g. [29].

Evidently, real root isolation is an important ingredient for the construction of algebraic numbers represented in isolating interval representation. Besides construction, which is equivalent to univariate real root isolation, we analyze the complexity of comparison, sign evaluation and simultaneous inequalities with real algebraic numbers. Even though the algorithms for these operations are not new, e.g. [3,11,26,29], the results from real solving and optimal algorithms for polynomial remainder sequences allow us to improve the complexity of all the algorithms, at least by a factor.

Our results extend directly to the bivariate case, i.e. real solving a bivariate polynomial system, sign evaluation of a bivariate polynomial evaluated over two algebraic numbers and simultaneous inequalities with two variables.

We consider the problem of exact real solving of well-constrained, bivariate systems of relatively prime polynomials. The main problem is to compute all common real roots in isolating interval representation, and to determine their intersection multiplicities. We present two algorithms and analyze their asymptotic bit complexity, obtaining a bound of $\widetilde{\mathcal{O}}_B(d^{13}\tau)$, or $\widetilde{\mathcal{O}}_B(N^{14})$, for the purely projection-based method, and $\widetilde{\mathcal{O}}_B(d^{10}\tau^2)$, or $\widetilde{\mathcal{O}}_B(N^{12})$ for a subresultant-based method, where d bounds the degree of the polynomials, τ bounds the maximum coefficient bit size, and $N = \max\{d, \tau\}$. The previous record bound was $\widetilde{\mathcal{O}}_B(N^{16})$ [18], using another representation of the real algebraic numbers, namely Thom's encoding. To the best of our knowledge the only known, up to the presentation of this thesis, complexity bound for bivariate polynomial real solving, using the the isolating interval representation was $\widetilde{\mathcal{O}}_B(N^{30})$ [2].

Our main tool is signed subresultant sequences, extended to several variables using the technique of binary segmentation. We exploit advances on the complexity of univariate root isolation, and extend them to multipoint sign evaluation, sign evaluation of bivariate polynomials over two algebraic numbers. We derive new bounds for the sign evaluation of bi- and multi-variate polynomials, computation and evaluation of polynomial remainder sequences of multivariate polynomials and real root counting over an extension field. Our algorithms apply to the problem of simultaneous inequalities. Moreover, they allow us compute the topology of real plane algebraic curves in $\widetilde{\mathcal{O}}_B(N^{12})$, whereas the previous bound was $\widetilde{\mathcal{O}}_B(N^{16})$ [18].

Last, but not least, we present a complete `C++` implementation of our algorithms for bivariate real solving and computations with real algebraic numbers and experimental results.

Part of our results appeared in [9,13,23].

2.3 Algebraic numbers and polynomials of small degree

For real algebraic numbers of degree up to 4 and polynomials in one variable of arbitrary degree, or in 2 variables of degree ≤ 2, we propose algorithms with constant arithmetic complexity for real solving and operations with real algebraic numbers.

In order to decide the number of real roots and their multiplicity of a polynomial of degree up to 4, we consider the coefficients as parameters and we use the discrimination systems, first introduced by Yang [28]. In our approach, the computation of such systems relies on Sturm-Habicht [19] sequences the coefficients of which are factorized by the use of minors of the Bézoutian matrix of the polynomial and its derivative and by the use of invariants.

We represent a real algebraic number by a polynomial and an isolating interval. We compute rational numbers that isolate the roots of every polynomial of degree up to 4, which are computed as functions in the coefficients of the polynomial.

In order to compare two algebraic numbers of degree up to 4, or to find the sign of a polynomial of arbitrary degree, evaluated over such a number, we use Sturm-based algorithms which rely on computations of the signs of certain quantities. We precompute these quantities, we factorize them by the use of invariants and/or by minors of the Bézoutian matrix; for our implementation, this is done in an automated way. We developed programs that produce all possible sign combinations of the tested quantities, so as to test as few quantities as possible. Our algorithms, for algebraic numbers of degree up to 3, are optimal with respect to the algebraic degree of the tested quantities since the degree agrees with that of the resultant.

Additionally, we solve bivariate problems, such as the computation of the sign of a bivariate polynomial of degree 2 evaluated over two algebraic numbers and the solution of a system of two such polynomials. We tackle these problems by the use of Sturm-Habicht sequences, where again certain quantities are precomputed and factorized. To be more specific, we consider the resultants R_x, R_y, of the two bivariate polynomials thus obtaining degree-4 polynomials in x and y. We solve R_x, R_y and the isolating points of the computed algebraic numbers define a grid of boxes. We can decide if a box is empty or if it contains a simple or a multiple root of the system by computing the signs of f_1 and f_2 over these 2 algebraic numbers, that define the box. We do an optimization by noticing that the intersections in a column (row) cannot exceed 2 nor the multiplicity of the algebraic number and thus excluding various boxes. Our algorithm does not make any assumption, such as that the boxes cannot contain any critical points of the intersecting polynomials, hence there is no need for refinement. Moreover, we are trying another approach, by considering the rational univariate representation that can be obtained by the specialization of the subresultant chain.

Our work on small degree real algebraic numbers appeared in [11,10,24,14].

3 Geometric applications

Curved objects are becoming increasingly important in computational geometry; one reason, is their wide range of applications, including those in solid modeling, CAD, molecular biology, GIS. Our work is inscribed in a general effort to extend current geometric software from linear to non-linear geometric objects. In particular, contributes in extending the CGAL [2] library with a kernel for curved objects and the related operations. It is clear that such a kernel relies heavily on real algebraic numbers, polynomial equations and systems of polynomials of bounded degree. Our ultimate goal is to propose a modular and efficient approach to extend the CGAL library to manipulate curved objects.

3.1 Arrangement of elliptic arcs in the plane

We have provided the tools for CGAL to build arrangements, using both the incremental and the vertical sweep line algorithms. The representations and predicates below rely on computations with real algebraic numbers of small degree [11], thus their arithmetic complexity is constant.

[2] http://www.cgal.org

A conic curve is a *curve*, represented by a bivariate polynomial of total degree 2, whose coefficients are integers. Two kinds of points —intersection points and endpoints— are considered in the same way, thus allowing us to have a unique representation. We call *endpoint* indifferently an endpoint of an arc or an intersection. An *endpoint* is represented by the two intersecting conics and its coordinates,

Representation: A conic *arc* is represented by a supporting conic, the two delimiting endpoints and a boolean indicating whether it lies on the upper or lower part The input of course allows for full curves as well as arbitrary arcs, including non-monotone arcs. These are broken into x-monotone arcs by the CGAL arrangements algorithms that fix the choice of axes and orientation.

We studied the main predicates and constructions for conic arcs that are required by the CGAL arrangements and that are provided by the curved kernel.

make_x_monotone: It subdivides the given arc (which may be an entire curve) into x-monotone arcs.

nearest_intersection_to_right: Given an endpoint p and two x-monotone arcs, find their first intersection to the right of p.

compare_y_to_right: Given two x-monotone arcs supported by the conics g_1, g_2, and one of their intersection points $p = (p_x, p_y)$, such that the arcs are defined to the right of p (i.e. for x larger than p_x), the predicate decides which arc is above immediately to the right of p.

compare_y_at_x: It decides whether a given arc is above or below a given endpoint $\gamma = (\gamma_x, \gamma_y)$.

Our work in this problem appeared in [7].

3.2 Voronoi diagram of ellipses

We study the Voronoi diagram of ellipses under the exact computation paradigm. The distance of an exterior point to an ellipse is defined to be the minimum Euclidean distance to any point of the ellipse. As is the case for almost all problems in computational geometry for curved objects, the algorithm relies heavily on predicates implemented by algebraic operations.

We design and implement exact and complete algorithms for the predicates needed in the framework of *abstract* Voronoi diagrams and, more particularly, for the incremental algorithm of Karavelas and Yvinec [20]. Our final goal is a CGAL software package for constructing the Voronoi diagram of ellipses, based on the CGAL implementation for circles [8], which uses the same incremental algorithm. Hence the crucial question is to analyze and implement the predicates for ellipses. Some of the presented predicates are also needed in computing the visibility complex and the convex hull of ellipses.

We offer a full investigation of the problem dealing with both degenerate and non-degenerate configurations. We study the case of *non-intersecting* ellipses, which we expect to generalize to arbitrary ellipses and even pseudo-circles [20]. We assume that the input ellipses are given *constructively* in terms of their axes, center and rotation, all being rational, or if they are given implicitly that we are able to switch representation using only rational arithmetic.

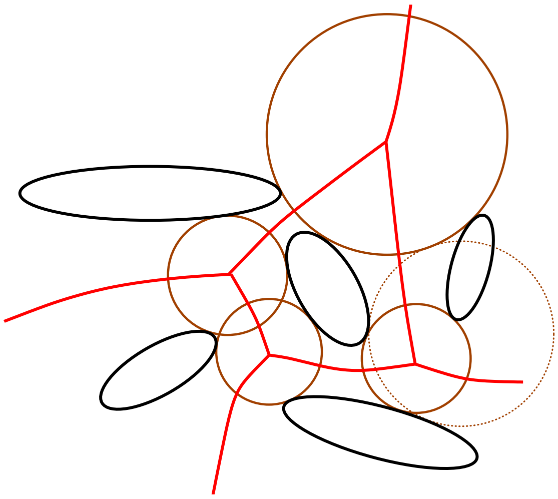

Fig. 1. Voronoi diagram of five ellipses

The four predicates of the incremental algorithm [20] are:

(κ_1) given two ellipses and a point outside of both, decide which is the ellipse closest to the point.

(κ_2) given two ellipses, decide the position of a third one relative to a specific external bitangent of the first two.

(κ_3) given three ellipses, decide the position of a fourth one relative to one (external tritangent) Voronoi circle of the first three; this is the InCircle predicate.

(κ_4) given four ellipses, compute the part of the bisector that changes due to the insertion of a fifth ellipse.

Our first contribution are algorithms for κ_1 and κ_2 that are optimal in terms of the degree of the algebraic numbers involved. In fact, for κ_2, we compute and characterize all bitangents of two ellipses using our own tools for dealing with algebraic numbers of degree four. Both algorithms satisfy the requirements of exact computation and are implemented in C++.

For the predicate κ_3, using the implicit representation, we obtain the first tight bound on the number of *complex* tritangent circles to three ellipses, namely 184. The number of real tritangent circles remains open. This approach does not lead to an efficient algorithm by itself, however, it provides a nearly optimal theoretical bound on the bit complexity of the problem.

Our work in this problem appeared in [16,15].

3.3 Minkowski decomposition

We study the decomposition of convex polygons with integral vertices (also called lattice polygons) under the Minkowski sum, which is defined as follows:

Definition 1. *For any two subsets A and B in $\mathbb{Z}^2$, their* Minkowski sum *is $A \oplus B = \{a + b | a \in A, b \in B\}$. We call A and B the* summands *of $A \oplus B$.*

The definition of the Minkowski sum can be generalized to arbitrary dimension.

The decomposition problem has a great interest on its own. The recent work on toric Bézier patches (e.g [21,22]), in geometric modelling, motivates several questions around this problem, mainly testing whether a given lattice polygon can be written as a Minkowski sum of two such polygons and, if so, finding one or all such decompositions. One important application of general Minkowski decomposition is bivariate (and, eventually, multivariate) polynomial factorization. This is so because, given a bivariate (multivariate) polynomial, we can associate with it its Newton polytope. As first observed by Ostrowski, if the polynomial factors, then its Newton polytope decomposes.

First, we focus on Minkowski decompositions where at least one of the summands is of constant size, namely it is a line segment, a triangle or a quadrangle. We estimate the hardness, from an asymptotic complexity viewpoint, and propose efficient algorithms for the case of constant-size summands. We relate Minkowski decomposition to the $k-$SUM problem, where an algorithm with time complexity $\mathcal{O}(n^{\lceil k/2 \rceil})$ or $\mathcal{O}(n^{\lceil k/2 \rceil} \lg n)$ exists but there are no matching lower bounds. We have implemented these algorithms and illustrated them on all lattice polygons with zero and one interior lattice points. Moreover, we performed experiments on various data sets against the algorithm of Gao and Lauder ([17]), which solves the general problem of Minkowski decomposition.

The decision problem of whether a lattice polygon admits a Minkowski decomposition is NP-complete [17]. In the same paper, a pseudo-polynomial algorithm is given with complexity in $\mathcal{O}((nDE)^3)$, where n is the number of edges in the polygon and DE is their maximum integer length. Note that DE is exponential with respect to the bit size of the input, which is $\mathcal{O}(n \lg (DE))$. We express the general problem by means of standard and well-studied problems in combinatorial optimization, such as the SUBSET-SUM problem. This leads to an algorithm that improves the above bound by a factor of nD. Our approach also leads immediately to approximation algorithms, to practical methods amenable to fast implementations and to a probabilistic algorithm. The implementation goes beyond the scope of the present paper.

A full description of our work can be found in [12].

References

1. A. Akritas. *Elements of Computer Algebra with Applications.* J. Wiley & Sons, New York, 1989.
2. D. Arnon and S. McCallum. A polynomial time algorithm for the topological type of a real algebraic curve. *J. Symbolic Computation*, 5:213–236, 1988.

3. S. Basu, R. Pollack, and M-F.Roy. *Algorithms in Real Algebraic Geometry*, volume 10 of *Algorithms and Computation in Mathematics*. Springer-Verlag, 2003.
4. G. Collins and A. Akritas. Polynomial real root isolation using Descartes' rule of signs. In *SYMSAC '76*, pages 272–275, New York, USA, 1976. ACM Press.
5. Z. Du, V. Sharma, and C. K. Yap. Amortized bound for root isolation via Sturm sequences. In D. Wang and L. Zhi, editors, *Int. Workshop on Symbolic Numeric Computing*, pages 113–129, School of Science, Beihang University, Beijing, China, 2005. Birkhauser.
6. A. Eigenwillig, V. Sharma, and C. K. Yap. Almost tight recursion tree bounds for the Descartes method. In *ISSAC '06: Proceedings of the 2006 International Symposium on Symbolic and Algebraic Computation*, pages 71–78, New York, NY, USA, 2006. ACM Press.
7. I. Z. Emiris, A. Kakargias, S. Pion, M. Teillaud, and E. P. Tsigaridas. Towards and open curved kernel. In J. Snoeyink and J.-D. Boissonnat, editors, *Proc. 20th Annual ACM Symp. on Computational Geometry (SoCG)*, pages 438–446, New York, USA, Jun 8–11 2004. ACM.
8. I. Z. Emiris and M. Karavelas. The predicates of the Apollonius diagram: algorithmic analysis and implementation. *Comp. Geom.: Theory & Appl., Spec. Issue on Robust Geometric Algorithms and their Implementations*, 33(1-2):18–57, 2006.
9. I. Z. Emiris, B. Mourrain, and E. P. Tsigaridas. Real Algebraic Numbers: Complexity Analysis and Experimentation. In P. Hertling, C. Hoffmann, W. Luther, and N. Revol, editors, *Reliable Implementations of Real Number Algorithms: Theory and Practice*, LNCS (to appear). Springer Verlag, 2007. also available in www.inria.fr/rrrt/rr-5897.html.
10. I. Z. Emiris and E. P. Tsigaridas. Computations with real algebraic numbers of degree up to 4. In *Proc. Int. Conf. on Polynomial System Solving (ICPSS), in honor of Daniel Lazard*, Paris, France, 2004.
11. I. Z. Emiris and E. P. Tsigaridas. Computing with real algebraic numbers of small degree. In S. Albers and T. Radzik, editors, *Proc. 12th European Symposium of Algorithms (ESA)*, volume 3221 of *LNCS*, pages 652–663, Bergen, Norway, Sep 14–17 2004. Springer Verlag.
12. I. Z. Emiris and E. P. Tsigaridas. Minkowski decomposition of convex lattice polygons. In M. Elkadi, B. Mourrain, and R. Piene, editors, *Algebraic geometry and geometric modeling*, pages 207–224. Springer, 2005.
13. I. Z. Emiris and E. P. Tsigaridas. Real solving of bivariate polynomial systems. In V. Ganzha and E. Mayr, editors, *Proc. Computer Algebra in Scientific Computing (CASC)*, volume 3718 of *LNCS*, pages 150–161. Springer, 2005.
14. I. Z. Emiris and E. P. Tsigaridas. Quantifier elimination for real algebra: the quadratic, cubic and quartic case. In *Abstracts in 12th Int. Conf. on Applications of Computer Algebra (ACA)*, Varna, Bulgaria, Jun 26–29 2006.
15. I. Z. Emiris, E. P. Tsigaridas, and G. M. Tzoumas. The InCircle predicates for ellipses. In *In Proc. European Workshop Computat. Geometry*, pages 225–228, Delphi, Greece, 2006.
16. I. Z. Emiris, E. P. Tsigaridas, and G. M. Tzoumas. The predicates for the Voronoi diagram of ellipses. In *Proc. 22th Annual ACM Symp. on Computational Geometry*, pages 227–236, Sedona, USA, 2006.
17. S. Gao and A. Lauder. Decomposition of polytopes and polynomials. *Discrete and Computational Geometry*, 26:89–104, 2001.
18. L. González-Vega and M. El Kahoui. An improved upper complexity bound for the topology computation of a real algebraic plane curve. *J. Complexity*, 12(4):527–544, 1996.

19. L. González-Vega, H. Lombardi, T. Recio, and M.-F. Roy. Sturm-Habicht Sequence. In *ISSAC*, pages 136–146, 1989.
20. M. Karavelas and M. Yvinec. Voronoi diagram of convex objects in the plane. In *Proc. ESA*, pages 337–348, 2003.
21. R. Krasauskas. Toric surface patches: Advances in geometrical algorithms and representations. *Adv. Comput. Math.*, 17(1-2):89–113, 2002.
22. R. Krasauskas and R. Goldman. Toric Bezier Patches with Depth. In R. Goldman and R. Krasauskas, editors, *Topics in Geometric Modeling and Algebraic Geometry*, volume 334, pages 65–91. AMS Mathematics of Computation, 2003.
23. B. Mourrain, J.-P. Pavone, P. Trébuchet, and E. P. Tsigaridas. SYNAPS: a library for symbolic-numeric computing. In *Proc. 8th Int. Symp. on Effective Methods in Algebraic Geometry (MEGA)*, Italy, May 2005. (software presentation).
24. B. Mourrain, S. Pion, S. Schmitt, J.-P. Técourt, E. P. Tsigaridas, and N. Wolpert. Algebraic issues in Computational Geometry. In J.-D. Boissonnat and M. Teillaud, editors, *Effective Computational Geometry for Curves and Surfaces*, Mathematics and Visualization, chapter 3. Springer, 2006.
25. B. Mourrain, M. Vrahatis, and J. Yakoubsohn. On the complexity of isolating real roots and computing with certainty the topological degree. *J. Complexity*, 18(2), 2002.
26. R. Rioboo. Towards faster real algebraic numbers. In *Proc. ACM Intern. Symp. on Symbolic & Algebraic Comput.*, pages 221–228, Lille, France, 2002.
27. E. P. Tsigaridas and I. Z. Emiris. Univariate polynomial real root isolation: Continued fractions revisited. In Y. Azar and T. Erlebach, editors, *Proc. 14th European Symposium of Algorithms (ESA)*, volume 4168 of *LNCS*, pages 817–828, Zurich, Switzerland, 2006. Springer Verlag.
28. L. Yang. Recent advances on determining the number of real roots of parametric polynomials. *J. Symbolic Computation*, 28:225–242, 1999.
29. C. Yap. *Fundamental Problems of Algorithmic Algebra.* Oxford University Press, New York, 2000.