数理解析研究所講究録 1335 巻 2003 年 84-90

Geometric applications of real elimination methods

フォルカー・ヴァイスフェニング

VOLKER WEISPFENNING

パッサウ大学

UNIVERSITÄT PASSAU *

Plan of the talk.

1. **The real elimination problem.** Motivation and history.
2. **A formal framework.** Elimination problems and elimination procedures in the real setting.
3. **Problems in science, engineering and operations research.** How to formulate some fundamental application problems as real elimination problems. The problems can be grouped naturally into problem types that are not geometric in their initial formulation, and problems that are of a geometric nature in their initial formulation.
4. **Three implemented real elimination methods.**
   (a) **QEPCAD** Quantifier elimination via partial cylindrical algebraic decomposition.
   (b) **CGB and MRRC** Comprehensive Gröbner bases and multivariate real root counting.
   (c) **REDLOG** Low-degree real elimination by virtual substitution of parametric test points.
5. **Computational examples in REDLOG, QEPCAD, CGB+MRRC.** Some successful application examples of these implementations.
6. **Conclusions.** Achievements, shortcomings, and potential of real elimination methods.

1 The real elimination problem

Since Tarski's discovery of algorithmic real elimination in the 1930, huge progress has been made concerning both theoretically and practically more efficient elimination methods. Nevertheless applications of implemented real elimination methods have been limited to small academic examples for a long time. Only since about 10 years these methods have begun to solve non-toy problems in mathematics, science, engineering, and operations research.

Purpose of the talk: A status report on the practical applicability of implemented real elimination methods.

*weispfen@uni-passau.de

Problem: "Eliminate" unwanted variables from an algebraic description of some situation. The unwanted variables may represent unknown quantities, e.g. quantities that can not be measured or determined directly in the given model. Geometrically elimination of variables corresponds to a projection along the coordinates of the eliminated variables.

A simple example.

$$\exists x(ax^2 + b = 0) \text{ is equivalent to}$$

$$a \neq 0 \text{ or } b = 0 \quad \text{in the complex domain}$$

$$ab < 0 \text{ or } (a = 0 \text{ and } b = 0) \quad \text{in the real domain}$$

2 The real and complex elimination problem

A **formal framework for elimination theory** can be sketched as follows:

We consider polynomials: $f = f(x, u) = f(x_1 \ldots, x_n, u_1 \ldots, u_m)$ with rational coefficients in two lists x and u of variables. We call x the **main variables** and u the **parameters**.

Equations will be expressions of the form $f = 0$ or more generally $f = g$ for polynomials f, g. In the real case we also consider **inequalities** of the form $f \geq 0,\ f > 0$. **Atomic formulas** are equations or inequalities.

quantifier-free (qf) formulas $\varphi(x, u)$ are boolean combinations of atomic formulas by the operators $\wedge, \vee, \neg$.

An **existential (ex) formula** is of the form $\varphi(x, u) : \exists x_1 \ldots \exists x_n \psi(x, u)$, where ψ is a qf-formula. Similarly a **universal (univ) formula** is of the form $\varphi(x, u) : \forall x_1 \ldots \exists x_n \psi(x, u)$, where ψ is a qf-formula.

A general (first-order) formula has several alternating blocks of existential and universal quantifiers in front of a qf formula.

The (real or complex) **quantifier-elimination (qe) problem** can be phrased as follows:

Given an existential formula $\varphi(u) : \exists x_1 \ldots \exists x_n \psi(x, u)$, find a qf formula $\varphi'(u)$ such that both are equivalent in the domain of real (or complex) numbers.XS A procedure computing such a φ' from φ is called a (real or complex) **quantifier-elimination (qe) procedure**.

Notice that a qe procedure can be iteratively applied to several blocks of existential and universal quantifiers to yield a quantifier elimination also for arbitrary formulas.

Quantifier elimination for an existential formula $\varphi(u) : \exists x_1 \ldots \exists x_n \psi(x, u)$ has a straightforward **geometric interpretation**:

Let M be the set in (x, u)-space defined by $\psi(x, u)$, and let M' be the set in u-space defined by $\varphi(u)$ or equivalently by $\varphi'(u)$. Then M' is the projection of M along the coordinate axes of the existentially quantified variables x onto the parameter space. Sets defined by first-order formulae in real or complex space are called **definable sets**. Sets defined by qf formulae in real or complex space are called **semialgebraic sets** and **constructible sets**, respectively. Notice that in the complex case inqualities are not allowed. So real or complex quantifier elimination asserts that every definable set is in fact semialgebraic, or constructible, respectively.

A qe procedure may be regarded as a generalization of a test that determines the solvability of a parametric system of equations in dependence of the parameters. The procedure may not give any information on the actual solutions of the system. So there is an obvious generalization of the real qe problem:

The **extended qe problem:** In the situation of the real qe problem, find in addition a finite list $(t_1(u), \ldots, t_k(u))$ of parametric test points (given by n-tuples of expressions in the parameters u), such that $\exists x_1 \ldots \exists x_n \psi(x, u) \rightarrow \bigvee_{i=1}^{k} \psi(t_i(u), u)$ holds in the reals.

A procedure achieving this goal will be called a (real or complex) **extended quantifier-elimination (qe) procedure**.

For fixed values of the parameters u one can then find a solution $x = t_j$ of ψ by testing all t_i.

3 Problems in science, engineering and operations research.

We explain by some typical examples how to formulate some fundamental application problems as real elimination problems.

The first group of problems concerns non-geometric problems.

1. Constraint solving.

   Here one has a number of real polynomial equations and inequalities and tries to test solvability and and to exhibit sample solutions. The first problem can be solved by real qe for existential formulas, the second by extended real qe.

2. Optimization problems.

   We consider the problem of mimimizing a polynomial (or rational) objective function q with respect to a boolean combination of polynomial inequalities as constraints. By introducing a new variable z and the additional constraint $q \leq z$, one can apply qe to the corresponding formula $\varphi(z)$ with existially quantified main variables and obtains a qf formula $\varphi'(z)$in z. From this formula one easily determines the minimal real value k satisfying $\varphi'(z)$. By applying extended qe to the original ex formula $\varphi(k)$ with k substituted for z one obtains the coordinates of a point, where q assumes the minimal value k.

   By introducing one or more parameters in the constraints and the objective function (e.g. time t) one obtains parametric optima, and can also test on sensitivity of optimal soultions wrt. variations of parameters.

   By allowing arbitrary boolean combinations of polynomial inequalities as constraints we can also model in this way a large class of scheduling problems.

3. Problems in simulation and diagnosis

   We consider technical networks (e.g. electrical or hydraulical networks), where the static behaviour of each component can be modeled by a qf formula in terms of flows, potentials etc. in connecting pipes. Then the behaviour of the whole network at specified in/out connections can be determined by real qe. Fault diagnosis of internal components can also be modelled as an extended qe problem.

4. Problems in control theory and stability

   We consider open loop linear control systems. Then the forward reachability problem concerns the set of states reachable in a given time interval from a given set of initial states for fixed control parameters. The backward reachability problem concerns the largest set of initial states that will keep the states in a given prescribed set in a given time interval for fixed control parameters. The control set problem concerns the largest set of control parameters that will for a given set of initial states keep the states in another given set in a given time interval.

   All these problems can be formulated as qe problems relative to a fundamental system of the corresponding homogeneous differential system and special solutions for the corresponding homogeneous differential system, where the control parameters are standard unit vectors.

B. Geometric problems.

1. Real implicitation problems.

   Given a polynomial (or rational) parametrization of a real variety, find an implicit description of this variety by a qf formula (involving possibly inequalities). This is a qe problem for the corresponding input formula with existentially quantified parameters.

2. Automatic theorem proving in geometry

   Successful popular methods for automatic theorem proving in geometry are Wu's method by extended charactersitic sets or Gr
   "obner basis methods. Both try to prove the given geometric statement as valid in the complex domain, and may therefore fail. Moreover they are not applicable to geometric statements involving inequalities.

   We formulate real geometric statements as universally quantified first-order formulas and apply real qe. If the output is "true", then the theorem is proved; otherwise the output specifies "forgotten" non-degeneracy conditions on the geometric configuration that are required to make the statement a theorem.

3. Computing projections, lighting and shading of solids.

   All these standard problems of solid geometry can be formulated as qe problems for existential formulas, provided the solids are given by qf formulas.

4. Reconstruction of solids from images.

   We consider images of solids or wire-frames obtained by parallel or central projections. Given the type of the original object we try to reconstruct its dimensions and position in space. This turns out to be an extended real qe problem.

5. Collision and path finding problems.

   Given a static or time-dependent semialgebraic environment of obstacles in two- or three-dimensional space and one or several semialgebraic solids in this space; then there are several types of problems that can all be formulated as extended real qe problems: Given translational speed vectors for the objects, will they collide with the environment or each other, and if yes, when will they collide. Given several translational speed vectors, try to find a continuous trajectories from given initial positions to given final positions for all objects such that the trajectories consist of a given number of pieces of these speed vectors and such that no collition occurs.

6. Solid modeling - offsets, rounding and blending.

   These operations on solids in three-space are achieved by moving a ball of constant radius in all possible positions inside, respectively outside the given solid. Then the set of all points covered, respectively deleted by this operation gives a rounding of the solid from inside, respectively from outside. Blendings between two solides result from rounding from outside of the union of both. All three operations applied to semialgebraic solids yield again semialgebraic solids that can be obtained by real qe.

4 Three implemented real elimination methods.

1. **QEPCAD** Quantifier elimination via partial cylindrical algebraic decomposition has been developed by G. Collins and his group, in particular H. Hong, S. McCallum and C. Brown. It is implemented in C by H. Hong and C. Brown and a variant also in REDUCE on top of REDLOG. Here all polynomials in an input formula are collected in a finite set F. A recursive projection operation produces from F successively new finite polynomial sets $F_1, \dots, F_n$ in lesser and lesser variables, such that the real zeros of each F_i are "delineated" over every connected set, where all polynomials in F_{i+1} are sign-invariant. In the extension phase one constructs recursively in $(-i)$ a partitioning of the variables space of F_i into connected semialgebraic cells on which all polynomials in F_i are sign-invariant. Moreover one obtains qf formulas describing each cell. Then the qe problem for the given input formula becomes a finite combinatorial problem of sign-evaluation of polynomials at one test point in each cell. Numerous variations of the construction obtained during 20 years have drastically reduced the number of cells and thus the size of the output formula. The method is in principle a complete real qe method without degree restrictions and has solved a number of interesting applications. Its practical complexity grows rapidly both with the number of quantifiers and the number of parameters. This limits its use to examples with a small total number of variables.

2. **CGB and MRRC** This method combines Comprehensive Gröbner bases and a parametric version multivariate real root counting a la Hermite. It has been implemented in MAS by A. Dolzmann. It typically works well for existential input formulas with many equations and very few inequalities in the quantified variables.

3. **REDLOG** REDLOG is a package of REDUCE 3.7 developed by T. Sturm and A. Dolzmann. Real qe in REDLOG is limited to input formulas, where the quantified variables occur only in polynno-mials of low degree. The method works by virtual substitution of parametric test points and has been significantly optimized over a period of 10 years. In this parameters costs almost nothing and elimination of linear variables is very efficient. So it has proved to be of great value in problems with only linear and quadratic quantified variables and many parameters. I. Mazzucco has developed a special purpose package SYMOPT for linear, quadratic and hyperbolic optimization under a boolean combination of linear constraints that is based on REDLOG methods.

5 Computational examples in REDLOG, QEPCAD, CGB+MRR

The talk has presented a number of successful application examples of these implementations taken from the application areas mentioned above. Many of them use REDLOG or SYMOPT only, but a number of advanced problems required a combination of REDLOG with QEPCAD or CGB + MRCC, or even both of them. In the examples involving only linear variables the maximal number of quantified variables or parameters ranges up to about 50. The examples show that real qe has by now definitely become a significant solution method for a wide variety of application problems due to ist great flexibility, even if the size of these problems is still somewhat limited.

6 Conclusions.

Real quantifier elimination has evolved from an esoteric method of mathematical logic to a serious tool for a number of application problems. Each of the implemented methods has its specific advantages and shortcomings, that makes a proper selection and/or combination of these methods hard for the non-expert. The future of real quantifier elimination as an application tool therefore lies in a smooth and widely automated combination of the available methods. Moreover specific application areas will need specialized qe packages that take advantage of restricted problem type. Moreover the acceptance of qe algorithms by users in a application field depends heavily on suitable user interfaces that hide the technicalities of the methods.

About half of the material in this talk is contained in the survey article [DSW98], that contains detailed references. More recent material is contained in the following references: [Bro98, Hon98a, Hon98b, McC98, SW98, Stu99, Dol99, Dol00, DW00, Dor00, AW01, Wei01b, Wei01a, Maz01, SS03].

References

[AW01] Hirokazu Anai and Volker Weispfenning. Reach set computations using real quantifier elimination. In *HSCC'2001, Hybrid Systems: Computation and Control*, volume 2034 of *LNCS*, pages 63–76. Springer, 2001.

[Bro98] C.W. Brown. Simplification of truth-invariant cylindrical algebraic decomposition. In *ISSAC'98*, pages 295–301. ACM, 1998.

[Dol99] Andreas Dolzmann. Solving geometric problems with real quantifier elimination. In Xiao-Shan Gao, Dongming Wang, and Lu Yang, editors, *Automated Deduction in Geometry*, volume 1669 of *Lecture Notes in Artificial Intelligence (Subseries of LNCS)*, pages 14–29. Springer-Verlag, Berlin Heidelberg, 1999.

[Dol00] Andreas Dolzmann. *Algorithmic Strategies for Applicable Real Quantifier Elimination*. Doctoral dissertation, Department of Mathematics and Computer Science. University of Passau, Germany, D-94030 Passau, Germany, March 2000.

[Dor00] Peter Dorato. Quantified multivariate polynomial inequalities - the mathematics of practical control design problems. *IEEE Control Systems Magazine*, 20(5):48–58, October 2000. Sign.: 80/SA 5505-20,5.

[DSW98] Andreas Dolzmann, Thomas Sturm, and Volker Weispfenning. Real quantifier elimination in practice. In B. H. Matzat, G.-M. Greuel, and G. Hiss, editors, *Algorithmic Algebra and Number Theory*, pages 221–247. Springer, Berlin, 1998.

[DW00] Andreas Dolzmann and Volker Weispfenning. Local quantifier elimination. In C. Traverso, editor, *ISSAC'2000*, pages 86–94. ACM-Press, 2000.

[Hon98a] Hoon Hong. An improvement of the projection operator in cylindrical algebraic decomposition. In B.F. Caviness and J.R. Johnson, editors, *Quantifier Elimination and Cylindrical Algebraic Decomposition*, Texts and Monographs in Symbolic Computation, pages 166–173. Springer, Wien, New York, 1998.

[Hon98b] Hoon Hong. Simple solution formula construction in cylindrical algebraic decomposition based quantifier elimination. In B.F. Caviness and J.R. Johnson, editors, *Quantifier Elimination and Cylindrical Algebraic Decomposition*, Texts and Monographs in Symbolic Computation, pages 201–219. Springer, Wien, New York, 1998.

[Maz01] Isolde Mazzucco. Symopt: Symbolic parametric mathematical programming. In V.G. Ganzha and E.W. Mayr, editors, *Computer Algebra in Scientific Computing 2001*, pages 417–429, Konstanz, Germany, Sept 2001.

[McC98] Scott McCallum. An improved projection operation for cylindrical algebraic decomposition. In B.F. Caviness and J.R. Johnson, editors, *Quantifier Elimination and Cylindrical Algebraic Decomposition*, Texts and Monographs in Symbolic Computation, pages 242–268. Springer, Wien, New York, 1998.

[SS03] Andreas Seidl and Thomas Sturm. A generic projection operator for partial cylindrical algebraic decomposition. Technical Report MIP-0301, FMI, Universität Passau, D-94030 Passau, Germany, January 2003.

[Stu99] Thomas Sturm. Reasoning over networks by symbolic methods. *Applicable Algebra in Engineering, Communication and Computing*, 10(1):79–96, September 1999.

[SW98] Thomas Sturm and Volker Weispfenning. Computational geometry problems in REDLOG. In Dongming Wang, editor, *Automated Deduction in Geometry*, volume 1360 of *Lecture Notes in Artificial Intelligence (Subseries of LNCS)*, pages 58–86. Springer-Verlag, Berlin Heidelberg, 1998.

[Wei01a] Volker Weispfenning. Semilinear motion planning among moving objects in REDLOG. In V.G. Ganzha, E.W. Mayr, and E.V. Vorozhtsov, editors, *CASC 2001*, pages 541–553. Springer Verlag, 2001.

[Wei01b] Volker Weispfenning. Semilinear motion planning in REDLOG. *AAECC*, 12(6):455–475, December 2001.