A new approach to quantifier elimination for real algebra and geometry

V. Weispfenning
Universität Passau, Germany

1 Introduction

Quantifier elimination for the elementary formal theory of real numbers is a fascinating area of research at the intersection of various field of mathematics and computer science, such as mathematical logic, commutative algebra and algebraic geometry, computer algebra, computational geometry and complexity theory. Originally the method of quantifier elimination was invented (among others by Th. Skolem) in mathematical logic as a technical tool for solving the decision problem for a formalized mathematical theory. For the elementary formal theory of real numbers (or more accurately of real closed fields) such a quantifier elimination procedure was established in the 1930's by A. Tarski, using an extension of Sturm's theorem of the 1830's for counting the number of real zeros of a univariate polynomial in a given interval. Since then an abundance of new decision and quantifier elimination methods for this theory with variations and optimizations has been published with the aim both of establishing the theoretical complexity of the problem and of finding methods that are of practical importance (see the discussion and references in [Renegar] for a comparsion of these methods). For subproblems such as elimination of quantifiers with respect to variables, that are linearly or quadratically restricted, specialized methods have been developed with good success (see [Weispfenning 1, Loos & Weispfenning, Hong 1]).

The theoretical worst-case complexity of the quantifier elimination problem for the reals is by now well-established (see [Renegar]); surprisingly the corresponding asymptotic lower bound is already valid for the elimination of linear quantifiers (see [Weispfenning 1]). Of course, this asymptotic complexity is established only up to multiplicative constants. It has turned out that the size of these constants varies extremely for the competing quantifier elimination methods, so that e. g. for practical use in problems of small to moderate size, the procedure of Collins (with or without optimizations, see [Collins & Hong]) performs much better, than asymptotically better procedures (see [Hong 2]). Moreover, the Collins' procedure (and its optimizations) remain up to now the only completely implemented quantifier elimination procedure for the full elementary theory of reals. It has meanwhile become apparent that a wealth of problems e.g. in geometry, algebra, analysis and robotics can be formulated as quantifier elimination problems (see [Collins & Hong, Lazard]). Hence the search for practicable quantifier elimination methods for the full elementary theory or fragments thereof is of great importance.

The purpose of this note is to sketch a new quantifier elimination procedure for the elementary theory of reals that differs from known ones among others by the fact that it eliminates whole *blocks* of quantifiers instead of one quantifier at a time. By analogy with the corresponding problem for algebraically closed fields (see [Weispfenning 2]), this feature may yield a good performance in some practical examples. At present, it is too early to estimate the performance; implementation has, however, begun at the University of Passau.

The method is based on an exiting new method for counting the number of real joint zeroes of multivariate polynomials with side conditions that was found recently independently by [Becker & Wörmann] and by [Pedersen & Roy & Szpirglas], based on ideas of Hermite-Sylvester. The method uses quadratic forms; it applies, however, only to zeros of zero-dimensional ideals (i.e. polynomial systems that have only finitely many complex zeros). It is this restriction that has to be overcome in order to apply the method for a quantifier elimination; moreover, the method has to be extended uniformly in arbitrary real parameters. The clue to the solution of these two problems is the use of *comprehensive Gröbner bases* that have proved to be of great value already for complex quantifier elimination.

In the following, I will first recall the basic facts concerning quantifier elimination, the real zero counting using quadratic forms and comprehensive Gröbner basis, and then outline the mains steps that combine these techniques into a quantifier elimination procedure.

2 Outline of the Method

2.1 The quantifier elimination problem for the elementary theory of the reals

An *atomic formula* is an expression of the form $f(X_1, \ldots, X_n) \; \rho \; g(X_1, \ldots, X_n)$, where $f, g \in Q[X_1, \ldots, X_n]$ and ρ is one of the relations $=, \leq, <$. *Formulas* are obtained from atomic formulas by means of the propositional operators $\wedge, \vee, \neg$ and quantification $\exists x_i, \forall x_i$ over variables x_i, together with appropriate use of parenthesis. The *quantifier elimination problem* asks for an algorithm that on input of a formula φ outputs a quantifier-free formula φ' (i.e. a propositional combination of atomic formulas) such that φ and φ' are equivalent in the ordered field $\mathbf{R}$ for real numbers (i.e. yield the same truth value for any assignment of real numbers to unquantified variables).

By a well-known and easy algorithm, any formula can be rewritten as an equivalent *prenex formula*, i.e. a formula beginning with a string of quantifiers followed by a quantifier-free formula. Any string $\exists x_1 \ldots \exists x_k$ or $\forall x_1 \ldots \forall x_k$ of similar quantifiers is called a *quantifier block*. In order to solve the quantifier elimination problem, it suffices by recursion on the number of quantifiers in a prenex formula to handle input formulas of the form $\exists x(\varphi)$, where φ is quantifier-free (notice that $\forall x(\varphi)$ is equivalent to $\neg\exists x(\neg\varphi)$). In a similar but more efficient way, the quantifier elimination problem is solved by recursion on the number of quantifier blocks provided one can handle input formulas of the form $\exists x_1 \ldots \exists x_k(\varphi)$, where φ is quantifier-free. Using the fact that φ can be put into disjunctive normal form and that disjunctions commute with existential quantifiers, it suffices therefore to handle input formulas of the form

$$(*) \qquad \exists x_1 \ldots \exists x_k (\bigwedge_{i=1}^{m} f_i(x_1, \ldots, x_n) = 0 \wedge \bigwedge_{i=1}^{m'} g_i(x_1, \ldots, x_n) > 0)$$

with $1 \leq k \leq n$, $f_i, g_i \in \mathbf{Q}[x_1, \ldots, x_n]$.

2.2 Counting real zeros using quadratic forms

Let F be a finite subset of $R = \mathbf{R}[x_1, \ldots, x_n]$ such that the ideal $I = Id(F)$ generated by F is zero-dimensional (i.e. has only finitely many complex zeros). Then the residue class ring R/I is finite-dimensional as $\mathbf{R}$-vector-space and an explicit basis of R/I consisting of residue classes of terms in R can be computed from a Gröbner basis G of I (see [Becker & Weispfenning]). Let $h \in R$; using the multiplication on R/I as linear map one can define a symmetric matrix B_h with real entries (see [Becker & Wörmann] or [Pedersen & Roy & Szpirglas]), such that the following holds: The signature of the quadratic from given by B_h (i.e. the difference between the number of positive and the number of negative eigenvalues of B_h) equals the number of real zeros of I, where h is positive, minus the number of real zeros of I, where h is negative.

Using the well-known technique of [Ben-Or & Kozen & Reif] this counting of real zeros of I with one side-condition given by h can be extended to finitely many side conditions.

2.3 Comprehensive Gröbner bases

For the basic facts on Gröbner bases we refer to [Becker & Weispfenning]. Let $R = \mathbf{Q}[U_1, \ldots, U_m, X_1, \ldots X_n]$ and fix a term-order $<$ on the set T of terms in $X_1, \ldots, X_n$. Let $I = I(\mathbf{U}, \mathbf{X})$ be an ideal in R and let $G = G(\mathbf{U}, \mathbf{X})$ be a finite subset of I. Then G is a *comprehensive Gröbner basis* of I if for every m-tuple $(a_1, \ldots, a_m)$ of elements in some extension field K of $\mathbf{Q}$, $G(\mathbf{a}, \mathbf{X})$ is a Gröbner basis of $I(\mathbf{a}, \mathbf{X})$ in $K[\mathbf{X}]$ with respect to the term-order $<$. For every finite $F \subseteq R$ one can compute a comprehensive Gröbner basis G of $I = Id(F)$. From G one can compute mutually exclusive quantifier-free formulas $\varphi_1, \ldots, \varphi_s$ in $U_1, \ldots, U_m$, whose disjunction is true, corresponding numbers $d_1, \ldots, d_s \in \{-1, \ldots, n\}$ and corresponding subsets $\mathcal{Y}_1, \ldots, \mathcal{Y}_s$, of $\{X_1, \ldots, X_n\}$ such that in every extension field K of $\mathbf{Q}$ and all $(a_1, \ldots, a_m)$ in K, if $\varphi_i(\mathbf{a})$ holds true in K, then the ideal $I(\mathbf{a}, \mathbf{X})$ has dimension d_i and $\mathcal{Y}_i$ is a maximal set of independent variables modulo $I(\mathbf{a}, \mathbf{X})$ (see [Weispfenning 2]).

2.4 Steps of the quantifier elimination method

By 2.1, it suffices to consider input formulas of the form (*) as in 2.1.

If $m = 0$, i.e. no equations are present, we may by a finite case distinction and by recursion on k adjoin equations of the type $\frac{\partial g}{\partial x_i} = 0$, where $g = \prod_{i=1}^{m'} g_i$.

If $m > 0$, we regard $x_{k+1}, \ldots, x_n$ as parameters, and compute a comprehensive Gröbner bais of $I = Id(f_1, \ldots, f_m)$ with respect to the main variables $x_1, \ldots, x_k$ and the quantifier-free formulas $\varphi_i(x_{k+1}, \ldots, x_n)$ together with d_i and $\mathcal{Y}_i \subseteq \{x_1, \ldots, x_k\}$ as described in 2.3

The indices i, for which $d_i = -1$ can be discarded.

For the indices i, for which $d_i = 0$, the computation of a number r of real zeros of $f_1, \ldots, f_m$ for which $g_1, \ldots, g_{m'}$ are positive yields quantifier-free formula ψ_r on the parameters which is necessary and sufficient (under the hypothesis φ_i) for this number r to be correct. Thus under the hypothesis φ_i, the quantifier-free equivalent to the given input formula is $\bigvee_{r>0} \psi_r$ (where r is bounded by the dimension of the corresponding residue class ring), in case $m' = 1$ and $g_1 = 1$. For the general case one employs the method of [Ben-Or & Kozen & Reif].

The indices i, for which $d_i > 0$, require additional effort: Here one adds the variables in $\mathcal{Y}_i$ to the parameters, recomputes a comprehensive Gröbner basis for this new situation and proceeds as before. This time the additional variables from $\mathcal{Y}_i$ in the output formula have to be existentially quantified and the whole procedure has to be repeated with this new input formula. Termination of this recursion is guaranteed since the number of main variables decreases in each recursive step.

3 Concluding Remarks

The algorithm sketched above is obviously in a first, very preliminary state that has to be optimized significantly for implementation. Its weak point is the possible recursion occuring for some input formulas, in case the dimension of the ideal to be considered is greater than zero in the quantified variables. There are, however, many interesting input formulas for which this situation will not occur, among them well-known benchmark examples, if formulated appropriately (comp. [Collins & Hong, Lazard].

References

[Becker & Wörmann] E. Becker, T. Wörmann, On the trace formula for quadratic forms and some applications, Proc. RAGSQUAD, Berkeley, 1991, to appear.

[Becker & Weispfenning] T. Becker, V. Weispfenning (in cooperation with H. Kredel), Gröbner bases - a computational approach to commutative algebra, Springer Verlag, Graduate Texts in Mathematics, 1993.

[Ben-Or & Kozen & Reif] M. Ben-Or, D. Kozen, J. Reif, The complexity of elementary algebra and geometry, J. Comp. System. Sciences 32 (1986), pp. 251-264.

[Collins & Hong] G.E. Collins, H. Hong, Partial cylindrical algebraic decomposition for quantifier elimination, J. Symb. Comp. 12 (1991), pp. 299-328.

[Hong 1] H. Hong, Quantifier elimination for formulas constrained by quadratic equation, RISC-Linz Report Series No. 92-53.

[Hong 2] H. Hong, Comparsion of several decision algorithms for the existential theory of the reals, RISC-Linz Report Series No. 91-41.0.

[Lazard] D. Lazard, Quantifier elimination: Optimal solution for two classical examples, J. Symb. Comp. 5 (1988), pp. 261-266.

[Loos & Weispfenning] R. Loos, V. Weispfenning, Applying linear quantifier elimination, preprint Passau 1992, to appear.

[Pedersen & Roy & Szpirglas] P. Pedersen, M.-F. Roy, A. Szpirglas, Counting real zeros in the multivariate case, to appear in Proc. MEGA '92.

[Renegar] J. Renegar, On the computational complexity of the first-order theory of reals; Parts I-III, J. Symb. Comp. 13 (1992), pp. 255-352.

[Weispfenning 1] V. Weispfenning, The complexity of linear problems in fields, J. Symb. Comp., pp. 3-28.

[Weispfenning 2] V. Weispfenning, Comprehensive Gröbner bases, J. Symb. Comp. 14 (1992), pp. 1-29.