Solving Geometric Problems with Real Quantifier Elimination

Andreas Dolzmann

Fakultät für Mathematik und Informatik
Universität Passau, D-94030 Passau, Germany
`dolzmann@uni-passau.de`
`http://www.fmi.uni-passau.de/~dolzmann/`

MIP-9903

26 January 1999

Abstract. Many problems arising in real geometry can be formulated as first-order formulas. Thus quantifier elimination can be used to solve these problems. In this note, we discuss the applicability of implemented quantifier elimination algorithms for solving geometrical problems. In particular, we demonstrate how the tools of REDLOG can be applied to solve a real implicitization problem, namely the Enneper surface.

1 Introduction

Since Tarski has introduced the first quantifier elimination algorithm for the real numbers in the 1930's, cf. [21], several other algorithms have been developed. Only some of them are implemented and widely available. Among them there are, for instance, the quantifier elimination by *partial cylindrical algebraic decomposition* implemented in the C-program QEPCAD, the quantifier elimination by *real root counting* implemented in the module QERRC within the Modula II computer algebra system MAS and the quantifier elimination by *virtual substitution* implemented in the REDUCE-package REDLOG. Whereas QEPCAD and QERRC provide a complete quantifier elimination procedure, the quantifier elimination of REDLOG is restricted in the degree of the quantified variables.

The naive approach to use one of the implemented quantifier elimination algorithms for solving a problem often fails in practice. Firstly, the programs can fail due to the limitations of computing time and memory. Secondly, the chosen quantifier elimination algorithm may not be able to handle the wanted class of problems.

Nevertheless it is possible to solve non-trivial problems using the implemented quantifier elimination algorithms. In general this requires both a combination of the available algorithms and a careful formulation of the problem as a first-order formula according to the chosen quantifier elimination method.

We give solutions of problems cited in the literature and compare the results of the different elimination procedures. In particular we discuss the real implicitization of the Enneper surface.

2 The General Framework

We consider multivariate polynomials $f(u,x)$ with rational coefficients, where $u = (u_1 \ldots, u_m)$ and $x = (x_1, \ldots, x_n)$. We call u *parameters* and we call x *main variables*. *Atomic formulas* are polynomial equations $f = 0$, polynomial inequalities $f \geqslant 0$, $f \leqslant 0$, $f > 0$, $f < 0$, and $f \neq 0$. *Quantifier-free* formulas are built from atomic formulas by combining them with the boolean connectors "$\neg$," "$\wedge$," and "$\vee$." *Existential formulas* are of the form $\exists x_1 \ldots \exists x_n \psi(u,x)$, where ψ is a quantifier-free formula. Similarly, *universal formulas* are of the form $\forall x_1 \ldots \forall x_n \psi(u,x)$. A *prenex first-order formula* has several alternating blocks of existential and universal quantifiers in front of a quantifier-free formula, the *matrix* of the prenex formula.

The real *quantifier elimination problem* can be phrased as follows: Given a formula φ, find a quantifier-free formula φ' such that both φ and φ' are equivalent in the domain of the real numbers. A procedure computing such a φ' from φ is called a real *quantifier elimination procedure*.

A *background theory* is a set of atomic formulas considered conjunctive. Two formulas φ and φ' are equivalent wrt. a background theory Θ, if and only if

$$\underline{\forall}\Big(\bigwedge \Theta \longrightarrow (\varphi \longleftrightarrow \varphi')\Big),$$

where $\underline{\forall}$ denotes the universal closure. Notice, that the formula $x^2 - x = 0$ contained in a background theory, does not imply a multiplicative idempotency law, but only describes an equation for the variable x.

A *generic* quantifier elimination procedure assigns to a formula φ a quantifier-free formula φ' and a background theory Θ', such that φ and φ' are equivalent wrt. the background theory Θ'. The computed background theory contains only negated equations. Hence the set

$$\left\{ a \in \mathbb{R}^m \;\middle|\; \neg\big(\varphi'(a) \longleftrightarrow \exists x \varphi(a, x)\big) \right\}$$

has measure zero. Notice, that each quantifier elimination procedure provides also a generic quantifier elimination assigning $\emptyset$ to Θ'. However, the computation of an appropriate Θ' leads in many cases to simpler quantifier-free equivalents and results in a considerable speed-up of the running times. Moreover, in the framework of automatic proving in real geometry generic quantifier elimination allows us to find sufficient conditions automatically, cf. [13] for details.

3 Quantifier Elimination Methods

In this section we sketch the three most important implemented quantifier-elimination algorithms. For a more detailed overview over these algorithms, cf. [14].

3.1 Quantifier Elimination by Partial Cylindrical Algebraic Decomposition

Cylindrical algebraic decomposition (CAD), cf. [6, 1], is the oldest and most elaborate implemented real quantifier elimination method. It has been developed by Collins and his students starting in 1974. During the last 10 years particularly Hong made very significant theoretical contributions that improved the performance of the method dramatically, cf. [16, 17], resulting in *partial* CAD, cf. [7]. Hong has implemented partial CAD in his program QEPCAD based on the computer algebra C-library SACLIB. QEPCAD is not officially published but available from Hong on request. Brown has contributed the latest very successful improvements to the algorithm, cf. [4]. Unfortunately, the improved version was not available when we made the computations for this article.

We sketch the basic ideas of CAD: Suppose we are given an input formula

$$\varphi(u_1, \dots, u_m) \equiv \mathsf{Q}_1 x_1 \dots \mathsf{Q}_n x_n \psi(u_1, \dots, u_m, x_1, \dots, x_n), \quad \mathsf{Q}_i \in \{\exists, \forall\}.$$

Let F be the set of all polynomials occurring in ψ as left hand sides of atomic formulas. Call $C \subseteq \mathbb{R}^{m+n}$ *sign invariant* for F, if every polynomial in F has constant sign on all points in C. Then $\psi(c)$ is either "true" or "false" for all $c \in C$.

Suppose we have a finite sequence $\Pi_1, \dots, \Pi_{m+n}$ with the following properties:

1. Each Π_i is a finite partition of $\mathbb{R}^i$ into connected semi-algebraic cells. For $1 \leqslant j \leqslant n$ each Π_{m+j} is labeled with Q_j.
2. Π_{i-1} consists for $1 < i \leqslant m+n$ exactly of the projections of all cells in Π_i along the coordinate of the i-th variable in $(u_1, \dots, u_m, x_1, \dots, x_n)$. For each cell C in Π_{i-1} we can determine the preimage $S(C) \subseteq \Pi_i$ under the projection.
3. For each cell C in Π_m we know a quantifier-free formula $\delta_C(u_1, \dots, u_m)$ describing this cell.
4. Each cell C in Π_{m+n} is sign invariant for F. Moreover for each cell C in Π_{m+n}, we are given a *test point* t_C in such a form that we can determine the sign of $f(t_C)$ for each $f \in F$ and thus evaluate $\psi(t_C)$.

A quantifier-free equivalent for φ is obtained as the disjunction of all δ_C for which C in Π_m is *valid* in the following recursively defined sense:

1. For $m \leqslant i < m+n$, we have that Π_{i+1} is labeled:
   (a) If Π_{i+1} is labeled "$\exists$," then C in Π_i is valid if at least one $C' \in S(C)$ is valid.
   (b) If Π_{i+1} is labeled "$\forall$," then C in Π_i is valid if all $C' \in S(C)$ are valid.
2. A cell C in Π_{m+n} is valid if $\psi(t_C)$ is "true."

Partial cylindrical algebraic decomposition (PCAD) is an improved version of CAD. It takes the boolean structure of the input formula into account. CAD and also PCAD is doubly exponential in the number of all variables.

3.2 Quantifier Elimination by Virtual Term Substitution

The virtual substitution method dates back to a theoretical paper by Weispfenning in 1988, cf. [22]. During the last five years a lot of theoretical work has been done to improve the method, cf. [18, 23, 11]. The method is implemented within the REDUCE package REDLOG by the author and Sturm, cf. [10].

The applicability of the method in the form described here is restricted to formulas in which the quantified variables occur at most quadratically. Moreover quantifiers are eliminated one by one, and the elimination of one quantifier can increase the degree of other quantified variables. On the other hand there are various heuristic methods included for decreasing the degrees during elimination. One obvious example for such methods is polynomial factorization.

For eliminating the quantifiers from an input formula

$$\varphi(u_1, \dots, u_m) \equiv \mathsf{Q}_1 x_1 \dots \mathsf{Q}_n x_n \psi(u_1, \dots, u_m, x_1, \dots, x_n), \quad \mathsf{Q}_i \in \{\exists, \forall\}$$

the elimination starts with the innermost quantifier regarding the other quantified variables within ψ as extra parameters. Universal quantifiers are handled by means of the equivalence $\forall x \psi \longleftrightarrow \neg \exists x \neg \psi$. We may thus restrict our attention to a formula of the form

$$\varphi^*(u_1, \dots, u_k) \equiv \exists x \psi^*(u_1, \dots, u_k, x),$$

where the $u_{m+1}, \ldots, u_k$ are actually x_i quantified from further outside.

We fix real values $a_1, \ldots, a_k$ for the parameters $u_1, \ldots, u_k$. Then all polynomials occurring in ψ^* become linear or quadratic univariate polynomials in x with real coefficients. So the set

$$M = \{\, b \in \mathbb{R} \mid \psi^*(a_1, \ldots, a_k, b) \,\}$$

of all real values b of x satisfying ψ^* is a finite union of closed, open, and half-open intervals on the real line. The endpoints of these intervals are among $\pm\infty$ together with the real zeros of the linear and quadratic polynomials occurring in ψ^*.

Candidate terms $\alpha_1, \ldots, \alpha_r$ for the zeros can be computed uniformly in $u_1, \ldots, u_k$ by the solution formulas for linear and quadratic equations. For open and half-open intervals, we add expressions of the form $\alpha \pm \varepsilon$, where α is a candidate solution for some left-hand side polynomial. The symbol ε stands for a positive infinitesimal number. Together with the formal expressions ∞ and $-\infty$ all these candidate terms form an *elimination set.* This means M is non-empty if and only if the substitution of at least one element of the elimination set satisfies ψ^*. After substitution of formal expressions possibly involving square roots, ε, or $\pm\infty$, we rewrite the substitution result in such a way that it does not contain any fractions nor one of these special symbols. This process of substituting a term and rewriting the formula is called *virtual substitution.* By disjunctively substituting all candidates into ψ^* we obtain a quantifier-free formula equivalent to $\exists x \psi^*$.

For practical applications this method, of course, has to be refined by a careful selection of smaller elimination sets and by a combination with powerful simplification techniques for quantifier-free formulas, cf. [11] for details. There is a variant of the virtual substitution method for generic quantifier elimination, cf. [13].

Quantifier elimination by virtual substitution is doubly exponential in the number of quantifier blocks but only singly exponential in the number of quantified variables. The number of parameters only plays a minor role in the complexity.

3.3 Quantifier Elimination by Real Root Counting

The basis for this quantifier elimination method is a theorem on real root counting found independently by Becker and Wörmann, cf. [2, 3], and Pedersen, Roy, and Szpirglas, cf. [19, 20]. It is based on a result for counting real zeros of univariate polynomials found by Hermite, cf. [15].

> *Let $I \subseteq \mathbb{R}[x_1, \ldots, x_n]$ be a zero-dimensional ideal. For $g \in \mathbb{R}[x_1, \ldots, x_n]$ consider the symmetric quadratic form $Q_g = \bigl(\operatorname{trace}(m_{gb_ib_j})\bigr)_{1 \leqslant i,j \leqslant d}$ on the linear $\mathbb{R}$-space $S = \mathbb{R}[x_1, \ldots, x_n]/I$, where $\{b_1, \ldots, b_d\} \subseteq S$ is a basis, and the $m_h : S \to S$ are linear maps defined by $m_h(f + I) = (hf) + I$. Let s be the signature of Q_g, and denote by n_+ and n_- the number*

of real roots of I at which g is positive or negative, respectively. Then $n_+ - n_- = s$.

The use of a Gröbner basis of the ideal I allows to obtain a basis of S, and to perform arithmetic there, cf. [5], thus obtaining the matrix Q_g.

This approach can be extended to obtain the exact number of roots under a side condition, and can be moreover extended to several side conditions:

Let F, $\{g_1, \dots, g_k\} \subseteq \mathbb{R}[x_1, \dots, x_n]$ be finite, and assume that $I = Id(F)$ is zero-dimensional. Denote by N the number of real roots $a \in \mathbb{R}^n$ of F for which $g_i > 0$ for $1 \leqslant i \leqslant k$. Define

$$\Gamma(\{g_1, \dots, g_k\}) = \{\, g_1^{e_1} \cdots g_k^{e_k} \mid (e_1, \dots, e_k) \in \{1, 2\}^k \,\}.$$

Then defining Q_g as above we have $2^k N = \sum_{\gamma \in \Gamma(\{g_1,\dots,g_k\})} \operatorname{sig}(Q_\gamma)$.

For real quantifier elimination, this root counting has to be further extended to multivariate polynomials with parametric coefficients in such a way that it will remain correct for *every* real specialization of the parameters including specializations to zero. This task has been carried out by Weispfenning using comprehensive Gröbner bases, cf. [24]. It has been implemented by the author within the package QERRC of the computer algebra system MAS, cf. [9]. A variant for generic quantifier elimination is under development.

4 Simplification Methods

Simplification of formulas means to compute to a given formula an equivalent one, which is simpler. The simplification of the input formulas and intermediate results are very important for a successful application of quantifier elimination by virtual substitution and for quantifier elimination by real root counting. QEPCAD does not depend heavily on simplification of formulas, because formulas are used only for input and output. For a detailed description of the simplification algorithms sketched in this section and a discussion of the notion of *simple* formulas, cf. [11].

4.1 The Standard Simplifier

The *standard simplifier* is a fast, though sophisticated, simplifier for quantifier-free formulas. It was developed for the implementation of the quantifier elimination by virtual term substitution in the REDLOG package. The standard simplifier was designed to be called very often, for instance, after each elimination step. Beside the simple methods to remove boolean constants and to keep only one of a set of identical subformulas, it implements three main strategies:

Firstly, it simplifies the atomic formulas. All right hand side of atomic formulas are normalized to zero. The left hand side polynomials are normalized to be primitive over $\mathbb{Z}$ in such a way that the highest coefficient wrt. a fixed term order is positive. Furthermore, we drop irrelevant factors of the polynomials. Trivial square sums are detected to be greater than zero or not less than zero, respectively. Optionally, we explode atomic formulas by decomposing the polynomial additively or multiplicatively.

Secondly, smart simplification is applied to conjunctions and disjunctions of atomic formulas: Each pair of atomic formulas involving identical left-hand sides, is replaced by "true," "false," or by one atomic formula using an appropriate relation. Similarly, this method can be applied to some pairs of atomic formulas which differs only in the absolute summand of the left-hand side polynomial.

Thirdly, the techniques used for the smart simplification of flat formulas are applied to nested formulas. This is done by constructing an implicit background theory for each boolean level of the formula.

The standard simplifier offers the option to simplify a formula wrt. a background theory. The output formula is then equivalent to the input formula wrt. the given background theory.

4.2 Simplification of boolean Normal Forms

For the simplification of boolean normal forms we use two further techniques additionally to the techniques used in the standard simplifier.

The *generalized subsumption* allows us to drop conjunctions of a CNF: Let t_i terms and $\varphi_i,\ \rho_i, \rho_i' \in \{<, \leqslant, =, \geqslant, \geqslant, >\}$. Then

$$(t_1\ \rho_1\ 0 \wedge \ldots \wedge t_n\ \rho_n\ 0) \vee (t_1\ \rho_1'\ 0 \wedge \ldots \wedge t_n\ \rho_n'\ 0 \wedge \ldots)$$

can be simplified to $(t_1\ \rho_1\ 0 \wedge \ldots \wedge t_n\ \rho_n\ 0)$, if $t_i\ \rho_i'\ 0 \longrightarrow t_i\ \rho_i\ 0$.

The *generalized cut* combines two conjunctions combined disjunctively into one conjunction: if $(t_i\ \rho_i\ 0 \vee t_i\ \rho_i'\ 0) \longleftrightarrow t_i\ \sigma_i\ 0$ then the disjunction

$$(t_1\ \rho_1\ 0 \wedge t_2\ \rho_2\ 0 \wedge \ldots \wedge t_n\ \rho_n\ 0) \vee (t_1\ \rho_1'\ 0 \wedge t_2\ \rho_2\ 0 \wedge \ldots \wedge t_n\ \rho_n\ 0)$$

can be simplified to $(t_1\ \sigma_1\ 0 \wedge t_2\ \rho_2\ 0 \wedge \ldots \wedge t_n\ \rho_n\ 0)$. In our implementation, not all possible applications of the generalized cut and the generalized subsumption are performed. We only apply the simplifications in cases, where the respective implication can be decided independently of the terms t_i. Analogous simplification rules hold for conjunctions of disjunctions.

4.3 The Gröbner Simplifier

The *Gröbner simplifier* is an advanced method for the simplification of boolean normal forms. The main technique used for this method is the computation of a Gröbner basis for deciding the ideal membership test, cf. [5]. Let F be a set of polynomials and G a Gröbner basis of F. Then the Gröbner simplifier replaces

$$\bigwedge_{f \in F} f = 0 \wedge \bigwedge_{h \in H} h\, \rho_h\, 0 \quad \text{by} \quad \bigwedge_{f \in G} f = 0 \wedge \bigwedge_{h \in H} \mathrm{Nf}_G(h)\, \rho_h\, 0.$$

Using a radical membership test, we can optionally replace the input formula by false, if $h \in \mathrm{Rad}(F)$ and $\rho_h \in \{<, \neq, >\}$.

There is, of course, a variant which simplifies disjunctions of atomic formulas. Conjunctive and disjunctive normal forms are simplified essentially by applying the Gröbner simplifier to each of the constituents. Additionally there are strategies to relate information contained in different constituents. For the simplification of an arbitrary formula, we compute a CNF or a DNF first. We have implemented a variant of the Gröbner simplifier which automatically decides, whether to compute a CNF or a DNF. This decision is based on a heuristic for estimating which of the normal forms is larger. Like the standard simplifier the Gröbner simplifier can simplify a formula wrt. a background theory.

Although the Gröbner simplifier operates on a boolean normal form, we consider it as a general simplification method. It turned out that in many cases the result of the Gröbner simplification is simpler than the input formula.

We illustrate the technique by means of a very simple example: Consider the input formula $xy + 1 \neq 0 \vee yz + 1 \neq 0 \vee x - z = 0$, which can be rewritten as

$$xy + 1 = 0 \wedge yz + 1 = 0 \longrightarrow x - z = 0.$$

Reducing the conclusion modulo the Gröbner basis $\{x - z, yz + 1\}$ of the premises, we obtain the equivalent formula $xy + 1 = 0 \wedge yz + 1 = 0 \longrightarrow 0 = 0$, which can in turn be easily simplified to "true."

4.4 The Tableau Method

Although the standard simplifier combines information located on different levels, it preserves the basic boolean structure of the formula. The Gröbner simplifier computes a boolean normal from and thus it changes the boolean structure completely. The tableau method, in contrast, provides a technique for changing the boolean structure of a formula slightly by constructing case distinctions. There are three variants of tableau simplifiers:

Given a formula φ and a term t the *tableau simplifier* constructs the following case distinction:

$$(t = 0 \wedge \varphi) \vee (t > 0 \wedge \varphi) \vee (t < 0 \wedge \varphi).$$

This formula is then simplified with the standard simplifier. Even though the constructed case distinction is about three times larger than the original formula, in some cases the simplified equivalent is much smaller than the original formula.

The *iterative tableau simplifier* chooses automatically an appropriate term t by trying all terms contained in φ. The result is then either the original formula or the best result obtained by the tableau simplifier, depending on which one is simpler. The *automatic tableau simplifier* applies the iterative tableau as long as the output is simpler than the input.

5 REDLOG

REDLOG is a REDUCE package implementing a *computer logic system*, cf. [10]. It provides algorithms to deal with first-order logic formulas over various languages and theories. Beside the theory of real closed fields there are algorithms for the theory of discretely valued fields [12] and algebraically closed fields. REDLOG provides an implementation of the quantifier elimination by virtual substitution including variants for generic quantifier elimination, extended quantifier elimination, and linear optimization using quantifier elimination techniques. There are also interfaces to QEPCAD and QERRC available such that these packages can be called from REDLOG and the results are available to be further processed. All simplification algorithms discussed in this note are available in REDLOG. Besides these important algorithms REDLOG provides many tools for normal form computations, constructing, analyzing, and decomposing formulas. The REDLOG source code and documentation are freely available on the WWW.[1]

6 Examples

By means of examples we discuss in this section the applicability of quantifier elimination to some problems taken from various scientific research areas. We compare the timings of the three considered implementations. Furthermore we will give some hints, how to apply quantifier elimination, even if the naive approach fails.

In this section we allow ourselves to use not only prenex formulas but also general first-order formulas, i.e. boolean combinations of prenex formulas. Furthermore, we use the implication $\Rightarrow$ and the equivalence $\Leftrightarrow$ inside formulas. Notice, that these general formulas can be easily transformed in prenex formulas containing only the boolean connectors $\wedge$ and $\vee$.

All example computations mentioned in this section have been performed on a SUN Ultra 1 Model 140 workstation using 32 MB of memory.

6.1 Real Implicitization

For $n < m$ let $f : \mathbb{R}^n \to \mathbb{R}^m$ be a rational map with the component functions p_i/q, where p_i, $q \in \mathbb{R}[x_1, \dots, x_n]$ for $1 \leqslant i \leqslant m$. The image $f(\mathbb{R}^n)$ of f is a definable and hence semi-algebraic subset of $\mathbb{R}^m$ described by the formula

$$\exists x_1 \dots \exists x_n \big(q(x_1, \dots, x_n) \neq 0 \wedge \bigwedge_{i=1}^{m} p_i(x_1, \dots, x_n) = u_i q(x_1, \dots, x_n)\big).$$

Our aim is to obtain a quantifier-free description of $f(\mathbb{R}^n)$ in the variables u_1, ..., u_m, preferably a single equation, which would provide an implicit definition of f.

[1] `http://www.fmi.uni-passau.de/~redlog/`

Example 1. Descartes' folium $d : \mathbb{R} \to \mathbb{R}^2$ is given by the component functions $3x_1/(1+x_1^3)$ and $3x_1^2/(1+x_1^3)$ for u_1 and u_2, cf. [8]. For obtaining an implicit form we apply quantifier elimination to

$$\exists x_1 \big(1 + x_1^3 \neq 0 \wedge 3x_1 = u_1(1+x_1^3) \wedge 3x_1^2 = u_2(1+x_1^3)\big).$$

QEPCAD obtains after 1 s the result $u_1^3 - 3u_1u_2 + u_2^3 = 0$. QERRC obtains after 1.6 s an elimination result with 7 atomic formulas. This can be automatically simplified to the QEPCAD result using the Gröbner simplifier. REDLOG fails on this example due to a violation of the degree restrictions. After simplifying the matrix of the formula with the Gröbner simplifier for CNF's we can eliminate the quantifier with REDLOG. The output formula computed in 0.3 s contains 21 atomic formulas.

Example 2. The Whitney Umbrella is given by

$$(x_1, x_2) \mapsto (x_1x_2, x_2, x_1^2).$$

QEPCAD produces in 1 s the result $u_3 \geqslant 0 \wedge -u_1^2 + u_2^2u_3 = 0$. Quantifier elimination by virtual substitution (QEVTS) produces in 0.01 s the much longer result

$$u_3 \geqslant 0 \wedge (u_1^2 - u_2^2u_3 = 0 \wedge u_1u_2 \geqslant 0 \vee u_1^2 - u_2^2u_3 = 0 \wedge u_1u_2 \leqslant 0).$$

However, including a Gröbner simplification we yield in 0.03 s the same result as produced by QEPCAD. Using QERRC we get the following quantifier-free equivalent in 0.8 s:

$$u_2 \neq 0 \wedge -u_1^2 + u_2^2u_3 = 0 \vee u_1 = 0 \wedge u_2 = 0 \wedge u_3 + 1 \neq 0 \wedge u_3 \geqslant 0.$$

6.2 Automatic Theorem proving in Geometry

Example 3 (Steiner–Lehmus theorem, variant). Assume that ABC is a triangle such that $AB > AC$. Then the angle bisector from B to AC is longer than the angle bisector from C to AB (i.e., the longer bisector goes to the shorter side).

In its original form, the Steiner–Lehmus theorem states that *any triangle with two equal internal bisectors is isosceles.* Its contrapositive follows immediately from the variant above.

We put $A = (-1, 0)$, $B = (1, 0)$, and $C = (x_0, y_0)$ with $y_0 > 0$. By $M = (0, b)$ we denote the center and by c the radius of the circumcircle.

The bisectors are constructed using the geometrical theorem proved as Example 4: Let $V = (0, b - c)$ be the point below the x-axis on the circumcircle having equal distance to A and B. Then the angle bisector from C to AB is obtained as CX, where $X = (x, 0)$ is the intersection of CV and AB. The angle bisector from B to AC is obtained analogously: Let $W = (x_1, y_1)$ be the point on the circumcircle with equal distance to A and C lying "west" of the line AC. Let $Y = (x_2, y_2)$ be the intersection of BW and AC. Then the angle bisector is BY.

Our algebraic translation obtained this way reads as follows:

$$\forall b \forall c \forall x \forall x_1 \forall y_1 \forall x_2 \forall y_2 \big(y_1(x_0+1) > x_1 y_0 \ \wedge \ y_0 > 0 \ \wedge \ c > 0 \ \wedge \\ c^2 = 1 + b^2 \ \wedge \ c^2 = x_0^2 + (y_0 - b)^2 \ \wedge \ x\big(y_0 + (c-b)\big) = x_0(c-b) \ \wedge \\ x_1^2 + (y_1 - b)^2 = c^2 \ \wedge \ (x_1+1)^2 + y_1^2 = (x_1 - x_0)^2 + (y_1 - y_0)^2 \ \wedge \\ (x_1 - 1)y_2 = y_1(x_2 - 1) \ \wedge \ (x_0+1)y_2 = y_0(x_2+1) \ \wedge \\ 4 > (x_0+1)^2 + y_0^2 \longrightarrow (x - x_0)^2 + y_0^2 < (x_2 - 1)^2 + y_2^2 \big).$$

Using QEVTS we obtain after 74 s an elimination result φ^* containing 243 atomic formulas together with the subsidiary conditions

$$\vartheta^* \equiv x_0^2 + 2x_0 + y_0^2 + 1 \neq 0 \ \wedge \\ x_0^2 - 2x_0 + y_0^2 - 3 \neq 0 \ \wedge \ x_0 + 1 \neq 0 \ \wedge \ x_0 \neq 0 \ \wedge \ y_0 \neq 0.$$

QEPCAD proves within 250 s that $\vartheta^* \longrightarrow \varphi^*$, while QEVTS, QERRC fail doing so.

Example 4. Let M be the center of the circumcircle of a triangle ABC. Then $\angle ACB = \angle AMB/2$ (see Figure 1). Choosing coordinates $A = (-a, 0)$, $B =$

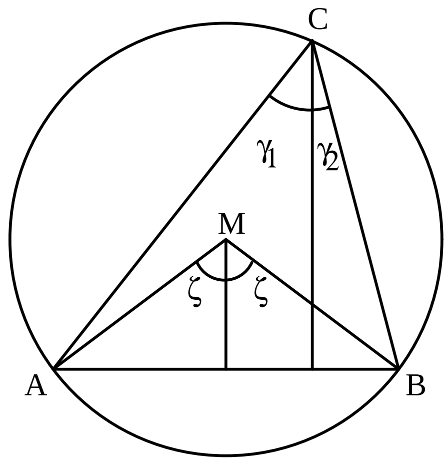

Fig. 1. The angle at circumference is half the angle at center (Example 4).

$(a, 0)$, $C = (x_0, y_0)$, and $M = (0, b)$ and encoding angles into tangents, an algebraic translation of this problem reads as follows:

$$\forall x \forall t_1 \forall t_2 \forall t \forall b \big(c^2 = a^2 + b^2 \wedge c^2 = x_0^2 + (y_0 - b)^2 \wedge \\ y_0 t_1 = a + x_0 \wedge y_0 t_2 = a - x_0 \wedge (1 - t_1 t_2)t = t_1 + t_2 \longrightarrow bt = a \big).$$

Both QEPCAD and QERRC fail on this input. QEVTS together with the Gröbner simplifier yields after 0.06 s the quantifier-free equivalent $a \neq 0 \vee x_0 \neq 0 \vee y_0 \neq 0$ containing non-degeneracy conditions for the triangles.

The generic variants of QEVTS and QERRC produce "true" as a quantifier-free equivalent wrt. the background theory $\{y \neq 0\}$. This computation takes 0.02 s with QEVTS and 2 s with QERRC.

6.3 The Enneper Surface

The Enneper surface is defined parametrically by

$$x = 3u + 3uv^2 - u^3 \quad y = 3v + 3u^2v - v^3 \quad z = 3u^2 - 3v^2,$$

cf. [8]; in other words as the image of the function

$$f : \mathbb{C}^2 \longrightarrow \mathbb{C}^3 \quad \text{with} \quad f(u, v) = (3u + 3uv^2 - u^3, 3v + 3u^2v - v^3, 3u^2 - 3v^2).$$

The smallest variety V containing the Enneper surface is given by the polynomial

$$\begin{aligned} p(x, y, z) = {} & 19683x^6 - 59049x^4y^2 + 10935x^4z^3 + 118098x^4z^2 - 59049x^4z + {} \\ & 59049x^2y^4 + 56862x^2y^2z^3 + 118098x^2y^2z + 1296x^2z^6 + {} \\ & 34992x^2z^5 + 174960x^2z^4 - 314928x^2z^3 - 19683y^6 + 10935y^4z^3 - {} \\ & 118098y^4z^2 - 59049y^4z - 1296y^2z^6 + 34992y^2z^5 - 174960y^2z^4 - {} \\ & 314928y^2z^3 - 64z^9 + 10368z^7 - 419904z^5. \end{aligned}$$

Using Gröbner bases techniques it is easy to proof that over the complex numbers the image of f is identical to the complete complex variety V. The real Enneper surface is given by the restriction $f \restriction_{\mathbb{R}^2}^{\mathbb{R}^3}$. The question is whether the real Enneper surface is identical to the real variety of p.

This problem can be easily stated as a real quantifier elimination problem. A first-order description of the real image of f is given by

$$\varphi \equiv \exists u \exists v \big(x = 3u + 3uv^2 - u^3 \wedge y = 3v + 3u^2v - v^3 \wedge z = 3u^2 - 3v^2\big).$$

Using this formula the complete problem can be stated as

$$\forall x \forall y \forall z (\varphi(x, y, z) \Leftrightarrow p(x, y, z) = 0).$$

It turns out, that none of the quantifier elimination algorithms considered in this paper can eliminate all the quantifiers of the above formula. Actually, none of the implementations is able to find a quantifier-free equivalent to φ. In the next paragraphs we will describe how to tackle the problem with the quantifier elimination algorithms and the tools available in the REDLOG system.

In a first step we compute a quantifier-free equivalent to φ. With the implementation of the virtual substitution method we can eliminate one of the existential quantifiers of φ. The solutions of eliminating u or eliminating v are up to a simple substitution identical. We start with the elimination of v and obtain in 0.2 s the result

$$\exists u \big(v_4 \geqslant 0 \wedge (v_1 = 0 \wedge v_2 = 0 \wedge v_3 \geqslant 0 \vee v_1 = 0 \wedge v_2 = 0 \wedge v_3 \leqslant 0)\big)$$

where

$$\begin{aligned}
v_1 &:= 108u^6 + 324u^4 - 9u^2z^2 - 54u^2z + 243u^2 - 27y^2 - z^3 - 18z^2 - 81z,\\
v_2 &:= 2u^3 - uz + 3u - x,\\
v_3 &:= 6u^2y + yz + 9y,\\
v_4 &:= 3u^2 - z.
\end{aligned}$$

Applying the generalized cut to both constituents of the disjunction, we obtain the formula:

$$\exists u\bigl(v_4 \geqslant 0 \wedge v_1 = 0 \wedge v_2 = 0\bigr).$$

REDLOG produces this formula by computing a disjunctive normal form. After this simplification only the package QERRC can eliminate the remaining quantifier, but the obtained elimination result φ' is very large. Though it has only 81 atomic formulas a textual representation contains approximately 500 000 characters.

However, we have found a quantifier-free description of the image of the function describing the Enneper surface. One of the atomic formulas contained in the result is the equation $p = 0$. But this fact does not imply any direction of the equivalence we want to prove.

The obtained result is in fact to large, to eliminate the universal quantifiers from

$$\forall x \forall y \forall z\bigl(\varphi(x, y, z) \Leftrightarrow p(x, y, z) = 0\bigr)$$

with one of our quantifier elimination procedures. Actually, we are not able to eliminate at least one universal quantifier. Thus we use REDLOG to simplify φ'.

An analysis of the formula yields that the result formula is a disjunction of nine subformulas. Five of these nine are simply conjunctions of atomic formulas and the remaining four subformulas are essentially conjunctive normal forms.

For a simplification of the formula we thus simplify each constituent of the top-level disjunctions with the Gröbner simplifier for conjunctive normal forms. In a first step, we take the Gröbner simplifier without a factorization of atomic formulas. In a second step we use the Gröbner simplifier with the automatic factorization option twice for each constituent of the top-level disjunction. After these simplification we obtain a formula with 50 atomic formulas and about 30000 characters. All these simplifications takes 434 s.

The automatic tableau method can simplify some of the resulting conjunctive normal forms in about 1 s. After these simplifications we get a disjunction of eight conjunctive normal forms. From these eight conjunctive normal forms are six pure conjunctions of atomic formulas. The two other ones are conjunctions containing atomic formulas and only one disjunction of two atomic formulas. Using the equivalents

$$(\alpha \leqslant 0 \vee \beta = 0) \longleftrightarrow (\alpha \cdot \beta^2 \leqslant 0) \quad \text{and} \quad (\alpha = 0 \vee \beta = 0) \longleftrightarrow (\alpha \cdot \beta = 0)$$

we can simplify the formula to a disjunctive normal form ψ with constituents ψ_i.

Let Θ_i be the set of atomic formulas of ψ_i. Using the Gröbner simplifier we can simplify $p = 0$ wrt. the theory Θ_i to "true." This means that $\psi_i \longrightarrow p = 0$ and hence $\psi \longrightarrow p = 0$.

Using a tool of REDLOG, which counts the frequencies of all included atomic formulas we analyze our result. The most frequently occurring atomic formulas in ψ are

$$x = 0, \quad y = 0, \quad z - 3 \neq 0, \quad \text{and} \quad z \neq 0$$

each of them with more than three occurrences.

This observation suggests, that we should study a special case of the implication. For arbitrary formulas Ψ, Γ and formulas $\alpha_1, \dots, \alpha_n$ with $\alpha_1 \wedge \cdots \wedge \alpha_n$ contradictive the following equivalence holds:

$$\begin{aligned}(\Psi \Rightarrow \Gamma) &\longleftrightarrow (\alpha_1 \wedge \cdots \wedge \alpha_n) \vee (\Psi \Rightarrow \Gamma)\\ &\longleftrightarrow (\neg\alpha_1 \wedge \Psi) \Rightarrow \Gamma) \wedge \ldots \wedge (\neg\alpha_n \wedge \Psi) \Rightarrow \Gamma)\\ &\longleftrightarrow (\neg\alpha_1 \Rightarrow (\Psi \Rightarrow \Gamma) \wedge \ldots \wedge (\neg\alpha_n \Rightarrow (\Psi \Rightarrow \Gamma)).\end{aligned}$$

Using $x \neq 0$, $y \neq 0$, $z \neq 0$, $z \neq 3$, and $(x = 0 \vee y = 0 \vee z = 0 \vee z = 3)$ for the α_i we can split our implication in a conjunction of five implications. Four of them include simple equations for one of the variables.

For proving the cases including an equation we substitute the values 0 and 3 for the respective variable in the formula $p = 0 \Rightarrow \psi$ and then we eliminate the universal closure of the substitution result. The timings for this elimination are summarized in Table 1. The elimination result is in all cases "true."

Table 1. Elimination times for the special cases.

	$x = 0$	$y = 0$	$z = 0$	$z = 3$
QEVTS	failed	0.7 s	0.1 s	failed
QEPCAD	1.0 s	23.0 s	1.0 s	1.0 s

After we have checked the special cases, we can exclude these cases by simplifying the formula ψ with respect to the theory $\{x \neq 0, y \neq 0, z \neq 0, z \neq 3\}$. This yields a disjunction of two conjunctions. One of the remaining constituents is contradictive as shown by the elimination of the existential closure with QEVTS in 0.8 s. Neither QEPCAD nor QERRC are able to prove this fact. The remaining constituent is a conjunction $\beta_1 \wedge \cdots \wedge \beta_4$ of atomic formulas, where β_1 is the equation $p = 0$. Instead of proving the complete implication, which is not possible with our quantifier elimination procedures, we prove $p = 0 \Rightarrow \beta_i$ for each atomic formula β_i in the conjunction. The first implication holds trivially.

While trying to eliminate one of the quantifiers REDLOG applies a heuristic to decrease the degree of the variables x and y. Namely, it replaces each occurrence of x^2, and y^2 by x and y respectively, adding the additional premise $x > 0 \wedge y > 0$. Finally the quantifier elimination fails. However, after the degree reduction QEPCAD is able to eliminate all universal quantifier. For the elimination it is necessary to give the quantifiers in the order $\forall z \forall y \forall x$. Altogether the three eliminations take 34 s. All results are "true" and thus we have finally proven the equivalence.

7 Conclusions

After approximately 50 years of development, quantifier algorithms can nowaday be used to solve geometrical problems. Even if a first approach fails, the several quantifier elimination methods can be applied in interaction with the user to appropriate subproblems, finally solving the problem. Our results show, that among the three considered algorithms there is no best algorithm, solving all problems. Furthermore they show that not only quantifier elimination algorithms are necessary but even powerful simplification algorithms and a wide spectrum of tools for analyzing and decomposing formulas. Important for the user is a common interface to all algorithms, like REDLOG provides one.

Acknowledgment

We acknowledge the influence of V. Weispfenning on the discussion of the Steiner–Lehmus theorem and the Enneper surface. In particular helpful were his many useful hints for the analysis of the real Enneper surface.

References

1. Dennis S. Arnon, George E. Collins, and Scott McCallum. Cylindrical algebraic decomposition I: The basic algorithm. *SIAM Journal on Computing*, 13(4):865–877, November 1984.
2. Eberhard Becker. Sums of squares and quadratic forms in real algebraic geometry. In *Cahiers du Séminaire d'Historie de Mathématiques*, volume 1, pages 41–57. Université Pierre et Marie Curie, Laboratoire de Mathématiques Fondamentales, Paris, 1991.
3. Eberhard Becker and Thorsten Wörmann. On the trace formula for quadratic forms. In William B. Jacob, Tsit-Yuen Lam, and Robert O. Robson, editors, *Recent Advances in Real Algebraic Geometry and Quadratic Forms*, volume 155 of *Contemporary Mathematics*, pages 271–291. American Mathematical Society, American Mathematical Society, Providence, Rhode Island, 1994. Proceedings of the RAGSQUAD Year, Berkeley, 1990–1991.
4. Christopher W. Brown. Simplification of truth-invariant cylindrical algebraic decompositions. In Oliver Gloor, editor, *Proceedings of the 1998 International Symposium on Symbolic and Algebraic Computation (ISSAC 98)*, pages 295–301, Rostock, Germany, Aug 1998. ACM, ACM Press, New York.
5. Bruno Buchberger. *Ein Algorithmus zum Auffinden der Basiselemente des Restklassenringes nach einem nulldimensionalen Polynomideal.* Doctoral dissertation, Mathematical Institute, University of Innsbruck, Innsbruck, Austria, 1965.

6. George E. Collins. Quantifier elimination for the elementary theory of real closed fields by cylindrical algebraic decomposition. In H. Brakhage, editor, *Automata Theory and Formal Languages. 2nd GI Conference*, volume 33 of *Lecture Notes in Computer Science*, pages 134–183. Gesellschaft für Informatik, Springer-Verlag, Berlin, Heidelberg, New York, 1975.
7. George E. Collins and Hoon Hong. Partial cylindrical algebraic decomposition for quantifier elimination. *Journal of Symbolic Computation*, 12(3):299–328, September 1991.
8. David Cox, John Little, and Donald O'Shea. *Ideals, Varieties and Algorithms.* Undergraduate Texts in Mathematics. Springer-Verlag, New York, Berlin, Heidelberg, 1992.
9. Andreas Dolzmann. Reelle Quantorenelimination durch parametrisches Zählen von Nullstellen. Diploma thesis, Universität Passau, D-94030 Passau, Germany, November 1994.
10. Andreas Dolzmann and Thomas Sturm. Redlog: Computer algebra meets computer logic. *ACM SIGSAM Bulletin*, 31(2):2–9, June 1997.
11. Andreas Dolzmann and Thomas Sturm. Simplification of quantifier-free formulae over ordered fields. *Journal of Symbolic Computation*, 24(2):209–231, August 1997.
12. Andreas Dolzmann and Thomas Sturm. P-adic constraint solving. Technical Report MIP-9901, FMI, Universität Passau, D-94030 Passau, Germany, January 1999.
13. Andreas Dolzmann, Thomas Sturm, and Volker Weispfenning. A new approach for automatic theorem proving in real geometry. *Journal of Automated Reasoning*, 21(3):357–380, 1998.
14. 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.
15. Charles Hermite. Remarques sur le théorème de M. Sturm. In Emile Picard, editor, *Œuvres des Charles Hermite*, volume 1, pages 284–287. Gauthier-Villars, Paris, 1905.
16. Hoon Hong. An improvement of the projection operator in cylindrical algebraic decomposition. In Shunro Watanabe and Morio Nagata, editors, *Proceedings of the International Symposium on Symbolic and Algebraic Computation (ISSAC 90)*, pages 261–264, Tokyo, Japan, August 1990. ACM, ACM Press.
17. Hoon Hong. Simple solution formula construction in cylindrical algebraic decomposition based quantifier elimination. In Paul S. Wang, editor, *Proceedings of the International Symposium on Symbolic and Algebraic Computation (ISSAC 92)*, pages 177–188, Berkeley, CA, July 1992. ACM, ACM Press.
18. Rüdiger Loos and Volker Weispfenning. Applying linear quantifier elimination. *The Computer Journal*, 36(5):450–462, 1993. Special issue on computational quantifier elimination.
19. Paul Pedersen. *Counting Real Zeros.* Ph.D. dissertation, Courant Institute of Mathematical Sciences, New York, 1991.
20. Paul Pedersen, Marie-Françoise Roy, and Aviva Szpirglas. Counting real zeroes in the multivariate case. In F. Eysette and A. Galigo, editors, *Computational Algebraic Geometry*, volume 109 of *Progress in Mathematics*, pages 203–224. Birkhäuser, Boston, Basel; Berlin, 1993. Proceedings of the MEGA 92.
21. Alfred Tarski. A decision method for elementary algebra and geometry. Technical report, RAND, Santa Monica, CA, 1948.
22. Volker Weispfenning. The complexity of linear problems in fields. *Journal of Symbolic Computation*, 5(1–2):3–27, February–April 1988.

23. Volker Weispfenning. Quantifier elimination for real algebra—the quadratic case and beyond. *Applicable Algebra in Engineering Communication and Computing*, 8(2):85–101, February 1997.
24. Volker Weispfenning. A new approach to quantifier elimination for real algebra. In B.F. Caviness and J.R. Johnson, editors, *Quantifier Elimination and Cylindrical Algebraic Decomposition*, Texts and Monographs in Symbolic Computation, pages 376–392. Springer, Wien, New York, 1998.