Journal of Automated Reasoning **21:** 357–380, 1998.

A New Approach for Automatic Theorem Proving in Real Geometry

ANDREAS DOLZMANN, THOMAS STURM,* and
VOLKER WEISPFENNING
Fakultät für Mathematik und Informatik, Universität Passau, Germany

(Received: April 1996; accepted: March 1997)

Abstract. We present a new method for proving geometric theorems in the real plane or higher dimension. The method is derived from elimination set ideas for quantifier elimination in linear and quadratic formulas over the reals. In contrast to other approaches, our method can also prove theorems whose complex analogues fail. Moreover, the problem formulation may involve order inequalities. After specification of independent variables, nondegeneracy conditions are generated automatically. Moreover, when trying to prove conjectures that – apart from nondegeneracy conditions – do not hold in the claimed generality, missing premises are found automatically. We demonstrate the applicability of our method to nontrivial examples.

Key words: real quantifier elimination, real geometry, automatic theorem proving over the reals.

1. Introduction

Theorems of elementary geometry have traditionally been considered an important test case for the scope of methods in automatic theorem proving. Such problems have stimulated a variety of algebraic techniques for their solution, in particular, the Wu–Ritt method (see [7, 37, 39]), Gröbner basis techniques (see [17, 18, 19]), and complex elimination methods (see [27, 28]), based on ideas by Seidenberg (see [25, 26]).

These methods have proved to be quite successful. Their common basis can be characterized as follows:

1. A translation of the geometrical assertion $\mathfrak{G}$ via a suitably positioned coordinate system into an algebraic statement φ involving multivariate polynomial equations.
2. The use of the corresponding algebraic method itself in an attempt to prove φ as a statement about *complex numbers*. Since φ is generally a universally quantified assertion, the validity of φ over the complex numbers entails the validity of φ over the reals and thus an automatic proof of the original geometrical assertion. If, in contrast, φ turns out to be false over the complex numbers, no decision on the validity of $\mathfrak{G}$ can be made.

* Supported by the DFG (Algorithmische Zahlentheorie und Algebra).

It is an amazing fact, which does not appear to have a sufficient theoretical explanation up to now, that for the overwhelming majority of theorems in the plane geometry of points, lines, circles, and cones the algebraic translation φ – if done "properly" – does hold in the field of complex numbers. Trivial exceptions may occur if the theorem asserts properties of points that do not exist in the real plane but exist in the complex plane; see our Example 12 in Section 5 taken from [7]. For a few examples of nontrivial exceptions, see [18] and our Example 7 in Section 5 taken from there.

A genuinely real method for deciding an algebraic translation of a geometric statement is provided by any decision method for the first-order theory of reals. A prominent example of such a real decision method by elimination of quantifiers is the CAD method by Collins and Hong [8] that is implemented in the QEPCAD package [15]. With the exception of Example 5 and Example 13, QEPCAD cannot cope with any of the automatic proof examples discussed in this paper. For an overview on real decision and quantifier elimination procedures, see [2], Section 2.3 of [16], and the bibliographies of [3, 24]. A combination of the Wu–Ritt method with QEPCAD for geometric theorem proving has been discussed in [22].

The "proper" formulation of an algebraic equivalent φ to a given geometrical assertion $\mathfrak{G}$ involves an adequate handling of *subsidiary* conditions. These consist of certain polynomial *disequations*, that is, negated polynomial equations that are required for the assertion $\mathfrak{G}$ to hold. Frequently, these subsidiary conditions can be interpreted as geometrical *nondegeneracy* conditions. There are several possibilities of how these conditions can be involved in some particular approach:

- They have to be found and added to a preliminary "naive" translation of $\mathfrak{G}$ by the user, then yielding the actual translation φ; see method 1 in [17].
- They are found automatically, provided the user has previously specified certain variables as *independent*; see method 2 in [17], [18, 19]. Such a specification of independent variables over $\mathbb{C}$ is not always completely obvious from the geometrical statement $\mathfrak{G}$; see [18, 21].
- They are found by the automatic prover without any human support; see [6, 27, 28].

In the two latter cases, the subsidiary conditions that are generated automatically may be stronger than needed for the validity of the geometrical assertion $\mathfrak{G}$.

The algebraic translation φ of $\mathfrak{G}$ is, as a rule, of the form

$$\bigwedge_{i=1}^{l} f_i(x_1, \ldots, x_k) = 0 \longrightarrow f_0(x_1, \ldots, x_k) = 0.$$

The complex methods considered above have the following strategy in common: First, the system $F = \{f_1, \ldots, f_l\}$ of polynomials is transformed into one or several systems of polynomials $G_1, \ldots, G_r$ the zero-sets of which are closely

related to that of F. The new systems are of some special form required by the corresponding method, for example, Gröbner bases or extended characteristic sets. In a next step, one attempts to *reduce* f_0 to zero wrt. all systems G_j. If all these reductions succeed, then φ holds in $\mathbb{C}$, and hence in $\mathbb{R}$, under some subsidiary conditions. In method 2 of [17], the conclusion enters the Gröbner basis to be computed already in the first step via the Rabinovich trick.

In the present note, we present an algebraic method for automatic theorem proving in geometry that differs from those described above by the following features:

1. The method does not work over the complex numbers but over the reals. It will therefore be able to prove the algebraic translation φ of a real geometric theorem $\mathfrak{G}$ even if φ fails in $\mathbb{C}$ (see Section 5, Examples 7, 12).

2. The input there may also contain polynomial order-inequalities (see Section 5, Examples 4, 5, 8, 9).

3. If the proof of the input conjecture φ fails in spite of all appropriate nondegeneracy conditions, the obtained result yields necessary and sufficient conditions for the conjecture to hold. These can be added as additional premises. In other words, we not only prove theorems but also *find* theorems (see Section 5, Examples 6, 18, 19).

4. In contrast to the CAD method by Collins and Hong [8], which has features 1–3 as well, our method is restricted to low degrees of the dependent variables. On the other hand, problems with many independent variables are usually handled better by our method.

5. The method uses iterated elimination of variables from the entire system in order to derive the desired conclusion. It thus avoids the computation of a normal form for the polynomial equations in the hypothesis. The fact that such computations do not involve the conclusion suggests that they are too general.

6. After specification of *parameters* in contrast to dependent variables, the method automatically constructs nondegeneracy conditions necessary for the given conjecture to hold.

Our method is derived from a general-purpose method for the elimination of a linear or quadratic variable from a Boolean combination of polynomial inequalities over the reals; see [20, 30, 33].

We have examined the applicability of our method to geometric reasoning only recently. Nearly all available data is presented in this paper.

In Section 2 we sketch the ideas governing the general method. Section 3 describes the changes and supplements to this method for geometric theorem proving. In Section 4 we describe the REDLOG package. In Section 5 we explain our method once more by example and then give some examples of automatic proofs. Section 6 summarizes the conclusions of this paper.

2. An Outline of the General Method

We consider *polynomial equations* $f = 0$, *weak polynomial inequalities* $f \geqslant 0$, $f \leqslant 0$, and *strict polynomial inequalities* $f > 0$, $f < 0$, $f \neq 0$, where f is a multivariate polynomial with rational coefficients. In order to distinguish the $f \neq 0$ from order inequalities, they are also called *disequations*. A *quantifier-free formula* ψ is a Boolean combination of such equations and inequalities obtained by applying the logical operators "$\wedge$," which stands for "and," and "$\vee$," which stands for "or." We call ψ of degree d in a variable x if all polynomials occurring in ψ have an x-degree of at most d. The x_i-degree of $f \in \mathbb{R}[x_1, \ldots, x_n]$ is the degree of the univariate polynomial $f \in \mathbb{R}[x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n][x_i]$.

Suppose now that ψ is quadratic (i.e., of degree 2) in some variable x, and denote $\exists x\big(\psi(x, u_1, \ldots, u_n)\big)$ by $\varphi(u_1, \ldots, u_n)$. Each u_i is either quantified further outside or a parameter. In the former case it will be eliminated by iterating the procedure described here. The algorithm given in [33] computes from φ a quantifier-free formula $\varphi^*(u_1, \ldots, u_n)$ not containing x such that over the field of the reals we have the equivalence

$$\varphi(u_1, \ldots, u_n) \longleftrightarrow \varphi^*(u_1, \ldots, u_n).$$

In other words, for arbitrary values $a_1, \ldots, a_n \in \mathbb{R}$ of the u_i, the assertion $\varphi^*(a_1, \ldots, a_n)$ holds in $\mathbb{R}$ iff there exists $b \in \mathbb{R}$ such that $\psi(b, a_1, \ldots, a_n)$ holds in $\mathbb{R}$. This is referred to as *quantifier elimination.*

The elimination of a universal quantifier can be reduced to that of an existential quantifier using the equivalence

$$\forall x \psi \longleftrightarrow \neg \exists x \neg \psi,$$

where "$\neg$" denotes logical negation. In our case, this works because the inner negation can be moved inside ψ using de Morgan's laws and can finally be encoded by modifying the contained equations and inequalities. For sketching the elimination method of [33], we may thus restrict ourselves to the elimination of an existential quantifier.

The idea for the construction of φ^* from φ is as follows: We fix real values a_i for the variables u_i. Then all polynomials occurring in ψ become linear or quadratic univariate polynomials in x with real coefficients. So the set

$$M_\varphi = \{b \in \mathbb{R} \mid \psi(b, a_1, \ldots, a_n)\}$$

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 $\alpha_1, \ldots, \alpha_m$ for the zeros can be computed uniformly in $u_1, \ldots, u_n$ by the solution formulas for linear and quadratic equations.

If all inequalities in ψ are weak, then all the intervals constituting M_φ will, into each direction, be either unbounded or closed. In the latter case, such an

interval will contain its real endpoint. Thus, M_φ is nonempty iff the substitution of $\pm\infty$ or of one of the candidate solutions α_j for x satisfies ψ. The substitution of $\pm\infty$ into a polynomial equation or inequality is evaluated in the obvious sense. The substitution of expressions in $u_1, \ldots, u_n$ of the form $(a + b\sqrt{c})/d$ among the α_j can be rewritten in such a way that all denominators involving the u_i and all square-root expressions are removed from the result; see [33]. By disjunctively substituting all candidates into ψ, we obtain a quantifier-free formula φ^* equivalent to $\exists x\psi$ over the reals. If ψ happens also to contain strict inequalities, we need to add to our candidates for points in M_φ expressions of the form $\alpha \pm \varepsilon$, where α is candidate solution for some left-hand side polynomial occurring in a strict inequality. The symbol ε stands for a positive infinitesimal number. Again, the substitution of these expressions into a polynomial equation or inequality can be rewritten in such a form that there occur neither denominators involving any of the u_i, nor any square root expressions, nor the symbol ε in the result; see [33]. Again, this yields a quantifier-free formula φ^* equivalent to $\exists x\psi$ over the reals. For practical applications, this method has to be refined by a careful selection of a smaller number of candidate solutions and by a combination with powerful simplification techniques for quantifier-free formulas; see [14] for details.

Recall that the well-known solution formula for quadratic equations $ax^2 + bx + c = 0$ requires $a \neq 0$. In our situation a is a term in $u_1, \ldots, u_n$, so $a \neq 0$ can in general not be decided uniformly but depends on the interpretation of the u_i. Thus, a quadratic polynomial $ax^2 + bx + c$ delivers not only two square-root expressions α_1 and α_2 as candidate solutions but also $\alpha_3 = -c/b$, which in turn requires $b \neq 0$. Let t_1, t_2, and t_3 be the candidate points for M_φ obtained from α_1, α_2, and α_3, respectively, by possibly adding or subtracting ε. With the substitution of the t_i into ψ, it is necessary to add the conditions on the nonvanishing of a and b. Formally, we obtain

$$\big(a \neq 0 \wedge \Delta \geqslant 0 \wedge (\psi[x/t_1] \vee \psi[x/t_2])\big) \vee \big(a = 0 \wedge b \neq 0 \wedge \psi[x/t_3]\big),$$

where Δ denotes the discriminant of the equation $ax^2 + bx + c = 0$. If, however, a is a rational constant, then the case distinction is superfluous. In particular, if a is nonzero, the second case can be dropped.

As indicated above, dramatic improvements of the general procedure sketched up to now can be obtained by reducing the number of test candidates for M_φ depending on the structure of the formula ψ; see [20, 33]. One simple instance for such an improvement is the following natural extension of *Gauss elimination*: Suppose ψ is of the form

$$bx + c = 0 \wedge \psi_1,$$

where at least one of the coefficient terms b, c is a rational nonzero constant. Then we know that under any interpretation of the u_i the equation is *nontrivial*, that is, different from $0 = 0$. Hence the only test candidate required in the construction of φ^* is $-c/b$, substituted, of course, with the condition $b \neq 0$. No additional test

candidates arising from equations or inequalities in the remainder ψ_1 of ψ need be considered. This idea can easily be extended to a quadratic equation instead of a linear one, taking into account again the discriminant.

We have seen that it is convenient to be able to decide whether coefficients are nonzero or not. To support such decisions, the elimination procedure may, more generally, allow as additional input a *theory* $\vartheta(u_1, \ldots, u_n)$. This is a conjunction of polynomial equations and inequalities in the parameters that may serve as a global hypothesis for the equivalence between $\exists x \psi$ and φ^*. In other words, the equivalence is asserted only for those real values of the u_i that satisfy ϑ. Then both simpler substitution and Gauss elimination can also be performed if the required coefficient conditions are part of the theory or can be automatically inferred from it.

Successive elimination of several existential and universal quantifiers by the method is possible as long as after each elimination step the degree of the next variable to be eliminated is at most 2 in the quantifier-free formula resulting from previous eliminations. Notice that the elimination of an innermost variable in general increases the degree of the outer variables in the elimination result compared with the original matrix formula ψ.

There are two techniques for coping with problems of a degree larger than 2. The first one is a *shift* in the degrees of a quantified variable x in a quantifier-free formula ψ in the following sense: Let g be the GCD of all exponents x occurs with in ψ. We divide all exponents of x in ψ by g yielding ψ'. If g is odd, we have $\exists x \psi \longleftrightarrow \exists x \psi'$; if g is even, we have $\exists x \psi \longleftrightarrow \exists x (x \geqslant 0 \wedge \psi')$. For $g > 1$ this reduces the x-degree of ψ. To obtain larger GCD's and hence a better degree reduction, we may in advance "adjust" the degree $n > 0$ of x in polynomials of the form $x^n f$, where x does not occur in f: In equations and disequations, n may be equivalently replaced by any $m > 0$. In ordering inequalities we may choose any $m > 0$ of the same parity as n.

The second method is *implicit factorization* of polynomials: Suppose we want to eliminate a variable x from $\exists x \psi$, where x is of a degree greater than 2 in the quantifier-free formula ψ but such that every polynomial of x-degree greater than 2 factors over $\mathbb{Q}$ into factors at most quadratic in x. We can then *in our minds* replace ψ by an equivalent formula ψ' that is at most quadratic in x. Taking into account which relations occur with the factors in ψ', we can use the zeros of the factors wrt. the variable x for constructing test candidates.

Because of the degree restrictions, our general method and hence also its adaption to geometric proving is fairly sensitive to the *formulation* of problems. This concerns both efficiency and succeeding at all (see Section 5, Example 14 vs. Example 15).

The method in this general form has been applied successfully to examples in industrial simulation and optimization; see [34].

A systematic extension of the method to arbitrary degrees has been sketched in [33]. The cubic case has been worked out in detail in [32].

3. Adapting the Method to Geometric Theorem Proving

Most of the geometric theorems considered so far in automatic theorem proving are closure theorems, asserting that for a certain configuration of points, lines, or circles in the real plane or real 3-space some of these points lie on a line or a circle or some of the lines intersect in a common point; see [7, 18, 39]. In an algebraic translation, theorems of this kind yield *universal Horn formulas*, that is, formulas of the type

$$\forall x_1 \ldots \forall x_k \left(\bigwedge_{i=1}^{l} f_i(x_1, \ldots, x_k) = 0 \longrightarrow f_0(x_1, \ldots, x_k) = 0 \right).$$

This allows one to apply methods based on the manipulation of systems of polynomial equations, as sketched in the introduction.

In contrast, our method derived from the quantifier elimination procedure sketched in the preceding section is not restricted to formulas of such a special form. Our algebraic translations φ may be arbitrary first-order formulas

$$\mathsf{Q}_1 x_1 \ldots \mathsf{Q}_n x_n \big(\psi(x_1, \ldots, x_n, u_1, \ldots, u_m)\big), \quad \mathsf{Q}_1, \ldots, \mathsf{Q}_n \in \{\exists, \forall\},$$

where ψ is a Boolean combination of polynomial equations, disequations, and order inequalities subject to degree restrictions wrt. the quantified variables $x_1, \ldots, x_n$.

We do not expect ψ to be true in the literal sense, that is, for all real values of the variables $u_1, \ldots, u_m$. Instead, we implicitly assume that the given configuration is *nondegenerate*: A given triangle should not degenerate to a line segment, a given circle should not degenerate to a point, and so on. On the algebraic side, these nondegeneracy conditions are reflected in the assertion that certain of the variables representing, for example, coordinates of points or coefficients of straight line equations should not satisfy some "unexpected" polynomial equation $g(u_1, \ldots, u_m) = 0$. These variables, namely, $u_1, \ldots, u_m$, are *parameters*. They remain unquantified.

A strong interpretation of the implicit assumption on the parameters would assert that $u_1, \ldots, u_m$ are assumed to be algebraically independent over the field $\mathbb{Q}$ of rational numbers. A more cautious interpretation may assert only that $u_1, \ldots, u_m$ satisfy such polynomial inequalities $g(u_1, \ldots, u_m) \neq 0$ that encode nondegeneracy conditions for the geometrical input problem $\mathfrak{G}$.

In our method, we will automatically generate assumptions stating that certain coefficients in the parameters are nonzero. We have seen in the preceding section that such assumptions can simplify substitution or enable Gauss elimination. In practice, it turns out that in most cases the assumptions made are actually geometrical nondegeneracy conditions. We call this modified quantifier elimination procedure *generic quantifier elimination*.

Given a geometrical statement $\mathfrak{G}$, we proceed as follows. We manually produce a "naive" algebraic translation φ by writing down polynomial relations between the

coordinates of points, coefficients of straight line equations, circle equations, etc. in a conveniently chosen coordinate system. We do *not* specify any conditions saying that the configuration is nondegenerate. Instead, we specify certain of the variables in φ as parameters, that is, independent variables, $u_1, \ldots, u_m$. As with the general method, we may specify a theory $\vartheta(u_1, \ldots, u_m)$ consisting of a conjunction of weak polynomial order inequalities in the parameters. Typically, for parameters u_i ranging over lengths of certain line segments, ϑ will contain an inequality $u_i \geqslant 0$.

Then the general elimination procedure described in the preceding section is applied to $\varphi(u_1, \ldots, u_m)$ and $\vartheta(u_1, \ldots, u_m)$ with the following modifications: In substitutions, all nontrivial equality conditions $a(u_1, \ldots, u_m) = 0$ for coefficients involving only parameters are assumed to fail. The corresponding disequations $a \neq 0$ are added to ϑ.

Recall from the preceding section that the substitutions also contain discriminant conditions. Intermediate simplification might equivalently replace such a condition $\Delta(u_1, \ldots, u_m) \geqslant 0$ in the parameters by an equation $\Delta'(u_1, \ldots, u_m) = 0$. For instance, $-d^2 \geqslant 0$ is equivalent to $d = 0$. This equation is then treated the same way as the coefficient conditions above. Notice that we do not add any new order inequalities to our theory. That is, our set of automatic assumptions cannot become inconsistent. Moreover, we neglect only a set of parameter values of measure zero.

Whenever a formula $bx + c = 0 \wedge \psi_1$ occurs but none of the coefficients b, c is a nonzero rational constant, it is checked whether any of them is a polynomial only in the parameters. If this is the case, say b does not contain any quantified variable, we add $b \neq 0$ to ϑ and perform Gauss elimination. For quadratic equations we proceed analogously. Note that we cannot make assumptions on quantified (i.e., dependent) variables.

There are situations where we have to decide between a linear Gauss elimination with a nonzero assumption on a coefficient and a quadratic one without such an assumption. For instance, consider

$$\exists x_2 \exists x_1 \big(u x_1 + x_2 = 0 \wedge x_1^2 + x_2 x_1 + u = 0 \wedge \psi_1(x_1, x_2, u) \big).$$

In spite of the necessary assumption $u \neq 0$, we prefer the linear Gauss application for the elimination of x_1 because the quadratic equation would produce square root expressions the substitution of which into ψ_1 may increase the degree of x_2.

Consider a possible Gauss application with assumption for a variable x, where several coefficients can be assumed to be nonzero. We then select the coefficient belonging to the highest power of x. It is not hard to see that this option saves conditions or cases in the corresponding substitution.

As an option, we can restrict the set of allowed assumptions to those being of the form $\prod_i u_i^{e_i} \neq 0$, which is equivalent to $\bigwedge_i u_i \neq 0$. This is typically used to avoid subsidiary conditions that cannot be interpreted geometrically (cf. Section 5, Example 7).

The output of our modified procedure consists in a quantifier-free formula $\varphi^*(u_1, \ldots, u_m)$ and a new theory $\vartheta^*(u_1, \ldots, u_m)$, which extends ϑ, that is, $\vartheta^* \longrightarrow \vartheta$, such that

$$\forall u_1 \ldots \forall u_m \big(\vartheta^* \longrightarrow (\varphi \longleftrightarrow \varphi^*)\big)$$

holds over the reals.

If φ^* equals "true," then we have proved φ and thus the geometrical assertion $\mathfrak{G}$ under the nondegeneracy conditions contained in ϑ^*. Notice that ϑ^* also undergoes simplification such that neither the conditions contained in ϑ nor the ones added need occur there literally.

Otherwise, it is still possible that φ^* holds wrt. ϑ^*, in other words,

$$\forall u_1 \ldots \forall u_m (\vartheta^* \longrightarrow \varphi^*).$$

This can be checked automatically by using some – unmodified – quantifier elimination procedure such as that of Section 2, if the degrees allow us to do so, or partial CAD. If we succeed in eliminating all the quantifiers, we definitely know whether the input conjecture φ is a theorem wrt. ϑ^* or not.

In the latter case there are two possibilities. Either our method has not found all necessary nondegeneracy conditions, that is, ϑ^* is not sufficient for φ to be an appropriate algebraic translation of the geometrical conjecture $\mathfrak{G}$, or $\mathfrak{G}$ itself does not hold in the claimed generality.

If we suspect that there are simply nondegeneracy conditions missing, we can apply a *theory generator*. This is a procedure that enlarges ϑ^* by further disequations until it (one hopes) implies φ^*. The technique is based on adding disequations that occur literally in φ^*. This procedure can certainly fail, which happens in particular when there are only few disequations in φ^* or none at all.

Notice, however, that in either case φ^* specifies additional constraints on the parameters $u_1, \ldots, u_m$ that are necessary and sufficient for the validity of $\mathfrak{G}$ under ϑ^*.

Both φ^* and ϑ^* can thus be used in order to turn a not-generally-valid geometrical conjecture $\mathfrak{G}$ into a true geometrical theorem, provided one succeeds in a geometrical back-translation of the algebraic assertions ϑ^* and φ^*.

4. The REDUCE Package REDLOG

REDLOG [11, 13] stands for REDuce LOGic system. It provides an extension of the computer algebra system REDUCE to a *computer logic system* implementing symbolic algorithms on first-order formulas wrt. temporarily fixed first-order languages and theories. For the purpose of this paper we are interested in the theory of *real closed fields* over the language of ordered rings. In contrast to *constraint logic programming* systems [9], not only is the algebraic component used for supporting the logical engine but the largest part of the logical algorithms is defined and implemented in terms of algebraic algorithms.

The algorithms implemented in REDLOG include the following:

- Several techniques for the *simplification* of quantifier-free formulas. The simplifiers not only operate on the Boolean structure of the formulas but also discover algebraic relationships. For this purpose, we make use of advanced algebraic concepts such as Gröbner basis [4] computations. For the notion of simplification and a detailed description of the implemented techniques, see [14].
- Quantifier elimination.
  - For formulas obeying certain degree restrictions, we use elimination set ideas [20, 30, 33].
  - There is also an interface to Hoon Hong's QEPCAD [15] package implementing a complete quantifier elimination.
- The generic quantifier elimination described in this paper.
- Variants of both conventional and generic quantifier elimination that provide answers, for example, satisfying sample points for existentially quantified formulas.
- A lot of useful tools for constructing, decomposing, and analyzing formulas.

REDLOG has been applied successfully for the solution of nonacademic problems, mainly for the simulation and error-diagnosis of physical networks [34].

Applications inside the scientific community include the following:

- Control theory [1].
- Stability analysis for PDEs [16].
- Geometric reasoning as described in this paper.
- Parametric scheduling.
- Nonconvex parametric linear and quadratic optimization [31].
- Transportation problems [20].
- Real implicitization of algebraic surfaces.
- Computation of comprehensive Gröbner bases.
- Implementation of *guarded expressions* for coping with degenerate cases in the evaluation of algebraic expressions [10, 12].

Some very promising work has been done in parallelizing the ordered field optimization code under PVM on a CRAY YMP4/T3D in cooperation with the Konrad-Zuse-Zentrum in Berlin.

For noncommercial use, the REDLOG source code is freely available on the WWW.*

* http://www.fmi.uni-passau.de/~redlog/

REDLOG is not implemented as an algebraic mode REDUCE program, but extends REDUCE on the (compiled) Lisp level using the built-in facilities as a library. The REDUCE facilities used are the following:

- polynomial representation,
- polynomial arithmetic and factorization, and
- list processing.

5. Examples

5.1. SAMPLE PROOFS

We are going to illustrate by two simple examples how our method works. The first example shows how nondegeneracy conditions are introduced and how we reduce universal quantifiers to existential quantifiers. It is, however, rather trivial concerning the elimination set construction: the elimination of both quantifiers can be reduced to our extended notion of Gauss elimination.

EXAMPLE 1. Two lines intersect in one and only one point.

The first line is modeled by the x-axis, the second one by an affine linear function $mx + b$:

$$\exists x\big(mx + b = 0 \ \wedge \ \forall y(y \neq x \longrightarrow my + b \neq 0)\big).$$

We start with making the formula positive and prenex:

$$\exists x \forall y\big(mx + b = 0 \ \wedge \ (y = x \ \vee \ my + b \neq 0)\big).$$

The elimination of $\forall y$ is reduced to that of

$$\neg\exists y\big(mx + b \neq 0 \ \vee \ (y \neq x \ \wedge \ my = -b)\big).$$

Since $mx + b \neq 0$ is independent of y, we may restrict our attention to the nested conjunction. We add $m \neq 0$ to our theory. Under this assumption the equation $my = -b$ is nontrivial, and it suffices to substitute $\frac{-b}{m}$ as a test term. The result is the following:

$$\neg\big(0 \neq 0 \ \vee \ (-b \neq mx \ \wedge \ -b = -b)\big).$$

After encoding the negation "$\neg$" into the atomic formulas, simplifying, and renormalizing wrt. the next quantifier $\exists x$, we have

$$mx = -b.$$

We have already made the assumption $m \neq 0$; hence the remaining equation is nontrivial. We substitute $\frac{-b}{m}$ for x obtaining "true" as the final elimination result.

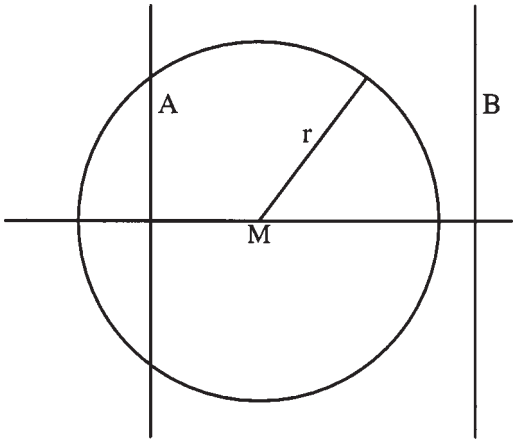

Figure 1. Intersection between a strip and a disk (Example 2).

The nondegeneracy condition $m \neq 0$ states that our two lines not be parallel. Our general method would have introduced case distinctions wrt. the vanishing of m.

The second example elucidates how we cope with inequalities and quadratic variables.

EXAMPLE 2. Consider in 2-space a disk with center M and radius r, and two parallel lines A, B. Find necessary and sufficient conditions for the strip between A and B to have a nonempty intersection with the disk (see Figure 1).

In our algebraic translation, we denote by (x, y) a point that is both inside the strip and inside the disk. For demonstration purposes we locate the center M of the disk at $(-1, 0)$. The lines A and B are defined as $\{(a, y) \mid y \in \mathbb{R}\}$ and $\{(b, y) \mid y \in \mathbb{R}\}$, respectively:

$$\exists x \exists y \big((x+1)^2 + y^2 \leqslant r^2 \ \wedge\ a \leqslant x \ \wedge\ x \leqslant b\big).$$

We start with the elimination of $\exists y$. The purely quadratic occurrence of y allows a shift $h = y^2$:

$$\exists h \big(h \leqslant r^2 - (x+1)^2 \ \wedge\ h \geqslant 0 \ \wedge\ a \leqslant x \ \wedge\ x \leqslant b\big).$$

There is both a lower bound 0 and an upper bound $r^2 - (x+1)^2$ for h. In this situation, we know that it suffices to substitute either all upper bounds together with the formal symbol $-\infty$ or all lower bounds together with ∞. We decide for the elimination set $\{\infty, r^2 - (x+1)^2\}$ yielding

$$\begin{aligned}&(\text{false} \wedge \text{true} \wedge a \leqslant x \wedge x \leqslant b)\\ &\quad \vee \big(r^2 - (x+1)^2 \leqslant r^2 - (x+1)^2 \wedge r^2 - (x+1)^2 \geqslant 0\\ &\quad \wedge a \leqslant x \wedge x \leqslant b\big).\end{aligned}$$

Note that we know the direction of the bounds because h does not occur with a parametric coefficient in the respective atomic formulas. In connection with strict inequalities there would also occur terms including infinitesimal formal symbols $\pm\varepsilon$. The substitution of terms with formal symbols into atomic formulas is described in [33].

After simplification and renormalization wrt. the next quantifier $\exists x$, we have

$$(x+1)^2 \leqslant r^2 \wedge x \geqslant a \wedge x \leqslant b$$

including linear bounds a, b, and quadratic bounds $r-1$ and $-r-1$ for x. We do not have to substitute the quadratic bounds because we are in an important special case: There is only one quadratic inequality. This can be treated by substituting the zero -1 of the derivative

$$\frac{\partial\big((x+1)^2 - r^2\big)}{\partial x} = 2x - 2.$$

This will not increase the degree in the parameters, which are possibly quantified from outside. Proceeding this way, however, we cannot decide between linear lower or upper bounds. Disjunctive substitution of the elimination set $\{a, b, -1, -\infty, \infty\}$ yields

$$\begin{aligned}&\big((a+1)^2 \leqslant r^2 \wedge a \geqslant a \wedge a \leqslant b\big)\\ &\quad\vee\big((b+1)^2 \leqslant r^2 \wedge b \geqslant a \wedge b \leqslant b\big) \vee (0 \leqslant r^2 \wedge -1 \geqslant a \wedge -1 \leqslant b)\\ &\quad\vee(\text{false} \wedge \text{false} \wedge \text{true}) \vee (\text{false} \wedge \text{true} \wedge \text{false}).\end{aligned}$$

In general, one has to substitute all the roots of the quadratic constraints possibly with $\pm\varepsilon$. Note that these roots can contain surds. In [33] there is described how to substitute the roots in such a way that the substitution result does not contain any surds.

Our sample elimination result is automatically simplified to the following quantifier-free formula:

$$\big((a+1)^2 \leqslant r^2 \wedge a \leqslant b\big) \vee \big((b+1)^2 \leqslant r^2 \wedge b \geqslant a\big) \vee (a \leqslant -1 \leqslant b).$$

5.2. AUTOMATIC PROOFS

As mentioned in the preceding section, REDLOG provides an interface to Hoon Hong's QEPCAD: it can spawn a QEPCAD process, communicate formulas to it, receive the results, and convert them back to its own internal formula format. We have actually tried to compute all examples discussed in this section with QEPCAD, which failed in most cases, probably because of the large number of variables. On the other hand, QEPCAD does a good job in checking whether $\vartheta^* \longrightarrow \varphi^*$ after application of our method, since both ϑ^* and φ^* contain only few variables, namely, at most the parameters u_i of the input problem φ.

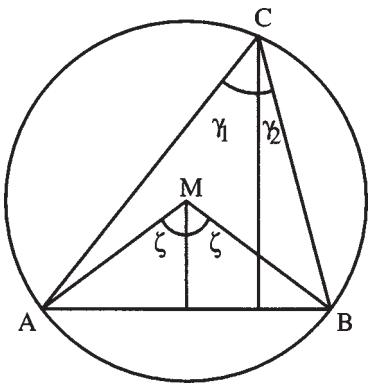

Figure 2. The angle at circumference is half the angle at center (Example 3).

We start with discussing the automatic proof of some examples of real geometry taken from Wu [40], Wang [28], Kutzler [18], and McPhee, Chou, and Gao [22]. Then we summarize the timings and solutions of several examples taken from Chou [7]. Most of the latter can also be proved by complex methods. All computations have been performed on a SUN SPARC-4 workstation using 10^6 Lisp cells. Such a cell takes four bytes of memory.

EXAMPLE 3 (angle at circumference vs. angle at center). Let M be the center of the circumcircle of a triangle ABC. Then $\angle ACB = \angle AMB/2$ (see Figure 2).

We choose coordinates $A = (-a, 0)$, $B = (a, 0)$, $C = (x_0, y_0)$, and $M = (0, b)$. The radius of the circumcircle is determined by

$$c^2 = a^2 + b^2 = x_0^2 + (y_0 - b)^2.$$

The angles are encoded into tangents: We construct $\angle ACB = \gamma_1 + \gamma_2$ with $y_0 \tan(\gamma_1) = a + x_0$, and $y_0 \tan(\gamma_2) = a - x_0$. By the addition theorem for tangents we know

$$\big(1 - \tan(\gamma_1)\tan(\gamma_2)\big)\tan(\gamma_1 + \gamma_2) = \tan(\gamma_1) + \tan(\gamma_2).$$

Let $\zeta = \angle AMB/2$. Then $b\tan(\zeta) = a$, and our claim is that $\tan(\zeta) = \tan(\gamma_1 + \gamma_2)$. Our translation φ with $t_1 = \tan(\gamma_1)$, $t_2 = \tan(\gamma_2)$, and $t = \tan(\zeta)$ reads as follows:

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

After 102 ms of computation time, we obtain $\varphi^* \equiv$ true and the nondegeneracy condition $\vartheta^* \equiv y_0 \neq 0$ stating that ACB is a nondegenerate triangle.

EXAMPLE 4 (median bisector theorem). For a nonisosceles triangle ABC the median over the side AB is always greater than the interior bisector on the same side (see Figure 3).

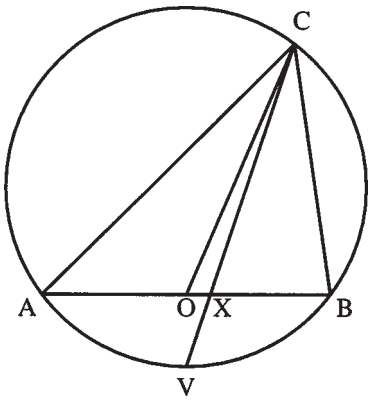

Figure 3. The median bisector theorem (Example 4).

This example and the ideas for its algebraic translation are taken from Wu [40], pp. 7–8. To prove the theorem, we take coordinates such that

$$A = (-1, 0), \quad B = (1, 0), \quad C = (x_0, y_0).$$

We may wlog. assume that $y_0 > 0$. Since the origin $O = (0, 0)$ is the midpoint of AB, we have that CO is the median on AB. We construct the bisector using the geometric theorem proved as Example 3: The center of the circumcircle is at $(0, b)$. Let $c > 0$ be its radius. Then $c^2 = 1 + b^2$, and $V = (0, b - c)$ is the lower extremity of the circumcircle. Let $X = (x, 0)$ be the intersection between CV and AB. Then CX is the interior bisector on the side AB. We come to the following translation φ with parameters x_0 and y_0:

$$\forall b \forall c \forall x \big(y_0 > 0 \wedge c > 0 \wedge c^2 = 1 + b^2 \wedge c^2 = x_0^2 + (y_0 - b)^2 \\ \wedge x\big(y_0 + (c - b)\big) = x_0(c - b) \longrightarrow x_0^2 + y_0^2 > (x_0 - x)^2 + y_0^2 \big).$$

After 714 ms elimination time, we obtain the nondegeneracy conditions $\vartheta^* \equiv x_0 \neq 0 \wedge y_0 \neq 0$, stating that ABC is a nondegenerate, plus a quantifier-free equivalent φ^* containing 18 atomic formulas. QEPCAD subsequently proves in 1283 ms that $\vartheta^* \longrightarrow \varphi^*$, which proves the theorem. This final step cannot be performed by our method because of the degree restrictions.

The next example is taken from Wang [28], pp. 158–160.

EXAMPLE 5 (Pedoe's inequality). Given two arbitrary triangles ABC and $A'B'C'$ with sides a, b, c and a', b', c', respectively, the areas Δ and Δ' of this triangles satisfy the following inequality:

$$a'^2(b^2 + c^2 - a^2) + b'^2(c^2 + a^2 - b^2) + c'^2(a^2 + b^2 - c^2) \geqslant 16\Delta'\Delta.$$

Wang's algebraic translation of this inequality slightly adopted to our framework reads as follows:

$$\forall a \forall a' \forall x \forall x' \forall y \forall y' (a \geqslant 0 \wedge a' \geqslant 0 \wedge x \geqslant 0 \wedge x' \geqslant 0 \wedge y \geqslant 0 \\ \wedge y' \geqslant 0 \longrightarrow a^2x'^2 + a^2y'^2 - 2aa'xx' - 2aa'yy' + a'^2x^2 + a'^2y^2 \geqslant 0).$$

After 102 ms we obtain $\varphi^* \equiv$ true without any subsidiary condition. QEPCAD yields the same result in 583 ms.

In the following example also taken from Wang [28], pp. 161–162, we not only prove but actually *find* a theorem.

EXAMPLE 6 (Qin–Heron's formula). Determine the area F of a triangle ABC in terms of its three sides.

We locate $A = (-z, 0)$, $B = (z, 0)$, and $C = (x_0, y_0)$. Then the side lengths are determined as follows: $a > 0$ with $a^2 = (z - x_0)^2 + y_0^2$, $b > 0$ with $b^2 = (z + x_0)^2 + y_0^2$, and $c = 2z$. On the other hand, we know $F = zy_0$. This yields our translation φ with parameters a, b, and c:

$$\exists x_0 \exists y_0 \exists z \big(F = zy_0 \\ \wedge\ a^2 = (z - x_0)^2 + y_0^2 \wedge b^2 = (z + x_0)^2 + y_0^2 \wedge c = 2z \big).$$

We put the conditions that the side lengths be positive into our input theory $\vartheta \equiv a \geqslant 0 \wedge b \geqslant 0 \wedge c \geqslant 0 \wedge f \geqslant 0$. After 136 ms we obtain $\vartheta^* \equiv a \geqslant 0 \wedge b \geqslant 0 \wedge c > 0 \wedge f \geqslant 0$; in other words, the condition $c \neq 0$ stating that the points A and B are different is added. The quantifier-free formula φ^* obtained contains five atomic formulas. Automatic simplification of φ^* wrt. ϑ^* by Gröbner basis methods, cf. [14], takes 136 ms, yielding

$$a^4 - 2a^2b^2 - 2a^2c^2 + b^4 - 2b^2c^2 + c^4 + 16F^2 = 0 \wedge a^2c^2 - 4F^2 \geqslant 0.$$

The inequality follows from the equation, as our pure quantifier elimination method shows in 34 ms. Alternatively, QEPCAD proves this in 1716 ms. Setting $s = (a + b + c)/2$, the equation can be rewritten as Heron's formula

$$F^2 = s(s - a)(s - b)(s - c).$$

EXAMPLE 7. Consider eight points $A, \ldots, H$ such that the following eight triples are collinear ABD, BCE, CDF, DEG, EFH, FGA, GHB, HAC. Then all eight points lie on a line.

This example is originally due to MacLane [21]. It holds in the real plane but fails in the complex one. We adopt the translation proposed by Kutzler [18], p. 154, setting $A = (0, 0)$, $B = (x_b, 0)$, $C = (x_c, y_c)$, $D = (x_d, 0)$, $E = (x_e, y_e), \ldots, H = (x_h, y_h)$:

$$\forall y_h \forall x_e \forall y_e \forall x_f \forall y_f \forall x_g \forall y_g (x_h y_c - x_c y_h = 0 \wedge x_g y_f - x_f y_g = 0 \\ \wedge x_b y_e - x_c y_e + x_e y_c - x_b y_c = 0 \wedge x_b y_h - x_g y_h + x_h y_g - x_b y_g = 0 \\ \wedge x_c y_f - x_d y_f - x_f y_c + x_d y_c = 0 \wedge x_d y_g - x_e y_g + x_g y_e - x_d y_e = 0 \\ \wedge x_e y_h - x_f y_h + x_h y_f - x_e y_f - x_h y_e + x_f y_e = 0 \longrightarrow x_b y_c = 0).$$

For understanding the translation, notice that (x_1, y_1), (x_2, y_2), and (x_3, y_3) are collinear iff

$$(y_2 - y_1)x_3 + (x_1 - x_2)y_3 + (x_2y_1 - x_1y_2) = 0.$$

We get after 8432 ms the elimination result $\varphi^* \equiv$ true. The subsidiary conditions ϑ^* obtained are

$$\begin{aligned}
&x_b^2x_h^2 - x_bx_cx_dx_h - x_bx_dx_h^2 + x_c^2x_d^2 - x_cx_d^2x_h + x_d^2x_h^2 \neq 0\\
&\quad \wedge x_b^2x_h - x_bx_cx_d - x_bx_cx_h + x_cx_dx_h \neq 0\\
&\quad \wedge x_b^2x_h - x_bx_cx_d - x_bx_dx_h + x_d^2x_h \neq 0\\
&\quad \wedge x_b - x_c \neq 0 \wedge x_b - x_d \neq 0 \wedge x_b - x_h \neq 0 \wedge x_c - x_d \neq 0\\
&\quad \wedge x_c - x_h \neq 0 \wedge x_c \neq 0 \wedge x_d \neq 0 \wedge x_h \neq 0.
\end{aligned}$$

Except for the first three disequations, all these conditions are obvious geometrical nondegeneracy conditions. The first disequation follows from the geometrical ones, as our general method proves in 1054 ms, and is thus redundant.

We rerun our method with the option permitting only monomial assumptions: After 15,572 ms we obtain a quantifier-free formula φ^* with 205 atomic formulas and the following nondegeneracy conditions ϑ^*:

$$x_c \neq 0 \wedge x_h \neq 0 \wedge y_c \neq 0.$$

Within 31,246 ms, our theory generator adds to ϑ^* assumptions, which make it sufficient for φ^* and thus for φ:

$$\begin{aligned}
&x_b^2x_h^2 - x_bx_cx_dx_h - x_bx_dx_h^2 + x_c^2x_d^2 - x_cx_d^2x_h + x_d^2x_h^2 \neq 0\\
&\quad \wedge x_b - x_d \neq 0 \wedge x_c - x_h \neq 0 \wedge x_c \neq 0 \wedge x_d \neq 0\\
&\quad \wedge x_h \neq 0 \wedge y_c \neq 0.
\end{aligned}$$

Again, our general method proves that the first disequation follows from the remaining nondegeneracy conditions (340 ms).

Examples 8 and 9 are taken from McPhee, Chou, and Gao [22], pp. 410–411 and 414, respectively.

EXAMPLE 8 (Pompeiu's theorem). If ABC is a equilateral triangle, and P is some point not on the circumcircle of ABC, then the segments AP, BP, CP can be used to form a triangle (i.e., the sum of the lengths of any two exceeds the length of the third).

We first adopt the algebraic formulation given in [22], p. 411:

$$\begin{aligned}
&\forall x_0 \forall x_1 \forall x_2 \forall x_3 \forall x_4 \forall u_0 \forall u_1 (4x_0^2 - 3 = 0 \wedge 2x_1 + 1 = 0\\
&\quad \wedge x_4^2 - 2x_4 + x_3^2 - u_0^2 + 1 = 0 \wedge u_0 > 0\\
&\quad \wedge x_4^2 - 2x_1x_4 + x_3^2 + 2x_0x_3 + x_1^2 + x_0^2 - u_1^2 = 0 \wedge u_1 > 0\\
&\quad \wedge x_4^2 - 2x_1x_4 + x_3^2 - 2x_0x_3 - x_2^2 + x_1^2 + x_0^2 = 0 \wedge x_2 > 0\\
&\quad \wedge x_4^2 + x_3^2 - 1 \neq 0 \longrightarrow x_2 - u_0 - u_1 < 0).
\end{aligned}$$

Note that the nondegeneracy condition $\gamma \equiv x_4^2 + x_3^2 - 1 \neq 0$ is explicitly added as a hypothesis. Eliminating all the quantifiers yields "true" after 391 ms.

Next, we delete γ from the hypotheses and eliminate only the dependent variables u_0, u_1, x_2. Our procedure yields after 202 ms a formula containing 7 atomic formulas. Unfortunately, it does not make any assumption. We proceed by eliminating also x_0 and x_1 in order to find a necessary and sufficient condition in terms of the point (x_3, x_4) for the theorem to hold. This elimination yields 12 atomic formulas after 187 ms. The Gröbner simplifier reduces this result within 153 ms to the following necessary and sufficient condition:

$$x_3^2 + x_4^2 - 1 \neq 0 \\ \quad \vee 2x_4^2 - x_4 - 1 > 0 \vee 2x_4 + 1 = 0 \vee x_4 + 2 \leqslant 0 \vee x_4 - 1 \geqslant 0.$$

In the second condition $2x_4^2 - x_4 - 1 > 0$, we can factorize the left-hand side, yielding

$$x_3^2 + x_4^2 - 1 \neq 0 \\ \quad \vee (x_4 - 1 > 0 \wedge 2x_4 + 1 > 0) \vee (x_4 - 1 < 0 \wedge 2x_4 + 1 < 0) \\ \quad \vee 2x_4 + 1 = 0 \vee x_4 + 2 \leqslant 0 \vee x_4 - 1 \geqslant 0,$$

which our standard simplifier immediately (0 ms) turns into

$$x_3^2 + x_4^2 - 1 \neq 0 \vee 2x_4 + 1 \leqslant 0 \vee x_4 - 1 \geqslant 0.$$

An extension of the standard simplifier, which automatically tries such expansions, is already implemented but not yet published.

The inequality $x_3^2 + x_4^2 - 1 \neq 0$ requires that (x_3, x_4) not be on the circumcircle. Surprisingly, the condition $2x_4 + 1 \leqslant 0$ allows (x_3, x_4) to be on the circumcircle provided that it lies below or on the basis BC. Similarly, the condition $x_4 - 1 \geqslant 0$ allows (x_3, x_4) to coincide with the vertex A. The reason is that the formulation $x_2 - u_0 - u_1 < 0$ of the conclusion is asymmetric, leaving out the cases $u_0 - x_2 - u_1 < 0$ and $u_1 - u_0 - x_2 < 0$. The vertices A, B, and C are excluded already by the hypothesis.

EXAMPLE 9 (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 by using the geometrical theorem proved as Example 3: Let $V = (0, b - c)$ 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:

$$\begin{aligned}&\forall b\forall c\forall x\forall x_1\forall y_1\forall x_2\forall y_2\big(y_1(x_0+1) > x_1y_0 \wedge y_0 > 0 \wedge c > 0\\ &\quad\wedge c^2 = 1 + b^2 \wedge c^2 = x_0^2 + (y_0 - b)^2 \wedge x\big(y_0 + (c - b)\big) = x_0(c - b)\\ &\quad\wedge x_1^2 + (y_1 - b)^2 = c^2 \wedge (x_1 + 1)^2 + y_1^2 = (x_1 - x_0)^2 + (y_1 - y_0)^2\\ &\quad\wedge (x_1 - 1)y_2 = y_1(x_2 - 1) \wedge (x_0 + 1)y_2 = y_0(x_2 + 1)\\ &\quad\wedge 4 > (x_0 + 1)^2 + y_0^2 \longrightarrow (x - x_0)^2 + y_0^2 < (x_2 - 1)^2 + y_2^2\big).\end{aligned}$$

We obtain after 142,103 ms an elimination result φ^* containing 243 atomic formulas together with the subsidiary conditions

$$\begin{aligned}\vartheta^* \;\equiv\; & x_0^2 + 2x_0 + y_0^2 + 1 \neq 0\\ & \wedge x_0^2 - 2x_0 + y_0^2 - 3 \neq 0 \wedge x_0 + 1 \neq 0 \wedge x_0 \neq 0 \wedge y_0 \neq 0.\end{aligned}$$

QEPCAD proves within 250,817 ms that $\vartheta^* \longrightarrow \varphi^*$, while our method fails in doing so due to the degree restrictions.

The following examples are taken from Chou [7]. These theorems, with the exception of Example 12 and our modification of Example 16, hold also over the complex numbers. We adopt the algebraic translations given by Chou.

EXAMPLE 10 (2.1, p. 6). We obtain the elimination result $\varphi^* \equiv$ true under the nondegeneracy conditions $\vartheta^* \equiv u_1 \neq 0 \wedge u_3 \neq 0$, which state that $ABCD$ is a proper parallelogram, after 102 ms.

EXAMPLE 11 (2.2, p. 7: Simson's theorem). We obtain $\varphi^* \equiv$ true and $\vartheta^* \equiv u_1^2 - 2u_1u_2 + u_2^2 + u_3^2 \neq 0 \wedge u_1 \neq 0 \wedge u_2 \neq 0 \wedge u_3 \neq 0$ after 374 ms. The condition $u_1 \neq 0 \wedge u_3 \neq 0$ states that ABC is a proper triangle. The first condition $(u_1 - u_2)^2 + u_3^2 \neq 0$ equivalent to $u1 - u2 \neq 0 \vee u3 \neq 0$ is implied by $u_3 \neq 0$ and can thus be dropped. The condition $u_3 \neq 0$ states that the triangle ABC is proper, and the condition $u_2 \neq 0$ states that $\angle BAC$ is not a right angle.

The following example fails over the complex numbers.

EXAMPLE 12 (3.9, p. 57). We obtain $\vartheta^* \equiv \varphi^* \equiv$ true after 17 ms.

EXAMPLE 13 (5.1, p. 58). After 136 ms we obtain the nondegeneracy condition $\vartheta^* \equiv u_1 \neq 0$ stating that $ABCD$ is a proper square and the elimination result $\varphi^* \equiv$ true. Besides Example 5, this is the only example discussed in this section from

which QEPCAD can eliminate the quantifiers: It computes $u_1 \neq 0$ as quantifier-free equivalent, which takes 1883 ms with 10^6 cells.

EXAMPLE 14 (5.2, p. 59: Feuerbach's theorem). We can eliminate 8 out of 9 quantifiers. Then the procedure fails due to the degree blowup, with x_1 being of degree 4.

EXAMPLE 15 (5.2, variant on p. 62: Feuerbach's theorem). For this choice of coordinates, Chou leaves out the conclusion. We use the conclusion

$$\begin{aligned}&(2x_8^2 + 2x_9^2 + x_7^2 - 2x_7x_8 - 2x_9u_2)^2\\ &\quad = 4(x_8^2 - 2x_7x_8 + x_7^2 + x_9^2)(x_8^2 + x_9^2 - 2x_9u_2 + u_2^2)\end{aligned}$$

expressing the fact that the distance between the center of the 9-point circle and the center of the incircle or an excircle equals the difference or the sum of the respective radii. We obtain as nondegeneracy conditions

$$\begin{aligned}\vartheta^* \equiv\ & u_1u_3 + u_2^2 \neq 0 \wedge u_1 + u_2 \neq 0\\ & \wedge u_1 - u_2 \neq 0 \wedge u_1 - u_3 \neq 0 \wedge u_1 \neq 0 \wedge u_2 \neq 0 \wedge u_3 \neq 0.\end{aligned}$$

The condition $u_1u_3+u_2^2 \neq 0$ states that $\angle ACB \neq 0$; the conditions $u_1+u_2 \neq 0$ and $u_1 - u_2 \neq 0$ say that $\angle BAC$ and $\angle CAB$ are not right angles, respectively. Finally $u_1 \neq 0 \wedge u_2 \neq 0 \wedge u_3 \neq 0$ states that ABC is a proper triangle. The elimination result is $\varphi^* \equiv$ true. This computation takes 2958 ms.

EXAMPLE 16 (5.3, pp. 62–63). Following the discussion on p. 63, we add the condition $\delta > 0$ to the hypothesis, where

$$\delta = \frac{-u_1^2u_3^2}{u_1^2u_2x_2 - u_1^2u_3x_1},$$

in the following way: The condition $\delta > 0$ can be expressed as $u_1 \neq 0 \wedge u_3 \neq 0 \wedge u_2x_2 - u_3x_1 < 0$. We actually drop the first two constituents of the conjunction because these are nondegeneracy conditions. Then we obtain $\vartheta^* \equiv u_3 \neq 0$ as a nondegeneracy condition and $\varphi^* \equiv$ true as an elimination result. This computation takes 85 ms.

EXAMPLE 17 (5.7, p. 71: originally by M. Paterson). After 1275 ms, we get $\varphi^* \equiv$ true and the following nondegeneracy conditions:

$$\begin{aligned}\vartheta^* \equiv\ & u_1^2 - 2u_1u_2 + u_2^2 + u_3^2 \neq 0 \wedge u_1u_3 - 2u_1u_4 + 2u_2u_4 \neq 0\\ & \wedge u_1u_3 + 2u_2u_4 \neq 0 \wedge u_1u_3 - 2u_2u_4 \neq 0 \wedge u_1 \neq 0 \wedge u_2 \neq 0.\end{aligned}$$

The first condition $(u_1 - u_2)^2 + u_3^2 \neq 0$ is equivalent to $u_1 \neq u_2 \wedge u_3 \neq 0$. This together with $u_1 \neq 0 \wedge u_2 \neq 0$ states that ABC be a proper triangle. The remaining disequations are noncollinearity conditions.

The final two examples taken from Chou are once more concerned with not only proving but finding theorems.

EXAMPLE 18 (5.8, pp. 72–73: Gergonne's theorem). This is a generalization of Simson's theorem discussed as Example 11. After 340 ms of computation time, we get the elimination result

$$\begin{aligned}\varphi^* \equiv\ & au_1^2u_2^2 + au_1^2u_3^2 - 2au_1u_2^3 - 2au_1u_2u_3^2 + au_2^4 + 2au_2^2u_3^2 + au_3^4 + \\ & + u_1^2u_2u_3^2y - u_1^2u_3^3x - u_1u_2^2u_3^2y - u_1u_3^4y + u_1u_3^3x^2 + u_1u_3^3y^2 = 0.\end{aligned}$$

This is exactly the equation $R_0 = 0$ of Chou for the locus of point D. We furthermore obtain the nondegeneracy conditions

$$\vartheta^* \equiv u_1^2 - 2u_1u_2 + u_2^2 + u_3^2 \neq 0 \wedge u_2 \neq 0 \wedge u_3 \neq 0.$$

The condition $u_3 \neq 0$ states that ABC is a proper triangle. As in Example 11 the first condition can be dropped. The condition $u_2 \neq 0$ states that $\angle BAC$ is not a right angle.

EXAMPLE 19 (5.9, p. 73: M. Paterson's problem). We obtain as elimination result

$$\begin{aligned}\varphi^* \equiv\ & u_1^2u_2y + u_1^2u_3x - 2u_1^2xy + u_1u_2^2y - 2u_1u_2u_3x + 2u_1u_2xy - \\ & - u_1u_3^2y - u_1u_3x^2 + u_1u_3y^2 - 2u_2^2xy + 2u_2u_3x^2 - 2u_2u_3y^2 + \\ & + 2u_3^2xy = 0 \vee u_1 = 0 \vee (u_2 = 0 \wedge u_3 = 0)\end{aligned}$$

under the subsidiary conditions

$$\vartheta^* \equiv u_1u_2 - u_2x - u_3y \neq 0 \wedge u_2 - x \neq 0 \wedge y \neq 0.$$

We suspect that there is a typo in Chou's solution on p. 74, which should probably read as follows:

$$\begin{aligned}R_0 =\ & u_1^2(u_3^2 + u_2^2) \cdot \\ & \cdot\big(ay^2 + 2bxy + \underline{cx^2} + (u_1u_3^2 - u_1u_2^2 - u_1^2u_2)y + (2u_1u_2 - u_1^2)u_3x\big).\end{aligned}$$

If this is the case, then φ^* provides a factorization of R_0, where $-u_1^2 = 0$ and $u_3^2 + u_2^2 = 0$ are equivalently replaced by $u_1 = 0$ and $u_2 = 0 \wedge u_3 = 0$, respectively. This example takes 272 ms.

6. Conclusions

We have shown that a method for elimination of linear and quadratic variables from a Boolean combination of polynomial equations and inequalities can be adapted to geometrical theorem proving. The resulting method is a genuinely real – not

complex – proof method that can handle not only polynomial equations but also ordering inequalities. In particular, it can prove also those geometrical theorems whose complex analogues fail. After specification of independent parameters in the given problem, our method specifies those nondegeneracy conditions that are actually used in the algorithm. In addition to the obtained nondegeneracy conditions, the method will supply additional assumptions for a given geometrical conjecture that turn the conjecture into a theorem.

The implementation of the method in the REDLOG package of REDUCE has shown that the algorithm can handle – besides well-known benchmark examples – some truly real geometry examples that have not been accessible to automatic proof methods so far. The present limitation of the elimination method to quadratic variables can be pushed up to higher degrees.

References

1. Abdallah, C. T., Dorato, P., Liska, R., Steinberg, S., and Yang, W.: Applications of quantifier elimination theory to control system design, in *4th IEEE Mediterranean Symposium on Control and Automation*, IEEE, 1996.
2. Arnon, D. S.: A bibliography of quantifier elimination for real closed fields, *J. Symbolic Comput.* **5**(1–2) (1988), 267–274.
3. Basu, S., Pollack, R., and Roy, M.-R.: On the combinatorial and algebraic complexity of quantifier elimination, in S. Goldwasser (ed.), *Proceedings of the 35th Annual Symposium on Foundations of Computer Science, Los Alamitos, CA, USA, November 1994*, IEEE Computer Society Press, 1994, pp. 632–641.
4. Buchberger, B.: Ein Algorithmus zum Auffinden der Basiselemente des Restklassenringes nach einem nulldimensionalen Polynomideal, Doctoral dissertation, Mathematical Institute, University of Innsbruck, Innsbruck, Austria, 1965.
5. Buchberger, B.: Applications of Gröbner bases in non-linear computational geometry, in R. Janßen (ed.), *Trends in Computer Algebra, Proceedings*, Lecture Notes in Comput. Sci. 296, Springer, 1988, pp. 52–80.
6. Carrá-Ferro, G. and Gallo, G.: A procedure to prove geometrical statements, Technical report, Dip. Mathematica Univ. Catania, Italy, 1987.
7. Chou, S.-C.: *Mechanical Geometry Theorem Proving*, Mathematics and Its Applications, D. Reidel Publishing Company, Dordrecht, Boston, Lancaster, Tokyo, 1988.
8. Collins, G. E. and Hong, H.: Partial cylindrical algebraic decomposition for quantifier elimination, *J. Symbolic Comput.* **12**(3) (1991), 299–328.
9. Colmerauer, A.: Prolog III, *Communications of the ACM* **33**(7) (1990), 70–90.
10. Corless, R. M. and Jeffrey, D. J.: Well ... it isn't quite that simple, *ACM SIGSAM Bulletin* **26**(3) (1992), 2–6. Feature.
11. Dolzmann, A. and Sturm, T.: Redlog user manual, Technical Report MIP-9616, FMI, Universität Passau, D-94030 Passau, Germany, October 1996. Edition 1.0 for Version 1.0.
12. Dolzmann, A. and Sturm, T.: Guarded expressions in practice, in W. W. Küchlin (ed.), *Proceedings of the 1997 International Symposium on Symbolic and Algebraic Computation (ISSAC 97)*, ACM Press, New York, 1997, pp. 376–383.
13. Dolzmann, A. and Sturm, T.: Redlog: Computer algebra meets computer logic, *ACM SIGSAM Bulletin* **31**(2) (1997), 2–9.
14. Dolzmann, A. and Sturm, T.: Simplification of quantifier-free formulae over ordered fields, *J. Symbolic Comput.* **24**(2) (1997), 209–231.

15. Hong, H., Collins, G. E., Johnson, J. R., and Encarnacion, M. J.: QEPCAD interactive version 12. Kindly communicated to us by Hoon Hong, September 1993.
16. Hong, H., Liska, R., and Steinberg, S.: Testing stability by quantifier elimination, *J. Symbolic Comput.* **24**(2) (1997), 161–187. Special issue on applications of quantifier elimination.
17. Kapur, D.: Using Gröbner bases to reason about geometry problems, *J. Symbolic Comput.* **2**(4) (1986), 399–408.
18. Kutzler, B. A.: Algebraic Approaches to Automated Theorem Proving, PhD Thesis, Johannes Kepler Universität Linz, 1988. RISC-Linz series no. 88-74.0.
19. Kutzler, B. A. and Stifter, S.: On the application of Buchberger's algorithm to automated geometry theorem proving, *J. Symbolic Comput.* **2**(4) (1986), 389–397.
20. Loos, R. and Weispfenning, V.: Applying linear quantifier elimination, *Comput. J.* **36**(5) (1993), 450–462. Special issue on computational quantifier elimination.
21. MacLane, S.: Some interpretations of abstract linear dependence in terms of projective geometry, *Amer. J. Math.* **58** (1936), 236–240.
22. McPhee, N. F., Chou, S.-C., and Gao, X.-S.: Mechanically proving geometry theorems using a combination of Wu's method and Collins' method, in Alan Bundy (ed.), *Automated Deduction – CADE-12*, Lecture Notes in Artif. Intell. 814, Springer, Berlin, Heidelberg, New York, 1994, pp. 401–415.
23. Preparata, F. P. and Shamos, M. I.: *Computational Geometry – An Introduction*, Texts and Monographs in Computer Science, Springer, New York, 1985.
24. Renegar, J.: On the computational complexity and geometry of the first-order theory of the reals, Part I–III, *J. Symbolic Comput.* **13**(3) (1992), 255–352.
25. Seidenberg, A.: An elimination theory for differential algebra, *Univ. California Publ. Math. (N.S.)* **3** (1956), 31–66.
26. Seidenberg, A.: Some remarks on Hilbert's Nullstellensatz, *Arch. Math.* **7** (1956), 235–240.
27. Wang, D.-M.: An elimination method for polynomial systems, *J. Symbolic Comput.* **16**(2) (1993), 83–114.
28. Wang, D.-M.: Reasoning about geometric problems using an elimination method, in J. Pfalzgraf (ed.), *Automatic Practical Reasoning*, Springer-Verlag, Wien, 1995, pp. 147–185.
29. Wang, D.-M. and Gao, X.-S.: Geometry theorems proved mechanically using Wu's method – part on Euclidean geometry, Mathematics-Mechanization Research Preprints 2, Institute of Systems Science, Academia Sinica, Beijing, China, November 1987.
30. Weispfenning, V.: The complexity of linear problems in fields, *J. Symbolic Comput.* **5**(1) (1988), 3–27.
31. Weispfenning, V.: Parametric linear and quadratic optimization by elimination, Technical Report MIP-9404, FMI, Universität Passau, D-94030 Passau, Germany, April 1994. To appear in the *J. Symbolic Comput.*
32. Weispfenning, V.: Quantifier elimination for real algebra – the cubic case, in *Proceedings of the International Symposium on Symbolic and Algebraic Computation in Oxford*, ACM Press, New York, 1994, pp. 258–263.
33. Weispfenning, V.: Quantifier elimination for real algebra – the quadratic case and beyond, *Appl. Algebra Eng. Comm. Comput.* **8**(2) (1997), 85–101.
34. Weispfenning, V.: Simulation and optimization by quantifier elimination, *J. Symbolic Comput.* **24**(2) (1997), 189–208. Special issue on applications of quantifier elimination.
35. Winkler, F.: A geometrical decision algorithm based on the Gröbner bases algorithm, in P. Gianni (ed.), *Symbolic and Algebraic Computation, Proceedings of ISSAC '88*, Lecture Notes in Comput. Sci. 358, Springer, Berlin, Heidelberg, 1988, pp. 356–363.
36. Wu, W.-T.: On the decision problem and the mechanization of theorem-proving in elementary geometry, *Scientia Sinica* **21** (1978), 159–172, also *Contemporary Mathematics* **29** (1984), 213–234.

37. Wu, W.-T.: Basic principles of mechanical theorem proving in elementary geometries, *J. Systems Sci. Math. Sci.* **4** (1984), 207–235.
38. Wu, W.-T.: Some recent advances in mechanical theorem-proving of geometries, *Contemporary Mathematics* **29** (1984), 235–241.
39. Wu, W.-T.: Basic principles of mechanical theorem proving in elementary geometry, *J. Automated Reasoning* **2** (1986), 219–252.
40. Wu, W.-T.: On problems involving inequalities, Mathematics-Mechanization Research Preprints 7, Institute of Systems Science, Academia Sinica, Beijing, China, March 1992.