A New Approach for Automatic Theorem Proving in Real Geometry

Andreas Dolzmann, Thomas Sturm * and Volker Weispfenning
Fakultät für Mathematik und Informatik, Universität Passau, D-94030 Passau.
e-mail: Andreas.Dolzmann@fmi.uni-passau.de, sturm@fmi.uni-passau.de, weispfen@alice.fmi.uni-passau.de

MIP-9611, May 20, 1996

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. After specification of independent variables, non-degeneracy conditions are generated automatically. Moreover, when trying to prove conjectures that do—apart from non-degeneracy conditions—not hold in the claimed generality, missing premises are found automatically. We demonstrate the applicability of our method to non-trivial examples. In particular, we can treat a variety of examples for which quantifier elimination by partial CAD fails.

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

* The second author was supported by the DFG (Schwerpunktprogramm: Algorithmische Zahlentheorie und Algebra).

1. Introduction

Theorems of elementary geometry have always 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, cf. [3, 26, 28], Gröbner Basis techniques, cf. [11, 10, 9], and complex elimination methods, cf. [17, 18], based on ideas by Seidenberg, cf. [16, 15].

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.

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, cf. our Example 8 in Section 4 taken from [3]. For a few examples of non-trivial exceptions cf. [10] and our Example 5 in Section 4 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, cf. [4], that is implemented in the QEPCAD package, cf. [8]. With the exception of Example 3 and Example 9, QEPCAD cannot cope with any of the examples discussed in this paper.

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

- They have to found and added to a preliminary "naive" translation of $\mathfrak{G}$ by the user then yielding the actual translation φ, cf. method 1 in [9].
- They are found automatically, provided the user has previously specified certain variables as *independent*, cf. method 2 in [9], [11, 10]. Such a specification of independent variables over $\mathbb{C}$ is not always completely obvious from the geometrical statement $\mathfrak{G}$, cf. [10, 13].
- They are found by the automatic prover without any human support, cf. [2, 17, 18].

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, e.g. Gröbner Bases or extended characteristic sets. In a next step, one attempts to *reduce* f_0 wrt. all systems G_j. If all these reductions of f_0 to zero succeed, then φ holds in $\mathbb{C}$, and hence in $\mathbb{R}$, under some subsidiary conditions. In method 2 of [9], 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 $\mathbb{C}$.

2. The input there may also contain polynomial order-inequalities.

3. If the proof of the input conjecture φ fails in spite of all appropriate non-degeneracy 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 do not only prove theorems but even *find* theorems.

4. In contrast to the CAD method by Collins and Hong [4], 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 avoids the computation of a normal form for the polynomial equations in the hypothesis. Instead it uses iterated elimination of variables from the entire system in order to derive the desired conclusion. We call this *lazy proving* since it avoids expensive computations that depend only on the hypothesis but non on the conclusion, which suggests that they are too general.

6. After specification of *parameters* in contrast to dependent variables, the method automatically constructs non-degeneracy conditions necessary for the given conjecture to hold. In contrast to the complex situation, over the reals it is, in general, easy to decide what the parameters are.

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, cf. [20, 12, 23].

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 explain our method once more by example and then give some examples of automatic proofs. Section 5 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. 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.

Suppose now that ψ is quadratic, i.e. of degree 2, in some variable x, and denote $\exists x(\psi(x, u_1, \dots, u_n))$ by $\varphi(u_1, \dots, u_n)$. Then the algorithm given in [23] computes from φ a quantifier-free formula $\varphi^*(u_1, \dots, u_n)$ not containing x such that over the field of the reals we have the equivalence

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

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

Notice that 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 [23], we may thus restrict 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

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

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 unbound or closed. In the latter case, such an interval will contain its real endpoint. Thus M_φ is non-empty 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, cf. [23]. 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 to contain also 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, cf. [23]. Again this yields a quantifier-free formula φ^* equivalent to $\exists x\psi$ over the reals. For practical applications this method, of course, 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, cf. [6] 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 $ax^2 + bx + c$ does not only deliver 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 non-vanishing of a and b. Formally, we obtain

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

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 non-zero, 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, cf. [12, 23]. One simple instance for such an improvement is some natural extension of *Gauss elimination*: Suppose ψ is of the form

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

where at least one of the coefficient terms b, c is a rational non-zero constant. Then we know that under any interpretation of the u_i the equation is *non-trivial*, i.e. 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 of coefficients whether they are non-zero 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 to 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. In order 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' which 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.

The method in this general form has been applied successfully to examples in industrial simulation and optimization, cf. [22].

An extension of the method to higher degrees has been sketched also in [23]. The cubic case has been worked out in detail in [21].

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, cf. [3, 10, 28]. In an algebraic translation, theorems of this kind yield *universal Horn formulas*, i.e., formulas of the type

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

This allows 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 previous section is not restricted to formulas of such a special form. Our algebraic translations φ may be arbitrary first-order formulas

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

where ψ is a Boolean combination of polynomial equations, disequations, and order inequalities subject to degree restrictions wrt. x_1, …, x_n.

As already indicated in the introduction, we do not expect ψ to be true in the literal sense, i.e., for all real values of the variables u_1, …, u_m. Instead, we implicitly assume that the given configuration is *non-degenerate*: A given triangle should not degenerate to a line segment, a given circle should not degenerate to a point, etc. On the algebraic side, these non-degeneracy conditions are reflected in the assertion that certain of the variables representing e.g. 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, …, 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 wish to assert only that u_1, …, u_m satisfy such polynomial inequalities $g(u_1, \ldots, u_m) \neq 0$, that encode non-degeneracy conditions for the geometrical input problem $\mathfrak{G}$.

In our method, we will automatically generate assumptions stating that certain coefficients in the parameters are non-zero. We have seen in the previous 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 non-degeneracy conditions.

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 non-degenerate. Instead, we specify certain of the variables in φ as independent parameters $u_1, \ldots, u_m$. 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 previous section is applied to $\varphi(u_1, \ldots, u_m)$ and $\vartheta(u_1, \ldots, u_m)$ with the following modifications: In substitutions, all non-trivial 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 previous section that the substitutions contain also 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.

Whenever a formula $bx + c = 0 \wedge \psi_1$ occurs but none of the coefficients b, c is a non-zero 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.

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

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

In spite of the necessary assumption $u \neq 0$ we then 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 non-zero. 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.

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, i.e. $\vartheta^* \longrightarrow \vartheta$, such that

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

holds over the reals.

If φ^* equals "true," then we have proved φ and thus the geometrical assertion $\mathfrak{G}$ under the non-degeneracy 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 using some—unmodified—quantifier elimination procedure such as that of Section 2, if the degrees allow 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 non-degeneracy conditions, i.e., 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 non-degeneracy conditions missing, we can apply a *theory generator*. This is a procedure that enlarges ϑ^* by further disequations until it, hopefully, 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. Examples

Both the original elimination procedure sketched in Section 2 and its modification described in Section 3 have been implemented within the REDUCE computer logic package REDLOG, cf. [5, 7]. 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 due to 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.

We start with discussing the automatic proof of some examples of real geometry taken from Wu [29], Wang [18], and Kutzler [10]. Then we summarize the timings and solutions of several examples taken from Chou [3]. Most of the latter can also be proved by complex methods. All computations have been performed on a SUN SPARC-4 workstation with 10^6 Lisp cells. Such a cell takes four bytes of memory.

EXAMPLE 1 (Angle at circumference vs. angle at center). Let M be the midpoint of the circumcircle of a triangle ABC. Then $\angle ACB = \angle AMB/2$ (see Figure 1).

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

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

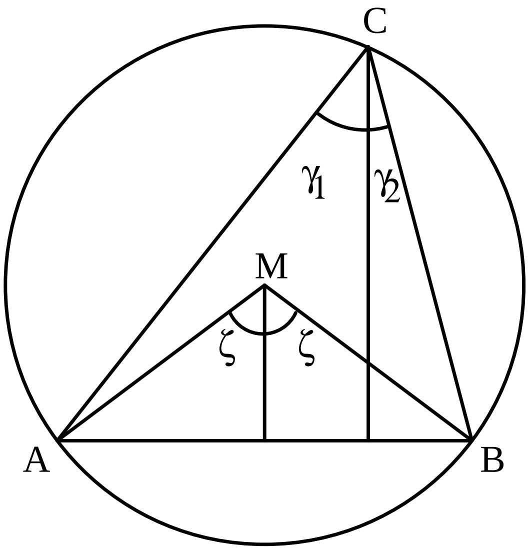

Figure 1. The angle at circumference is half the angle at center (Example 1).

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

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

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:

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

After 85 ms of computation time, we obatin $\varphi^* \equiv$ true and the non-degeneracy condition $\vartheta^* \equiv y_0 \neq 0$ stating that AMB is a non-degenerate triangle.

EXAMPLE 2 (Median Bisector Theorem). For a non-isosceles triangle ABC the median over the side AB is always greater than the interior bisector on the same side (see Figure 2).

This example and the ideas for its algebraic translation are taken from Wu [29], pp. 7–8. To prove the theorem, we take coordinates such

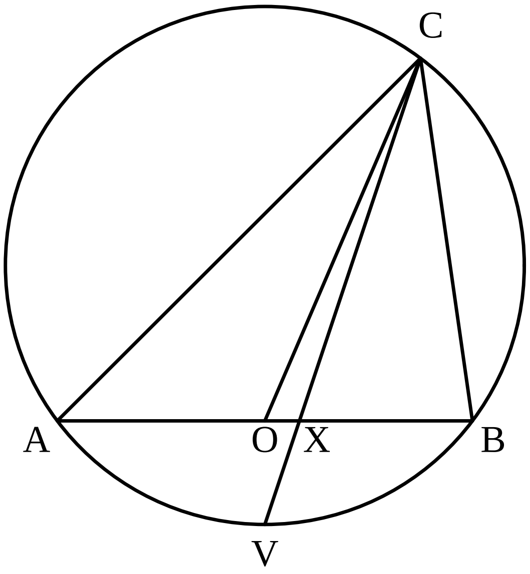

Figure 2. The median bisector theorem (Example 2).

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 mid point of AB, we have that CO is the median on AB. We construct the bisector using the geometric theorem proved as Example 1: The center of the circumcicle 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 circumcicle. 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 2380 ms elimination time, we obtain the non-degeneracy conditions $\vartheta^* \equiv x_0 \neq 0 \ \wedge \ y_0 \neq 0$, stating that ABC is a non-degenerate non-isosceles triangle, plus a quantifier-free equivalent φ^* containing 21 atomic formulas. QEPCAD subsequently proves in 1633 ms that already $\vartheta^* \longrightarrow \varphi^*$, which proves the theorem.

The next example is taken from Wang [18], pp. 158–160.

EXAMPLE 3 (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:

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

After 85 ms we obtain $\varphi^* \equiv$ true without any subsidiary condition. QEPCAD yields the same result in 517 ms.

In the following example also taken from Wang [18], pp. 161–162, we do not only prove but actually *find* a theorem.

EXAMPLE 4 (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:

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

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 153 ms we obtain $\vartheta^* \equiv a > 0 \ \wedge \ b \geqslant 0 \ \wedge \ c \geqslant 0 \ \wedge \ f \geqslant 0$, i.e., the condition $a \neq 0$ stating that ABC does not degenerate to a point is added. The quantifier-free formula φ^* obtained contains 5 atomic formulas. Automatic simplification of φ^* wrt. ϑ^* by Gröbner basis methods, cf. [6], takes 340 ms yielding:

$$9a^4 - 10a^2b^2 + b^4 + 16F^2 = 0 \ \wedge \ a^2b^2 - F^2 \geqslant 0.$$

The inequality follows from the equation as our pure quantifier eliminiation method shows in 34 ms. Alternatively, QEPCAD proves this in

566 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 5. Consider eight points A, ..., 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 [13]. It holds in the real plane but fails in the complex one. We adopt the translation proposed by Kutzler [10], p. 154, setting $A = (0, 0)$, $B = (x_b, 0)$, $C = (x_c, y_c)$, $D = (x_d, 0)$, $E = (x_e, y_e)$, ..., $H = (x_h, y_h)$:

$$\begin{aligned}
&\forall y_h \forall x_e \forall y_e \forall x_f \forall y_f \forall x_g \forall y_g (\\
&\quad x_h y_c - x_c y_h = 0 \ \wedge\ x_g y_f - x_f y_g = 0 \ \wedge \\
&\quad x_b y_e - x_c y_e + x_e y_c - x_b y_c = 0 \ \wedge\ x_b y_h - x_g y_h + x_h y_g - x_b y_g = 0 \ \wedge \\
&\quad x_c y_f - x_d y_f - x_f y_c + x_d y_c = 0 \ \wedge\ x_d y_g - x_e y_g + x_g y_e - x_d y_e = 0 \ \wedge \\
&\quad x_e y_h - x_f y_h + x_h y_f - x_e y_f - x_h y_e + x_f y_e = 0 \longrightarrow x_b y_c = 0)
\end{aligned}$$

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

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

We get after 6256 ms a quantifier-free formula φ^* with 125 atomic formulas. The subsidiary conditions ϑ^* obatined are

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

Within 56134 ms, our theory generator adds the following assumptions to ϑ^*, which make it sufficient for φ^* and thus for φ:

$$x_b - x_d \neq 0 \ \wedge\ x_c - x_h \neq 0 \ \wedge\ x_d \neq 0 \ \wedge\ x_h \neq 0.$$

The following examples are taken from Chou [3]. These theorems, with the exception of Example 8 and our modification of Example 11, hold also over the complex numbers. We adopt the algebraic translations given by Chou.

EXAMPLE 6 (2.1, p. 6). We obtain the elimination result $\varphi^* \equiv \text{true}$ under the non-degeneracy conditions $\vartheta^* \equiv u_1 \neq 0 \ \wedge \ u_3 \neq 0$, which state that $ABCD$ is a proper parallelogram, after 136 ms.

EXAMPLE 7 (2.2, p. 7: Simson's theorem). We obtain $\varphi^* \equiv \text{true}$ 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 8 (3.9 p. 57). We obtain $\vartheta^* = \varphi^* = \text{true}$ after 17 ms.

EXAMPLE 9 (5.1, p. 58). After 102 ms we obtain the non-degeneracy condition $\vartheta^* \equiv u_1 \neq 0$ stating that $ABCD$ is a proper square and the elimination result $\varphi^* \equiv \text{true}$. Besides Example 3, this is the only example discussed throughout this section, from which QEPCAD can eliminate the quantfiers: It computes $u_1 \neq 0$ as quantifier-free equivalent, which takes 1917 ms with 10^6 cells.

EXAMPLE 10 (5.2, variant on p. 62: Feuerbach's theorem).
Chou leaves out the conclusion for this choice of coordinates. We use the conclusion

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

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 non-degeneracy 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 6715 ms.

EXAMPLE 11 (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 since these are non-degeneracy conditions. Then we obtain $\vartheta^* \equiv u_3 \neq 0$ as non-degeneracy condition, and $\varphi^* \equiv$ true as elimination result. This computation takes 85 ms.

EXAMPLE 12 (5.7, p. 71: originally by M. Paterson).
After 1343 ms, we get $\varphi^* \equiv$ true and the following subsidiary conditions:

$$\begin{aligned}
\vartheta^* \equiv\ & 3u_1^2u_3 - 4u_1^2u_4 + 4u_1u_2u_4 - 4u_2^2u_4 - 4u_3^2u_4 + 4u_3u_4^2 \neq 0 \ \wedge \\
& u_1^2 - 2u_1u_2 + u_2^2 + u_3^2 \neq 0 \ \wedge \ u_1u_3 - 2u_2u_4 \neq 0 \ \wedge \\
& u_1 - u_2 \neq 0 \ \wedge \ u_1 \neq 0 \ \wedge \ u_2 \neq 0 \ \wedge \ u_4 \neq 0.
\end{aligned}$$

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

EXAMPLE 13 (5.8, pp. 72–73: Gergonne's theorem). This is a generalization of Simson's theorem discussed as Example 7. 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 non-degenerary 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 7 the first condition can be dropped. The condition $u_2 \neq 0$ states that $\angle BAC$ is not a right angle.

EXAMPLE 14 (5.9, p. 73: M. Paterson's problem).
As elimination result, we obtain

$$\varphi^* \equiv u_1^2 u_2 y + u_1^2 u_3 x - 2u_1^2 xy + u_1 u_2^2 y - 2u_1 u_2 u_3 x + 2u_1 u_2 xy - u_1 u_3^2 y - u_1 u_3 x^2 + u_1 u_3 y^2 - 2u_2^2 xy + 2u_2 u_3 x^2 - 2u_2 u_3 y^2 + 2u_3^2 xy = 0 \vee u_2^2 + u_3^2 = 0,$$

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

$$R_0 = u_1^2(u_3^2 + u_2^2) \cdot (ay^2 + 2bxy + \underline{cx^2} + (u_1 u_3^2 - u_1 u_2^2 - u_1^2 u_2)y + (2u_1 u_2 - u_1^2)u_3 x).$$

If this is the case, then φ^* provides a factorization of R_0 with a factor $-u_1^2$ missing. Our subsidiary conditions

$$\vartheta \equiv u_1 u_2 - u_2 x - u_3 y \neq 0 \ \wedge \ u_1 \neq 0 \ \wedge \ u_2 - x \neq 0 \ \wedge \ y \neq 0,$$

however, contain $u_1 \neq 0$, which allows to cancel it in the elimination result. This example takes 306 ms.

5. 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 non-degeneracy conditions that are actually used in the algorithm. In addition to the obtained non-degeneracy 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. Bruno Buchberger. Applications of Gröbner bases in non-linear computational geometry. In Rainer Janßen, editor, *Trends in computer algebra, Proceedings*, volume 296 of *Lecture Notes in Computer Science*, pages 52–80, Berlin u.a., 1988. Springer.
2. Giuseppa Carrà-Ferro and Giovanni Gallo. A procedure to prove geometrical statements. Technical report, Dip. Mathematica Univ. Catania, Italy, 1987.
3. Shang-Ching Chou. *Mechanical Geometry Theorem Proving.* Mathematics and its applications. D. Reidel Publishing Company, Dordrecht, Boston, Lancaster, Tokyo, 1988.
4. George E. Collins and Hoon Hong. Partial Cylindrical Algebraic Decomposition for Quantifier Elimination. *Journal of Symbolic Computation*, 12(3):299–328, September 1991.
5. Andreas Dolzmann and Thomas Sturm. *Redlog, a Reduce Logic Package.* FMI, Universität Passau, D-94030 Passau, Germany, preliminary edition, July 1995. User Manual.
6. Andreas Dolzmann and Thomas Sturm. Simplification of quantifier-free formulas over ordered fields. Technical Report MIP-9517, FMI, Universität Passau, D-94030 Passau, Germany, October 1995. To appear in the Journal of Symbolic Computation.
7. Andreas Dolzmann and Thomas Sturm. Redlog—computer algebra meets computer logic. Technical Report MIP-9603, FMI, Universität Passau, D-94030 Passau, Germany, February 1996.
8. Hoon Hong, George E. Collins, Jeremy R. Johnson, and Mark J. Encarnacion. QEPCAD interactive version 12. Kindly communicated to us by Hoon Hong, September 1993.
9. Deepak Kapur. Using Gröbner Bases to Reason About Geometry Problems. *Journal of Symbolic Computation*, 2(4):399–408, December 1986.
10. Bernhard A. Kutzler. *Algebraic Approaches to Automated Theorem Proving.* PhD thesis, Johannes Kepler Universität Linz, 1988. RISC-Linz series no. 88-74.0.

11. Bernhard A. Kutzler and Sabine Stifter. On the Application of Buchberger's Algorithm to Automated Geometry Theorem Proving. *Journal of Symbolic Computation*, 2(4):389–397, December 1986.
12. Rüdiger Loos and Volker Weispfenning. Applying linear quantifier elimination. *The Computer Journal*, 36(5):450–462, 1993. Special issue on computational quantifier elimination.
13. Saunders MacLane. Some interpretations of abstract linear dependence in terms of projective geometry. *American Journal of Mathematics*, 58:236–240, 1936.
14. Franco P. Preparata and Michael I. Shamos. *Computational Geometry—An Introduction*. Texts and monographs in computer science. Springer, New York, 1985.
15. Abraham Seidenberg. An elimination theory for differential algebra. *Univ. California Publ. Math (N.S.)*, 3:31–66, 1956.
16. Abraham Seidenberg. Some remarks on Hilbert's Nullstellensatz. *Arch. Math.*, 7:235–240, 1956.
17. Dong-Ming Wang. An elimination method for polynomial systems. *Journal of Symbolic Computation*, 16(2):83–114, August 1993.
18. Dong-Ming Wang. Reasoning about geometric problems using an elimination method. In J. Pfalzgraf, editor, *Automatic Practical Reasoning*, pages 147–185, Wien, 1995. Springer-Verlag.
19. Dong-Ming Wang and Xiao-Shan Gao. Geometry theorems proved mechanically using Wu's method—part on euclidean geometry. Mathematics-Mechanization Research Preprints 2, Institute of Systems Science, Academia Sinicia, Beijing, China, November 1987.
20. Volker Weispfenning. The complexity of linear problems in fields. *Journal of Symbolic Computation*, 5(1):3–27, February 1988.
21. Volker Weispfenning. Quantifier elimination for real algebra—the cubic case. In *Proceedings of the International Symposium on Symbolic and Algebraic Computation in Oxford*, pages 258–263, New York, July 1994. ACM Press.
22. Volker Weispfenning. Applying quantifier elimination to problems in simulation and optimization. Technical Report MIP-9607, FMI, Universität Passau, D-94030 Passau, Germany, April 1996.
23. Volker Weispfenning. Quantifier elimination for real algebra—the quadratic case and beyond. To appear in AAECC, 1996.
24. Franz Winkler. A Geometrical Decision Algorithm Based on the Gröbner Bases Algorithm. In P. Gianni, editor, *Symbolic and Algebraic Computation, Proceedings of ISSAC'88*, volume 358 of *Lecture Notes in Computer Science*, pages 356–363, Berlin, Heidelberg, 1988. Springer.
25. Wen-Tsun Wu. On the decision problem and the mechanization of theorem-proving in elementary geometry. *Scientia Sinica*, 21:159–172, 1978. also: Contemporary Mathematica, vol. 29 (1984), pp. 213-234.
26. Wen-Tsun Wu. Basic principles of mechanical theorem proving in elementary geometries. *Journal of Systems Sciences and Mathematical Sciences*, 4:207–235, 1984.
27. Wen-Tsun Wu. Some recent advances in mechanical theorem-proving of geometries. *Contemporary Mathematics*, 29:235–241, 1984.

28. Wen-Tsun Wu. Basic principles of mechanical theorem proving in elementary geometry. *Journal of Automated Reasoning*, 2:219–252, 1986.
29. Wen-Tsun Wu. On problems involving inequalities. Mathematics-Mechanization Research Preprints 7, Institute of Systems Science, Academia Sinicia, Beijing, China, March 1992.