ALGEBRAIC PROOFS FOR GEOMETRIC STATEMENTS

by
Mihai Cipu

1 Principles of algebraic methods in geometric reasoning

It is well-known that in the first half of the 17th century Ren´e Descartes proposed a program of problem solving based on the assumption that solving a problem in mathematics means essentially solving a problem in algebra, more precisely, solving a system of algebraic equations. It is less known that precisely the same method was in current use in China long before Descartes, as witnessed by the book Jade Mirror of Four Elements by Shi-jie Zhu, dated 1303 (cf. [3]). However, as a consequence of Godel's work, in the first part of the 20th century it became clear that not all geometric statements can be derived in this way from a small set of axioms.

The advent of fast computers has revived the interest in algebraization of geometric reasoning. The most successful methods currently available are based on either Grobner-bases theory or on Ritt-Wu characteristic sets method. Other approaches are described in various chapters of [5]. An impressive bibliography can be found on Dongming Wang's web site [10].

The automatic methods for proving theorems can be classified according to several criteria. Thus one has to distinguish those who use coordinates from the coordinate-free approaches. The method of the former kind have a common structure:

a) An appropriate coordinate system is chosen.

b) The hypotheses and the thesis are translated into polynomial relations among the geometric data (e.g., coordinates of points, lengths of segments, areas of figures, etc.).

c) It is shown that the thesis polynomial is a consequence of the hypothesis polynomials.

The specific implementation of these steps makes the difference between methods of this type. In a classical approach, a thesis (expressed by the vanishing of a polynomial) t is a consequence of hypotheses (expressed by the vanishing of polynomials) $h_1, h_2, ..., h_s$, hs if t belongs to the radical of the ideal generated by $h_1, h_2, ..., h_s$.

This approach is successful in many instances. However, it is not as simple as it looks. Apart from not being able to deal with all geometric statements (Godel's theorem), there are several other reasons for failure, nicely discussed in [1]. For instance, the theorem cubes of equal volume have equal sides has apparently the hypothesis ideal generated by $H := x^3 - y^3$ and the thesis polynomial $C := x - y$. Since $x - y$ does not belong to $Rad\left(x^3 - y^3\right)$ except in fields of characteristic 3, we cannot prove automatically this simple theorem! Indeed, we cannot check that the thesis polynomial vanishes on the common zeroes of the hypothesis polynomial. Over the field of complex numbers this statement is patently false, since there are three complex cubic roots for any non-zero number. This phenomenon does not occur in the real field, and one may hope that the statement can be automatically checked in this case. As $x^3 - y^3 = (x - y)\left(x^2 + xy + y^2\right)$, the only component of interest in the geometric context is $x - y$, since $x^2 + xy + y^2$ can never vanish for real numbers.

Such examples suggest to amend the classical approach in the form [1]: Let $Q_1, Q_2, ..., Q_r$ be the minimal primes of $\mathrm{Rad}(\mathrm{Ideal}(h_1, ..., h_s))$, so that $Q_1 \cap Q_2 \cap ... \cap Q_s$ is a reduced primary decomposition of the radical of $\mathrm{Ideal}(h_1, ..., h_s)$.

We say that the theorem is algebraically true on the component Q_i if *t* belongs to Q_i.

The most powerful computer algebra systems can compute primary decompositions by means of Grobner-bases computations, so the goal of automatically proving (some) geometric theorems is presently within our reach.

The work ofWen-ts¨unWu [12] allows one another specialization of the generic steps a)–c):

Step 1 (algebraization) Choose an appropriate coordinate system. Proving the theorem is converted to deciding whether one can derive the conclusion equation from the hypothesis equations.

Step2 (triangulation) Transform the set of hypothesis polynomials into a characteristic set CS by Wu's well-ordering principle.

Step3 (successive pseudo-division) Obtain $R = prem(C, CS)$. If $R = 0$ then the theorem is valid under the subsidiary conditions $I_k \neq 0$.

Using Wu-Ritt zero decomposition theorem, one has

$$Zero(HS / D) = \cup_k Zero(CS_k / DJ_k)$$

with J_k the initial product of the characteristic set CS_k. A conclusion $C = 0$ is true on the component $Zero(CS_k / DJ_k)$ if $prem(C, CS_k) = 0$. The converse is true if

CS_k is irreducible. Here *D* denotes a polynomial whose vanishing represents some degenerate cases of the geometric configuration, and $Zero(HS/D)$ denotes the set of all roots of the polynomial set *HS* for which *D* is non-zero.

A major drawback is the fact that the non-degeneracy conditions depend on the choice of coordinates. The task of interpreting the geometric meaning of the subsidiary conditions obtained algebraically is hard and not susceptible of automatization. Even the choice of coordinates is not as easy as it may seem. Obviously it is desirable to select a coordinate system such that subsequent calculations become simpler. To this end, one may choose a coordinate system such that many points have coordinates as simple as possible. An appropriate selection of the ordering of variables and hypothesis polynomials can also shorten the computation.

Let us consider the following example (cf. [2]):

Example 1. Draw squares *ABDE* and *CAFG* on the sides *AB* and *AC* of a triangle *ABC*. Prove that *EC* is perpendicular to *BF*.

Suppose we choose a coordinate system such that the points are located at $B(0,0), C(x_1,0), A(x_2,x_3), E(x_4,x_5), F(x_6,x_7)$. Remark that the points *D* and *G* do not appear in the thesis and also the hypothesis can be expressed without invoking these points. The assumptions are translated into the polynomials

$$\begin{aligned}
H_1 &:= x_5^2 - 2x_3x_5 + x_4^2 - 2x_2x_4, && (AB = AE)\\
H_2 &:= x_3x_5 + x_2x_4 - x_3^2 - x_2^2, && (AB \perp AE)\\
H_3 &:= x_7^2 - 2x_3x_7 + x_6^2 - 2x_2x_6 + 2x_2x_1 - x_1^2, && (AC = AF)\\
H_4 &:= x_3x_7 + (x_2 - x_1)x_6 - x_3^2 - x_2^2 + x_1x_2, && (AC \perp AF)
\end{aligned}$$

and the thesis is written

$$C := x_5x_7 + (x_4 - x_1)x_6. \qquad (EC \perp BF)$$

It is natural to assume that the triangle is non-degenerated, that is

$$\begin{aligned}
&D_1 := x_2^2 + x_3^2 \neq 0, && (A \neq B)\\
&D_2 := (x_2 - x_1)^2 + x_3^2 \neq 0, && (A \neq C)\\
&D_3 := x_1 \neq 0. && (B \neq C)
\end{aligned}$$

One obtains

$$Zero(HS/DS) = Zero(AS_1/J_1) \cup \ldots \cup Zero(AS_4/J_4),$$

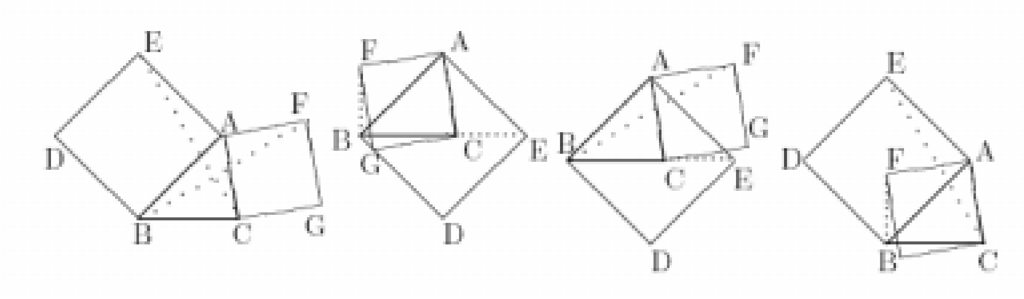

Figure 1: Example 1

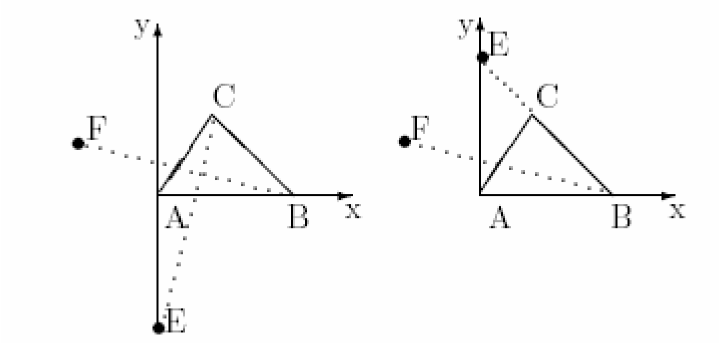

Figure 2: Another view of Example 1

With

$$\begin{aligned}
AS_1 &= \{ P_1, P_2, P_3, P_4 \}, \;\; AS_2 = \{ P_5, P_6, P_7, P_8 \},\\
AS_3 &= \{ P_1, P_2, P_7, P_8 \}, \;\; AS_4 = \{ P_5, P_6, P_3, P_4 \},
\end{aligned}$$

where

$$\begin{aligned} P_1 &:= x_4 + x_3 - x_2, & P_2 &:= x_3(x_5 - x_3 - x_2), \\ P_3 &:= x_6 - x_3 - x_2, & P_4 &:= x_3(x_7 - x_3 + x_2 - x_1), \\ P_5 &:= x_4 - x_3 - x_2, & P_6 &:= x_3(x_5 - x_3) + x_2(x_4 - x_2), \\ P_7 &:= x_6 + x_3 - x_2, & P_8 &:= x_3(x_7 - x_3 - x_2 + x_1). \end{aligned}$$

Computations show that $prem(C, AS_1) = 0$, $prem(C, AS_2) = 0$ while $prem(C, AS_3) \neq 0 \neq prem(C, AS_4)$. This means that in non-degenerate triangles, the theorem is true if the two squares are both erected outwardly or inwardly, and is generically false if one square is drawn outwardly and the other inwardly, cf. Fig. 1.

An experienced solver would take a system of coordinates with origin in the vertex A which appears “more frequently” than B and C in the hypothesis. If, say, $A(0,0), B(x_1,0), C(x_2, x_3)$, and $F(x_4, x_5)$, then *E* is sitting on the *Oy* axis (because $AB \perp AE$) and his ordinate is $\pm x_1$ (since *AE* = *AB*). At this moment it is apparent that one has to distinguish the configuration with the square *ABDE* exterior to triangle *ABC* from the configuration with *ABDE* cutting the interior of the triangle. We therefore have *two* thesis polynomials. In general, this situation is due to the need to take into account the orientation of real geometric configurations. It is very difficult to treat automatically this subtle issue. The danger of overlooking some configurations is minimized by working with coordinates as symmetrical as possible.

The two configurations are described algebraically by the same hypothesis Polynomials

$$H_1 := x_5^2 + x_4^2 - x^3 - x^2, \qquad (AC = AF)$$

$$H_2 := x_3 x_5 + x_2 x_4, \qquad (AC \perp AF)$$

while the thesis polynomial is

$$C_1 := (x_3 + x_1)x_5 + (x_4 - x_1)x_2 \qquad (ABDE \;\; \text{outwardly})$$

for the situation depicted on the left side, and

$$C_2 := (x_3 - x_1)x_5 + (x_4 - x_1)x_2 \qquad (ABDE \;\; \text{inwardly})$$

for the other situation.

The computations proceed as above and lead to the conclusion already stated.

2 Deduction of new theorems

Basic techniques to algebraically check whether the conclusion of a geometric theorem follows from a given set of hypotheses have been presented in the previous section. A modification of the principle allows one to discover geometric theorems. The key idea is to find new additional hypotheses such that the thesis becomes a consequence of the extended set of hypotheses. In the approach based on the Ritt-Wu method, if the pseudo-remainder of the thesis polynomial with respect to a characteristic set is non-zero, it is factored and each of its factors is candidate to become additional hypothesis. In the method based on Grobner-bases computations, the complementary hypotheses are selected from the factors of the normal form of the thesis polynomial with respect to a Grobner basis of the original hypothesis ideal.

To discover a new relation relating parameters involved in the description of a geometric configuration or to prove the equivalence of two conditions, one may proceed along the following lines.

2.1 Qin-Heron formula

An automatic deduction of a formula for the area of a triangle in terms of its sidelengths is a frequently used example of the sort.

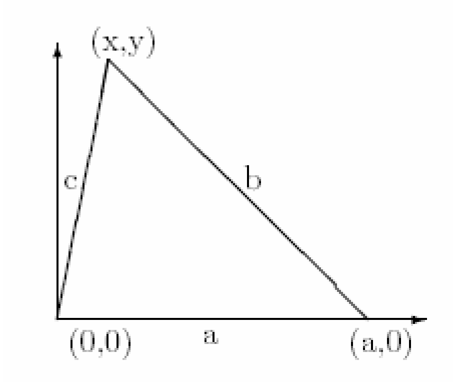

Figure 3: Qin-Heron formula

A convenient system of coordinates is as shown in the figure Fig. 3. By Pythagoras' theorem one has $b^2 = (a-x)^2 + y^2, c^2 = x^2 + y^2$, and evidently $2S = ay$ 2. Let us consider the ideal I generated by the polynomials $b^2-(a-x)^2-y^2, c^2-x^2-y^2, 2S-ay$ in the polynomial ring $IR[x,y,a,b,c,S]$. Eliminating x and y by computing $I \cap IR[a,b,c,S]$, one finds a principal ideal generated by

$$16S^2+a^4+b^4+c^4-2a^2b^2-2b^2c^2-2c^2a^2 \ .$$

One recognizes the familiar Qin-Heron formula for the area in terms of sidelengths.

2.2 Characterization of isosceles triangle

Using usual notations and relations, a Grobner basis computation shows that any triangle can be described by the following polynomial relations (cf. [6]):

$$p_1 := 2s-a-b-c, \quad p_2 := S-rs, \quad p_3 := 4RS-abc,$$
$$p_4 := (b+c-a)(a+b-c)(a-b+c)-8Sr.$$

A triangle is isosceles if and only if

$$p_5 := (a-b)(b-c)(c-a)=0.$$

What is the corresponding relation in terms of R, r, and s? To answer this question, we compute a Grobner basis of the ideal generated by $p_1,...,p_5$ with respect to the lexicographic ordering with $S > a > b > c > s > R > r$. One finds a polynomial $p_6r^2s^2$, with

$$p_6 := 64R^3r+48R^2r^2-4R^2s^2+12Rr^3-20Rrs^2+r^4+2r^2s^2+s^4.$$

Since s and r stand for positive quantities, it follows that p_6 vanishes in any isosceles triangle. To see whether its vanishing is a suffcient condition for a triangle to be isosceles, we compute a Grobner basis of $\mathrm{Ideal}(p_1,p_2,p_3,p_4,p_6)$ with respect to the lexicographic ordering with $S > s > R > r > a > b > c$. The output contains the polynomial $(a-b)^2(b-c)^2(c-a)^2b^2c$. The component relevant in the geometric context is p_5, so we conclude: *A triangle is isosceles if and only if* $p_6=0$.

2.3 Characterization of right triangles

Playing the same game, we automatically discovered the following facts:

Theorem 1.

$$\hat{A} = 90^\circ \Leftrightarrow ra = R(b + c - a) \Leftrightarrow 2Rs = a(r + 2R) \Leftrightarrow a = 2R \Leftrightarrow$$
$$\Leftrightarrow b + c = 2(R + r) \Leftrightarrow b + c = r + s \Leftrightarrow bc(b + c) = 4S(R + r).$$

Several implications are known and all of them are easy to prove by using elementary relations in the geometry of triangles. The point is that even having no clue of what one is searching for, one may obtain relevant information by simply changing the ordering used in Grobner basis computations.

3 A conjecture in the Euclidean geometry

Further modification of the fundamental techniques of automatic theorem proving allows one to automatically determine geometric loci. The key idea [8] is to make the hypothesis conditions depend on an indeterminate point *X* (locus point). In the process of reconciliation of the thesis polynomial with the hypothesis polynomials, a new condition involving *X* appears. Its factors containing the locus coordinates are the candidates to define equations of components of the geometric locus.

More than 20 years ago, Al.V. Mihai proposed the following problem:
Let M be a point in the interior of a square ABCD. Prove that the quadrilateral having vertices in the incenters of triangles ABM, BCM, CDM, DAM is cyclic.

Daia [4] found a counterexample to this statement: for M chosen such that ΔABM is equilateral, the incenters are not on the same circle. This configuration is well-known in the elementary geometry, and Daia uses some of its numerous properties to numerically compute the relevant distances, deriving a contradiction.

It is easy to see that any point on the diagonals of the square has the property Mihai asked for, so the question is to find all the points for which the property holds. As soon became clear, the answer seems to be:

Conjecture. *A point M in the interior of a square ABCD has the property that the quadrilateral having vertices in the incenters of triangles ABM, BCM, CDM, DAM is cyclic if and only if M belongs to AC or BD.*

The difficulty of this conjecture is due, on the one hand, to the fact that trigonometric functions are unavoidable when expressing the incenter in terms of the vertices of the triangle, and, on the other hand, to the intrinsic difficulty of checking that four points are on the same circle. When turning to computer algebra systems, the difficulties are the huge amount of computing time and memory needed to tackle the conjecture. However, the improvements of the hardware and software we have access to finally allowed a successful attack of the conjecture. Details will appear in a forthcoming paper [3].

References

[1] L. Bazzotti, G. Delzotto, L. Robbiano, Remarks on geometric theorem proving, in Automated Deduction in Geometry, 3rd Internat. Workshop ADG 2000, Z¨urich, Switzerland, Sept. 25–27, 2000, (J. Richter-Gebert, D. Wang, eds.), LNCS 2061, Springer, Berlin, 2001, pp. 104–128.
[2] S.-C. Chou, D. Lin, Wu's method for automated geometry theorem proving and discovering, in [5], pp. 125–146.
[3] M. Cipu, Cyclic quadrilaterals determined by incenters of a triangulation of the square, in preparation.
[4] L. Daia, On a conjecture (in Romanian), Gaz. Math., 89(1984), 276–279.
[5] X.-S. Gao, D. Wang, (eds.), Mathematical Mechanization and Applications, Academic Press, San Diego, 2000.
[6] W. Koepf, Gr¨obner bases and triangle, The Internat. J. Computer Algebra in Mathematics Education, 4(1997), 371–386.
[7] A.C. Hearn, REDUCE User's manual, version 3.6, RAND CO., Santa Monica, CA, 1996.
[8] E. Roanes-Mac´ýas, E. Roanes-Lozano, Automatic determination of geometric loci. 3D-extension of Simson-Steiner theorem, in Artificial Intelligence and Symbolic Computation, Internat. Conf. AISC 2000, Madrid, July 2000, (J.A. Campbell, E. Roanes-Lozano, eds.), LNAI 1930, Springer, 2001, pp. 157–173.
[9] G.-M. Greuel, G. Pfister, and H. Sch¨onemann. Singular 2.0. A Computer Algebra System for Polynomial Computations. Centre for Computer Algebra, University of Kaiserslautern (2001). http://www.singular.uni-kl.de.
[10] http://www-calfor.lip6.fr/~wang/index.html
[11] W.-t. Wu, Mechanical Theorem Proving in Geometry, Texts and Monographs in Symbolic Computation, Springer-Verlag, 1994.
[12] W.-t. Wu, The characteristic set method and its applications, in [5], pp. 3–41.

Author:
Mihai Cipu
Simion Stoilow Institute of Mathematics of the Romanian Academy, P.O. Box

1-764, RO-01400 Bucharest, Romania
email: mihai.cipu@imar.ro

Supported by the CERES program of the Ministry of Education, Research and Youth, contract nr. 39/2002