Automated Theorem Proving and GCLC Provers

Predrag Janičić
Faculty of Mathematics, University of Belgrade, Serbia
www.matf.bg.ac.yu/~janicic
email: janicic@matf.bg.ac.yu

Università degli Studi di Roma "La Sapienza"
Dipartimento di Matematica
Roma, Italy, November 13, 2008.

Agenda

- Early history of automated theorem proving in geometry
- Coordinate-free and coordinate-based methods:
  - The area method
  - Wu's and Gröbner bases methods
- Theorem provers built-into GCLC
- Intelligent mathematical software

Early History of Automated Theorem Proving in Geometry

Axiomatizations:

- Euclid's *Elements*
- Hilber's *Foundations of Geometry*
- Tarski's elementary geometry
- Avigad's Euclid-style geometry

Geometrical Theorems of Constructive Type

- Conjectures that corresponds to properties of constructions
- Usually, only Euclidean plane geometry
- Non-degenerate conditions are very important

Coordinate-free methods

Give traditional (human readable) proofs:

- Gelertner's theorem prover (Gelertner 1950's)
- Area method (Chou et.al.1992)
- Angle method (Chou et.al.1990's)
- ...

Coordinate-based methods

- Algebraic methods (no synthetic geometry proofs, just algebraic arguments):
  - Gröbner basis method (Buchberger 1965)
  - Wu's method (Wu 1977)
  - ...

Area method

The method deals with the following geometry quantities:

ratio of directed segments: for four collinear points P, Q, A, and B such that $A \neq B$, it is the ratio $\frac{\overrightarrow{PQ}}{\overrightarrow{AB}}$;

signed area: it is the signed area S_{ABC} of a triangle ABC or the signed area S_{ABCD} of a quadrilateral $ABCD$;

Area method (2)

Pythagoras difference: for three points, P_{ABC} is defined as follows:

$$P_{ABC} = AB^2 + CB^2 - AC^2 \ .$$

Pythagoras difference for four points, P_{ABCD} is defined as follows:

$$P_{ABCD} = P_{ABD} - P_{CBD} \ .$$

real number: it is a real number, constant.

Area method (3)

- All construction steps are reduced to a limited number of specific constructions

- The conjecture is also expressed as an equality over geometry quantities (over points already introduced)

- The goal is to prove the conjecture by reducing it to a trivial equality (0=0)

Area method (4)

points A and B are identical	$P_{ABA} = 0$
points A, B, C are collinear	$S_{ABC} = 0$
AB is perpendicular to CD	$P_{ACD} = P_{BCD}$
AB is parallel to CD	$S_{ACD} = S_{BCD}$
O is the midpoint of AB	$\frac{\overrightarrow{AO}}{\overrightarrow{OB}} = 1$
AB has the same length as CD	$P_{ABA} = P_{CDC}$
points A, B, C, D are harmonic	$\frac{\overrightarrow{AC}}{\overrightarrow{CB}} = \frac{\overrightarrow{DA}}{\overrightarrow{DB}}$

Area method (5)

- For reducing the goal, different simplifications are used:

$$\begin{aligned} x \cdot 1 &\rightarrow x \\ x \cdot 0 &\rightarrow 0 \\ S_{AAB} &\rightarrow 0 \\ S_{ABC} &\rightarrow S_{BCA} \end{aligned}$$

- Crucially, for each pair quantity-construction step there is one *elimination lemma* that enable eliminating a relevant point

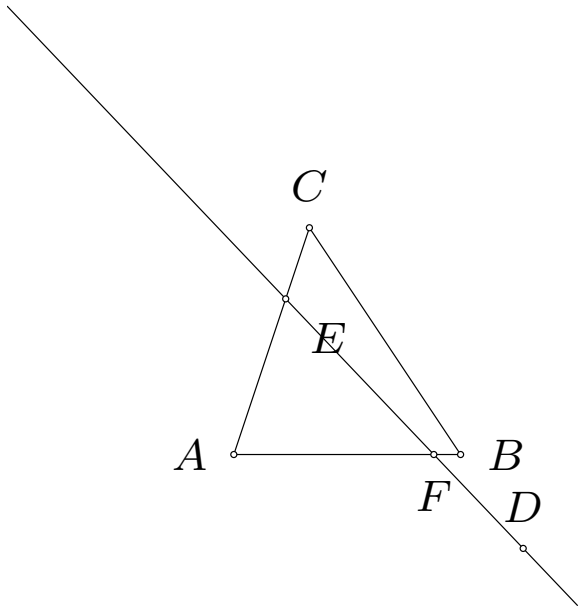
- Thank to these lemmas, the point are eliminated from the conjecture in opposite direction that they were introduced one by one

Area Method — Elimination lemmas

For instance, if a point Y was introduced as the intersection of lines UV and PQ, then Y can be eliminated from expression of the form $\frac{\overrightarrow{AY}}{\overrightarrow{CD}}$ using the following equality:

$$\frac{\overrightarrow{AY}}{\overrightarrow{CD}} = \begin{cases} \frac{S_{APQ}}{S_{CPDQ}}, & \text{if } A \in UV \\ \frac{S_{AUV}}{S_{CUDV}}, & \text{if } A \notin UV \end{cases}$$

Example: Menelaus's Theorem



- Conjecture:

$$\frac{\overrightarrow{AF}}{\overrightarrow{FB}} \cdot \frac{\overrightarrow{BD}}{\overrightarrow{DC}} \cdot \frac{\overrightarrow{CE}}{\overrightarrow{EA}} = -1$$

Example: Menelaus's Theorem (2)

- Fragment of the proof:

  $\left(\frac{\overrightarrow{AF}}{\overrightarrow{BF}} \cdot \left(\frac{\overrightarrow{BD}}{\overrightarrow{DC}} \cdot \frac{\overrightarrow{CE}}{\overrightarrow{EA}}\right)\right) = 1$, by algebraic simplifications

  $\left(\frac{S_{ADE}}{S_{BDE}} \cdot \left(\frac{\overrightarrow{BD}}{\overrightarrow{DC}} \cdot \frac{\overrightarrow{CE}}{\overrightarrow{EA}}\right)\right) = 1$, by Lemma 8 (point F eliminated)

  ...

  $0 = 0$, by algebraic simplifications

Coordinate-based (Algebraic) methods

- Geometry statements have the form of equalities

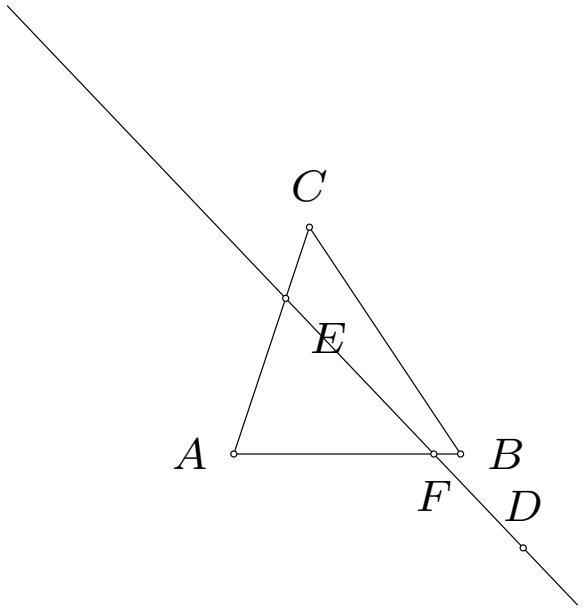
- Construction steps are converted into a polynomial system

$$\begin{aligned} h_1(u_1, u_2, \ldots, u_d, x_1, \ldots, x_n) &= 0 \\ h_2(u_1, u_2, \ldots, u_d, x_1, \ldots, x_n) &= 0 \\ &\ldots \\ h_t(u_1, u_2, \ldots, u_d, x_1, \ldots, x_n) &= 0 \end{aligned}$$

- The goal is to check whether for the conjecture it holds that

$$g(u_1, u_2, \ldots, u_d, x_1, \ldots, x_n) = 0$$

Example: Menelaus Theorem



- Coordinates assigned to the points:

  $A(0,0), B(u_1,0), C(u_2,u_3), D(x_1,u_4), E(x_2,u_5), F(x_4,0)$

Example: Menelaus Theorem (2)

- Conditions:

  D on BC: $p_1 = -u_3 x_1 + (u_4 u_2 - u_4 u_1 + u_3 u_1)$

  E on AC: $p_2 = -u_3 x_2 + u_5 u_2$

  F on DE: $p_3 = (-u_5 + u_4) x_4 - u_4 x_2 + u_5 x_1$

- Conjecture:

$$p_4 = (-u_5 u_3 + u_4 u_3) x_4 + (-u_5 u_4 u_1 + u_5 u_3 u_1)$$

Wu's Method

- Invented by Wu in 1977
- Considered to be the most efficient method for automated theorem proving in all fields (not only geometry)
- Considered to be one of the four modern great Chinese inventions
- Similar to Gauss' elimination procedure

Wu's Method on Menelaus Theorem

- For the above example, triangulation gives:

$$\begin{aligned} p_1 &= -u_3x_1 + (u_4u_2 - u_4u_1 + u_3u_1) \\ p_2 &= -u_3x_2 + u_5u_2 \\ p_3 &= (-u_5 + u_4)x_4 - u_4x_2 + u_5x_1 \end{aligned}$$

- Wu's elimination procedure in several steps gives $p_4 = 0$, which was required to prove

Gröbner-bases Method

- Invented by Buchberger in 1965, widely used CAS algorithm with many applications

- Gröbner basis (GB) is a particular kind of generating subset of an ideal of a polynomial ring R.

- Buchberger's algorithm builds GB for the set of polynomials corresponding to the construction and then it checks the conjecture, by efficiently testing whether its remainder with respect to GB is 0

- For reducing w.r.t. the Gröbner base, the ordering of reducing is irrelevant

Theorem Provers Built-into GCLC

- There are three theorem provers built-into GCLC:
  - a theorem prover based on the area method
  - a theorem prover based on the Wu's method
  - a theorem prover based on the Buchberger's method

- All of them are very efficient and can prove many non-trivial theorems in only milliseconds.

Using Theorem Provers Built-into GCLC

- The theorem provers are tightly built-in: the user has just to state the conjecture about the construction described.

- For example:

```
prove { identical O_1 O_2 }
```

Demo: Several Examples

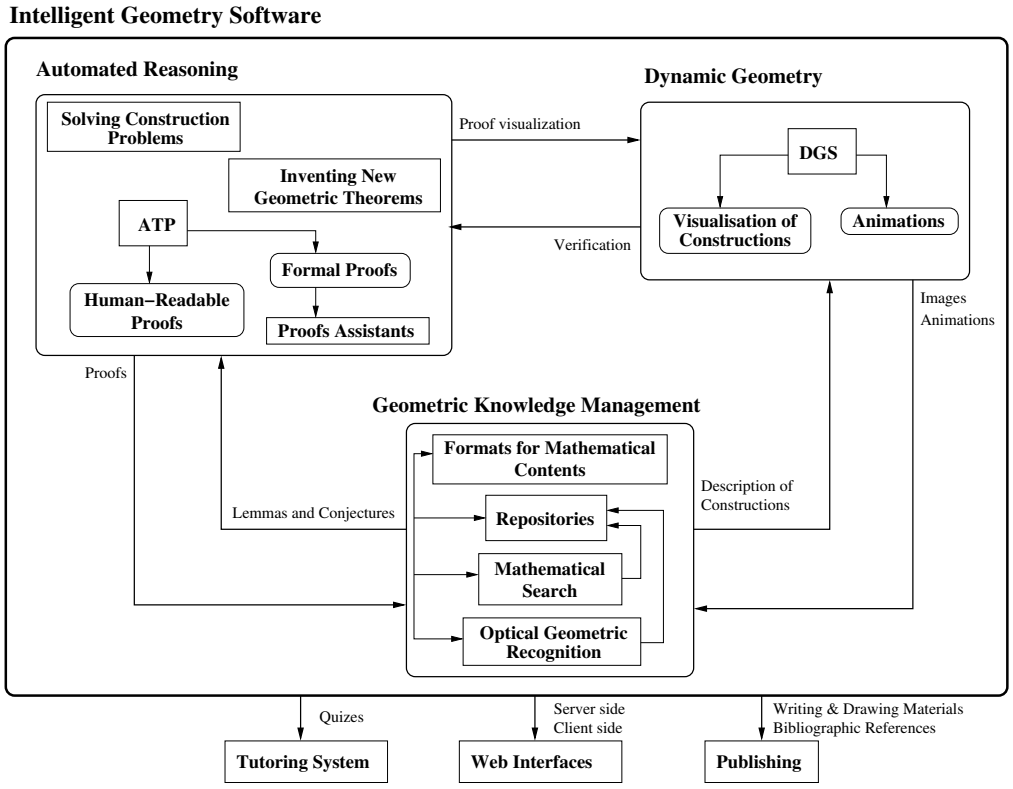
- The repository GeoThms `http://hilbert.mat.uc.pt/~geothms` (developed by Pedro Quaresma (Portugal) and Predrag Janičić) contains >100 theorems automatically proved

- Most of these theorems are included in the GCLC distribution available from the Internet

Processing Descriptions of Constructions

- Syntactical check
- Semantical check (e.g., whether two concrete points determine a line)
- Deductive check — verifies if a construction is regular (e.g., whether two constructed points never determine a line)

Intelligent Geometrical Software



Conclusions

- Dynamic geometry tools are around for twenty years but just recently they started to be very intelligent

- Automated geometrical theorem provers are around for forty years but just recently they started to work in harmony with dynamic geometry tools

- GCLC aims to be a powerful geometrical assistant