Automated Geometry Theorem Proving: Readability vs. Efficiency

Predrag Janičić
URL: www.matf.bg.ac.rs/~janicic
Faculty of Mathematics, University of Belgrade, Serbia

CADGME; Convergence on Mathematics Assistants
RISC, Castle of Hagenberg, Austria, July 11-13, 2009.

Agenda

- Brief history of automated theorem proving in geometry
- Provers and proofs in GCLC
- Some remedies for readability vs. efficiency issues

Geometrical Theorems of Constructive Type

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

Automated Theorem Proving in Geometry

- Around for more than 50 years
- Early AI-based approaches in 50's
- Huge successes made by algebraic theorem provers in 80's
- Successes made by semi-algebraic theorem provers in 90's
- Synthetic proofs generated by coherent-logic provers in 2000's

Coordinate-based (Algebraic) Methods

- No synthetic geometry proofs, only algebraic justification
- Premises and goals have the form of equalities
- Construction steps are converted into a polynomial system

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

- Check whether for the conjecture it holds that

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

Gröbner-bases Method

- Invented by Buchberger in 1965, widely used 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 premises and then it checks the conjecture, by testing if its remainder with respect to GB is 0

Wu's Method

- Invented by Wu in 1977
- Considered to be one of the four modern great Chinese inventions
- Similar to Gauss' elimination procedure: it performs triangulation of the system, and then reduces the goal polynomial

Coordinate-free Methods

Attempt to give traditional (human readable) proofs:

- Area method (Chou et.al.1992) (semi-algebraic)
- Angle method (Chou et.al.1990's) (semi-algebraic)
- ...

Area Method: Geometric Quantities

The method deals with the following geometry quantities:

ratio of directed segments: $\frac{\overrightarrow{PQ}}{\overrightarrow{AB}}$ for collinear points P, Q, A, B

signed area: S_{ABC} and S_{ABCD}

Pythagoras difference: $P_{ABC} = AB^2 + CB^2 - AC^2$

real number: a constant real number

Area Method: Some Properties Expressed

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	$P_{ABA} = P_{CDC}$

Area Method: Stating a Conjecture

- 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: Basic Idea

- For reducing the goal, a range of simplification rules are used
- Crucially, for each pair quantity-construction step there is one *elimination lemma* that enable eliminating a relevant point
- Example: if a point Y was introduced as the intersection of lines UV and PQ, then Y can be eliminated from $\frac{\overrightarrow{AY}}{\overrightarrow{CD}}$ by using:

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

Coherent Logic-based Theorem Provers

- Coherent logic — sometimes called *geometry logic*
- Only formulae of the following form are considered:

$$\forall \vec{x}(A_1 \wedge \ldots \wedge A_n) \Rightarrow \exists \vec{y}(B_1 \vee \ldots \vee B_m))$$

- Explored by Skolem in 1920's
- Automated by Kordić and Janičić in 1993
- From 2000, given a good theoretical ground and promoted by Marc Bezem and his coauthors

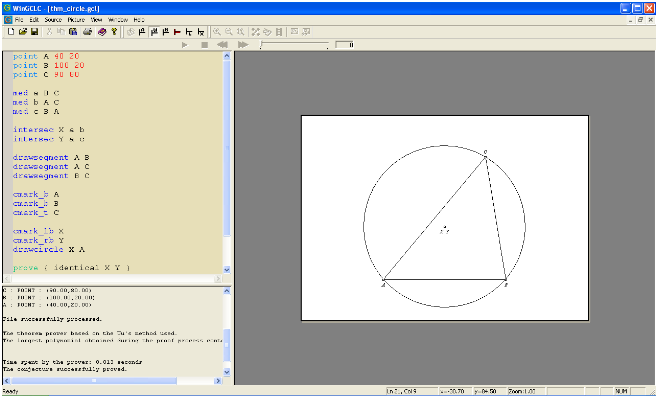
Coherent Logic-based Theorem Provers

- It is suitable for automation, by simple forward chaining
- Produces fully readable, traditional, synthetic geometry proofs
- In a sense, it is an alternative to the resolution method (admits existential quantification)
- The goal to be proved is not transformed, so the link between automated and interactive proving is preserved
- Many theories can be expressed within coherent logic

GCLC/WinGCLC

- Developed since 1996.
- Originally, a tool for producing geometrical illustrations in LaTeX, today — much more than that
- Freely available from
  http://www.matf.bg.ac.rs/~janicic/gclc
- Used in:
  - producing digital mathematical illustrations
  - mathematical education
  - storing mathematical contents
  - studies of automated geometrical reasoning

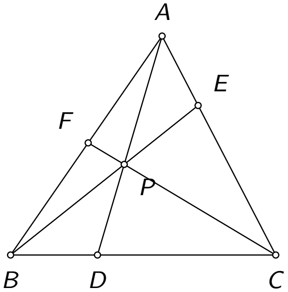
Screenshot of WinGCLC



Theorem Provers Built-into GCLC

- There are three theorem provers built-into GCLC:
  - a theorem prover based on Wu's method
  - a theorem prover based on Buchberger's method
  - a theorem prover based on the area method
- All of them are very efficient and can prove many non-trivial theorems in only milliseconds
- The provers are tightly built-in: the user has just to state the conjecture after the description of a construction, for example:
  `prove { identical O_1 O_2 }`

Example: Ceva's Theorem



- Conjecture:

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

- Outputs by the three provers...

New Coherent-logic Based Prover (Current Work)

- New, generic theorem prover, implemented in C++
- Being developed with geometry in mind
- To be built into GCLC
- Exports formal, machine verifiable, proofs to proof assistants Isabelle and Coq
- More suitable for low level conjectures (based directly on axioms), rather than high-level conjectures (about constructions)

Example (generated by the prover from 1990's)

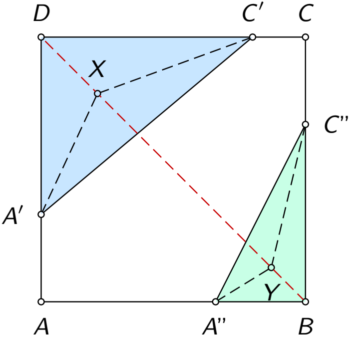
- Conjecture: if two lines *a* and *b* both contain two distinct points *A* and *B*, then *a* and *b* are identical.
- Proof: Since both *a* and *b* contain *A*, they intersect.
  By Axiom 1.3, since *a* and *b* contain two different points (*A* and *B*), they are identical.
  The theorem was proved (time: 0.00s)
- Nice, but it couldn't prove there is a point between two distinct points

Currently Typical Pattern

Algebraic	Semi-algebraic	Synthetic
Efficient		Readable

Using Lemmas: Example

- If the bisectors of angles $DC'A'$ and $DA'C'$ intersect in X, and the bisectors of $BC''A''$ and $BA''C''$ intersect in Y, then D, X, Y, are B collinear



- Use the fact that all three angle bisector intersect in one point

Using Lemmas: Basic Idea

- Detect all lemmas (from a database) that apply
- Reduce the goal polynomial w.r.t. lemmas' goals
- Prove the new goal
- The proof will still be algebraic, but it would point to relevant facts used, which can be very helpful

Improving Coherent Provers: Basic Ideas

- Coherent-logic-based provers use simple forward chaining and not much guiding
- They do not try to detect irrelevant facts and to use such knowledge in further search
- Use techniques from other automated reasoning tasks (e.g., backjumping from SAT solving) that do such things
- Another idea: use lemmas

Conclusions and Future Work

- Automated reasoning in geometry is around for a half of a century, but there are still no provers that are efficient and produce traditional, readable proofs
- The most efficient theorem provers produce least readable proofs
- Efficient, algebraic provers can use lemmas and point to relevant facts used
- There is a room for improving efficiency of synthetic provers
- It is still to be explored how different proving methods can benefit from each other