Automated Proving in Geometry using Gröbner bases in Isabelle/HOL

Danijela Petrović Filip Marić Predrag Janičić
{danijela,filip,janicic}@matf.bg.ac.rs

Department of Computer Science
Faculty of Mathematics
University of Belgrade

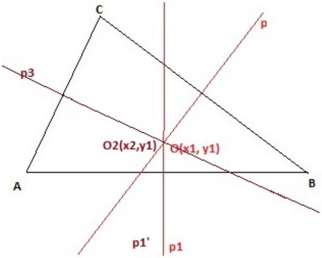
Fourth Workshop on Formal and Automated Theorem Proving and Applications

Outline

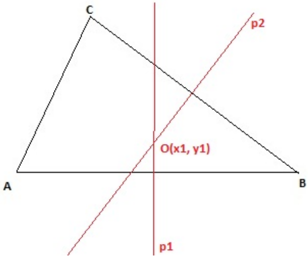
Outline

Motivation example

- The goal is to show that bisetors of the sides of triangle are intersecting in one point

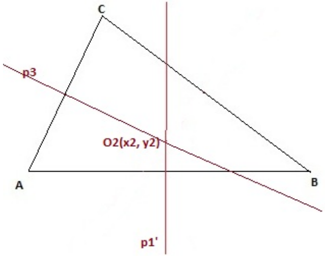


Motivation example



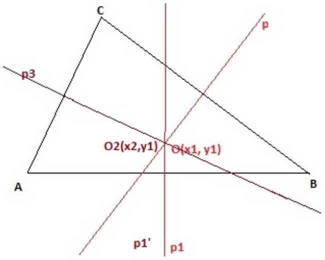
- A(0, 0), B(0, c), C(a, b)
- $O_1(x_1, y_1) = p_1 \cap p_2$
- $p_1 = x_1 - \frac{c}{2}$
- $p_2 = \frac{c-a}{b}x_1 - y_1 + \frac{b^2-c^2+a^2}{2b}$

Motivation example



- A(0, 0), B(0, c), C(a, b)
- $O_2(x_2, y_2) = p_1' \cap p_3$
- $p_1' = x_2 - \frac{c}{2}$
- $p_3 = \frac{a}{b}x_2 + y_2 - \frac{b}{2} - \frac{a^2}{2b}$

Motivation example



- $A(0,0), B(0,c), C(a,b)$
- $O_1(x_1,y_1) = O_2(x_2,y_2)$
- $G = \{x_1 - \frac{c}{2},\ \frac{c-a}{b}x_1 - y_1 + \frac{b^2-c^2+a^2}{2b},\ x_2 - \frac{c}{2},\ \frac{a}{b}x_2 + y_2 - \frac{b}{2} - \frac{a^2}{2b}\}$

Motivation example

The problem $O_1(x_1, y_1) = O_2(x_2, y_2)$ is now to show that polynomials
$g_1 = x_1 - x_2$ and $g_2 = y_1 - y_2$
belong to the ideal generated over the set G.
We can do that by calculating the Gröbner basis G' of the set G and showing:

i) $g_1 = x_1 - x_2 \xrightarrow{*}_{G'} 0$

ii) $g_2 = y_1 - y_2 \xrightarrow{*}_{G'} 0$

Motivation example

- New set: $G' = \{p_1, p_2, p_3, p_1', S_1, S_2\} =$
  $\{x_1 - \frac{c}{2},$
  $\frac{c-a}{b}x_1 - y_1 + \frac{b^2-c^2+a^2}{2b},$
  $\frac{a}{b}x_2 + y_2 - \frac{b}{2} - \frac{a^2}{2b},$
  $x_2 - \frac{c}{2},$
  $-y_1 + \frac{b}{2} + \frac{a^2}{2b} - \frac{ac}{2b},$
  $y_2 - \frac{b}{2} - \frac{a^2}{2b} + \frac{ac}{2b}\}$
- We can show: $g_1 = x_1 - x_2 \xrightarrow{*}_{G'} 0$
- We can show: $g_2 = y_1 - y_2 \xrightarrow{*}_{G'} 0$

Outline

Term representation of geometry constructions

- We use term representation for geometry constructions
- Each object has term representation, for example:
  - line = Line point point
  - or: line = Bisector point point
  - etc.
- Each statement has term representation, for example:
  - In point line
  - Equal point point
  - etc.

Outline

Algorithm

- Term representation of our example:

Equal(
Intersect(Bisector(Point 1, Point 2), Bisector(Point 2, Point 3))),
Intersect(Bisector(Point 1, Point 2), Bisector(Point 1, Point 3))))

- Algorithm for making two set of polynomials from term representation of geometry construction
- From the second set we get Gröbner basis G'
- From the first set we get polynomials that should go to 0 by polynomial reduction with elements from G'

Algorithm

- Algorithm is recursive, for each object we add new variables and call function to read the rest of the term
- For examle:
  - In point_t line_t
  - add variables x1 i y1 - coordinates for point (for examle $O(x_1, y_1)$)
  - add variables a1 i b1 - coefficients for line (for example $p = a_1 \cdot x + b_1 \cdot y + 1$)
  - call point_poly(point_t, x1, y1)
  - call line_poly(line_t, a1, b1)
  - we add in first set the polynomial: a1x1 + b1y1 + 1
- For representing polynomials in Isabelle we use work of Christian Sternagel and Ren Thiemann - *Executable Multivariate Polynomials*

Outline

Conclusion and future work

- Including more geometry objects
- Implementing algorithm in wider range of geometry statements to show their corectness
- Using implemented method for calculating Gröbner basis in Isabelle
- Implementing Buchberger's algorithm (with heuristics) for transforming the set of polynomials in Gröbner basis in some imperative language (for examle C) and proving its corectness in Isabelle