Automatic rewrites of input expressions in complex algebraic geometry provers

Zoltán Kovács[1], Tomás Recio[2] and Csilla Sólyom-Gecse[3]

[1]Private University College of Education
of the Diocese of Linz, Austria

[2]Depto. de Matemáticas, Estadística y Computación
Universidad de Cantabria, Santander

[3]Babeș-Bolyai University, Cluj-Napoca, Romania

Abstract

We present an algorithm to help converting expressions having non-negative quantities (like distances) in Euclidean geometry theorems to be usable in a complex algebraic geometry prover. The algorithm helps in refining the output of an existing prover, therefore it supports immediate deployment in high level prover systems.

Introduction

- Dynamic geometry systems (DGS) + Automated theorem proving (ATP)
  - Thesis in elementary geometry theorems
    - equation in variables of lengths, angles, areas or volumes (e.g. Pythagorean theorem, Ptolemy's theorem, Heron's formula)

Entering formulas in OpenGeoProver

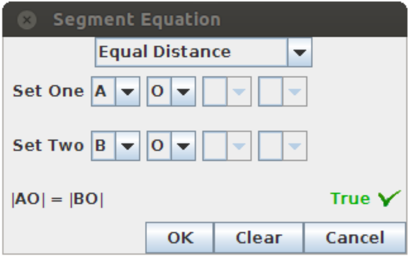
Example (Ptolemy's theorem)

If $ABCD$ is convex quadrilateral inscribed in given circle k, then $AC \cdot BD = AB \cdot CD + BC \cdot DA$ holds, i.e. product of diagonals is equal to sum of products of opposite edges.

```
<statement>
    <algsumsegs>
        <segprod>
            &lt;segment point1="A" point2="C" /&gt;
            &lt;segment point1="B" point2="D" /&gt;
        </segprod>
        <segprod>
            &lt;segment point1="A" point2="B" /&gt;
            &lt;segment point1="C" point2="D" /&gt;
        </segprod>
        <segprod>
            &lt;segment point1="B" point2="C" /&gt;
            &lt;segment point1="D" point2="A" /&gt;
        </segprod>
    </algsumsegs>
</statement>
```

Entering formulas in Java Geometry Expert 0.80

Example (Distance between a circle's center and its points)



Chou's list

Chou 1987 presents a list of cases when translating statements into unordered geometry:

- the length of a segment (which should be substituted by its square),
- the equality of length of two segments ($a = b \iff a - b = 0 \to a^2 - b^2 (= 0)$),
- the equality of product of two segments ($a \cdot b = c \cdot d \iff ab - cd = 0 \to a^2 b^2 - c^2 d^2$),
- a ratio of length of two segments ($3a = 7b \to 9a^2 - 49b^2$),
- the sum of length of two segments is a third length ($a + b = c \to$ $(a - b - c) \cdot (a - b + c) \cdot (a + b - c) \cdot (a + b + c)$).

The difficulty of the case $a + b = c$

Theorem

Let a be the length of the segment joining the free points A and B. Define point C as an arbitrary point of this segment and let the length of segment AC be b and that of BC be c. Now $a = b + c$.

Proof by using Gröbner bases, Kapur 1986, Cox 2007.

- Variables: $v_1, v_2, v_3, v_4, v_5, v_6, a, b, c, z$.
- Points: $A = (v_1, v_2)$, $B = (v_3, v_4)$, $C = (v_5, v_6)$.
- Hypotheses equations:
  - $v_1 v_4 + v_3 v_6 + v_5 v_2 - v_1 v_6 - v_3 v_2 - v_5 v_4 = 0$,
  - $a^2 = (v_1 - v_3)^2 + (v_2 - v_4)^2$,
  - $b^2 = (v_1 - v_5)^2 + (v_2 - v_6)^2$,
  - $c^2 = (v_3 - v_5)^2 + (v_4 - v_6)^2$.
- Denied thesis: $z(a - b - c) = 1$.

The difficulty of the case $a + b = c$

Theorem

Let a be the length of the segment joining the free points A and B. Define point C as an arbitrary point of this segment and let the length of segment AC be b and that of BC be c. Now $a = b + c$.

Proof by using Gröbner bases, Kapur 1986, Cox 2007.

- CAS input (Singular):

```
ring r=(0,v1,v2,v3,v4,v5),(v6,a,b,c,z),dp;
ideal i=v1*v4+v3*v6+v5*v2-v1*v6-v3*v2-v5*v4,
 a^2-(v1-v3)^2-(v2-v4)^2,
 b^2-(v1-v5)^2-(v2-v6)^2,
 c^2-(v3-v5)^2-(v4-v6)^2,
 z*(a-b-c)-1;
groebner(i);
```

- CAS output should be $\langle 1 \rangle$, but it differs.

The difficulty of the case $a + b = c$

Theorem

Let a be the length of the segment joining the free points A and B. Define point C as an arbitrary point of this segment and let the length of segment AC be b and that of BC be c. Now $a = b + c$.

Proof by using Gröbner bases, Kapur 1986, Cox 2007.

- Modified CAS input (Singular):

```
ring r=(0,v1,v2,v3,v4,v5),(v6,a,b,c,z),dp;
ideal i=v1*v4+v3*v6+v5*v2-v1*v6-v3*v2-v5*v4,
 a^2-(v1-v3)^2-(v2-v4)^2,
 b^2-(v1-v5)^2-(v2-v6)^2,
 c^2-(v3-v5)^2-(v4-v6)^2,
 z*((a-b-c)*(a-b+c)*(a+b-c)*(a+b+c))-1;
groebner(i);
```

- CAS output is $\langle 1 \rangle$.

$\square$

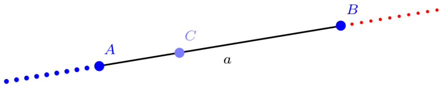
The difficulty of the case $a + b = c$: a reformalized theorem

Theorem

Let us denote by a the length of the segment AB by joining the free points A and B. Define point C as an arbitrary point of the line going through A, B*, and let length*$(AC) = b$ *and length*$(BC) = c$*. Now* $a = b + c$*, unless* $b = a + c$ *or* $c = a + b$.

Degenerate and essential conditions

- Degenerate:
  - $a + b + c \neq 0$
- Essential:
  - $b \neq a + c$ $\cdots$
  - $c \neq a + b$ $\cdots$



Minimal extended polynomial (MEP)

Given the input polynomial equation $p = 0$ where p is squarefree, we define $\mathrm{MEP}(p)$ which will be used instead of p but with the same role. In our example, let $p = a - b - c$.

```
>> factor(eliminate([a-b-c,a^2=A^2,b^2=B^2,c^2=C^2],
    [a,b,c]))
```

that is, we eliminate all terms from p which are not of even powers of a, b, c. The result is:

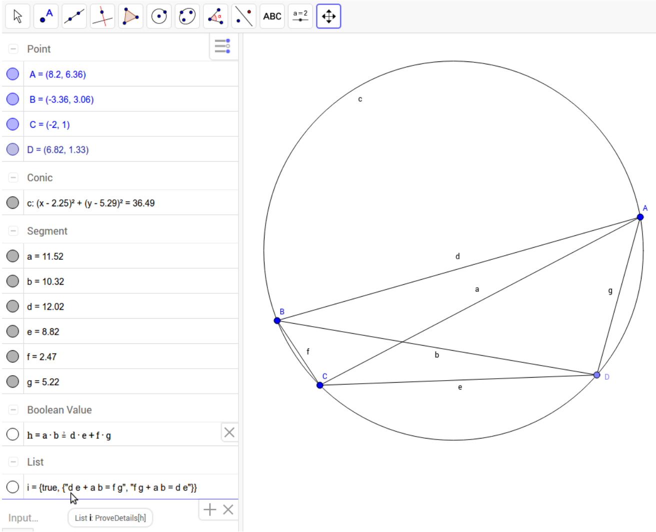
```
[(A-B-C)*(A-B+C)*(A+B-C)*(A+B+C)]
```

Theorems checked with the MEP approach

- Pythagorean –
- the cathetus –
- the geometric mean –
- the angle bisector –
- the intercept –
- Ceva's –
- Menelaus' –
- Ptolemy's –
- Heron's formula

Detailed list at `http://tinyurl.com/adg16-formula-rewrite` (generated on a daily basis automatically from the latest source code of the open DGS GeoGebra)

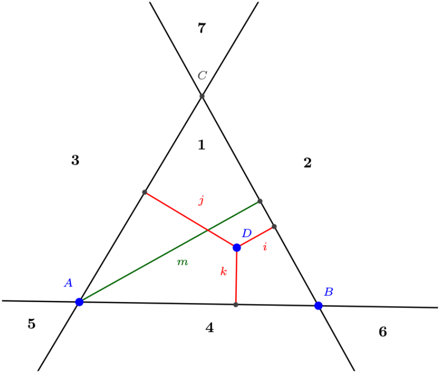
Entering formulas in GeoGebra 5.0.250.0



Viviani's theorem

Theorem

Let ABC be a regular triangle and D an internal point of it. Let i, j and k be the distance of D from the sides of the triangle, respectively. Then $i + j + k$ is a constant (namely, the height m of the triangle).



Viviani's theorem, essential conditions

Area	Equation	Condition
1	$i + j + k - m = 0$	(thesis)
2	$i - j - k + m = -(-i + j + k - m) = 0$	essential
3	$i - j + k - m = 0$	essential
4	$i + j - k - m = 0$	essential
5	$i - j - k - m = -(-i + j + k + m) = 0$	essential
6	$i - j + k + m = 0$	essential
7	$i + j - k + m = 0$	essential
(8)	$i + j + k + m = 0$	degeneracy

The minimal extended polynomial

$$
\begin{aligned}
\mathrm{MEP}(i+j+k-m) =& (i+j+k-m)\cdot \\
& (i-j-k+m)\cdot \\
& (i-j+k-m)\cdot \\
& (i+j-k-m)\cdot \\
& (i-j-k-m)\cdot \\
& (i-j+k+m)\cdot \\
& (i+j-k+m)\cdot \\
& (i+j+k+m)
\end{aligned}
$$

Viviani's theorem (reformalized)

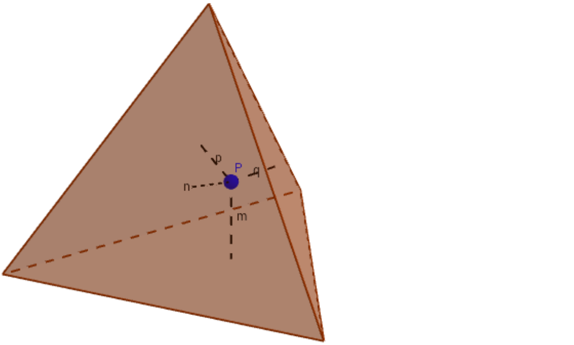
Theorem

Let ABC be a regular triangle and D another point on the plane. Let i, j and k be the distance of D from the sides of the triangle, respectively. Let m be the height of the triangle. Then, provided that none of the conditions

- $i + m = j + k$,
- $i + k = j + m$,
- $i + j = k + m$,
- $i = j + k + m$,
- $j = i + k + m$,
- $k = i + j + m$

hold, $i + j + k = m$ follows.

Viviani's theorem (3D generalization)



GeoGebra applet is available at
`https://www.geogebra.org/m/a9J4F4Qj`

Other uses: definition of hyperbola/ellipse

Given a hyperbola h with foci A and B and point C, another point P is an element of the hyperbola if and only if $|AC - CB| = |AP - PB|$, that is, $(AC - CB)^2 = (AP - PB)^2$. Let $p_h = (AC - CB)^2 - (AP - PB)^2 = (AC - CB - AP + PB) \cdot (AC - CB + AP - PB)$. Similarly, for an ellipse e described with the same points, $AC + CB = AP + PB$ holds, so we set $p_e = AC + CB - AP - PB$.

By using the MEP approach for the inputs p_h and p_e we get

$$\begin{aligned}
\mathrm{MEP}(p_h) = \mathrm{MEP}(p_e) = & p_h \cdot p_e \cdot \\
& (AC + CB - AP - PB) \cdot \\
& (AC + CB + AP - PB) \cdot \\
& (AC + CB + AP + PB) \cdot \\
& (AC - CB - AP - PB) \cdot \\
& (AC - CB + AP + PB)
\end{aligned}$$

The last 5 factors are geometrically degenerate cases, that is, the hyperbola and the ellipse are undistinguishable, but there are no other geometrical curves which can be mixed with them in the CAG approach.

Computational complexity

Given a squarefree input polynomial p with ℓ terms which are not of even power, (independently of the number of even powers in p) the output polynomial will consist of 2^{ℓ} (or eventually $2^{\ell-1}$) factors: the expansion of the output polynomial will consist of doubly exponential number of terms of the number of not even powers:

Theorem

Let p consist of k terms of even power: $a_1 t_1^2, a_2 t_2^2, \ldots, a_k t_k^2$, and ℓ terms which are not of even power: $t'_1, t'_2, \ldots, t'_\ell$, that is, $p = a_1 t_1^2 + \ldots + a_k t_k^2 + t'_1 + \ldots + t'_\ell$. Now $\mathrm{MEP}(p)$ is

- *a product of 2^{ℓ} factors if $k > 0$,*
- *a product of $2^{\ell-1}$ factors if $k = 0$.*

Summary

The opportunity to type arbitrary expressions (involving distances, lengths, volumes, etc.) is, in our opinion, a desirable feature of theorem provers in a DGS, allowing the user to access new horizons in studying, discovering and enjoying Euclidean geometry.

References I

A. Bogomolny.
Viviani's 3D Analogue from Interactive Mathematics Miscellany and Puzzles.
Downloaded from http://www.cut-the-knot.org/triangle/VivianiTetrahedron.shtml, accessed in April 2016.

F. Botana, M. Hohenwarter, P. Janičić, Z. Kovács, I. Petrović, T. Recio and S. Weitzhofer.
Automated Theorem Proving in GeoGebra: Current Achievements.
J Autom Reasoning, 55(1):39–59, March 2015.

K. Brown.
Polynomials For Sums of Square Roots.
Downloaded from http://www.mathpages.com/home/kmath111/kmath111.htm, accessed in February 2016.

References II

S.-C. Chou.
Mechanical Geometry Theorem Proving.
Springer Science + Business Media, 1987.

D. Cox, J. Little and D. O'Shea.
Ideals Varieties and Algorithms.
Springer New York, 2007.

W. Decker, G.-M. Greuel, G. Pfister and H. Schönemann.
SINGULAR 4-0-2 — A computer algebra system for polynomial computations.
2015.
http://www.singular.uni-kl.de.

References III

Z. Kovács and B. Parisse.
Giac and GeoGebra – Improved Gröbner basis computations.
Computer Algebra and Polynomials, Volume 8942 of the series Lecture Notes in Computer Science, 126–138.
Springer, 2015.

D. Kapur.
Using Gröbner bases to reason about geometry problems.
Journal of Symbolic Computation, 2(4):399–408, December 1986.

Z. Kovács, C. Sólyom-Gecse.
GeoGebra Tools with Proof Capabilities, 2016.
http://arxiv.org/abs/1603.01228.

References IV

B. Kutzler and S. Stifter.
On the application of Buchberger's algorithm to automated geometry theorem proving.
Journal of Symbolic Computation, 2(4):389–397, December 1986.

I. Petrović and P. Janičić.
Integration of OpenGeoProver with GeoGebra, 2012.
http://argo.matf.bg.ac.rs/events/2012/fatpa2012/slides/IvanPetrovic.pdf.

T. J. Recio Muñiz.
Cálculo simbólico y geométrico.
Editorial Síntesis. Madrid, 1998.

References V

Z. Ye, S.-C. Chou and X.-S. Gao.
An Introduction to Java Geometry Expert.
In *Automated Deduction in Geometry*, pages 189–195.
Springer Science + Business Media, 2011.