数理解析研究所講究録
第 1976 巻 2015 年 52-61

初等幾何学の階層付けと自動定理証明 - Hierarchies of Elementary Geometry and Automated Theorem Proving -

佐藤洋祐*
東京理科大学
YOSUKE SATO
TOKYO UNIVERSITY OF SCIENCE

1 Introduction

Any theorem of elementary geometry can be represented as a polynomial sentence. It can be automatically proved by real Quantifier Elimination(real QE) at least from theoretical point of view.
But the computation of real QE is very heavy in general, there exist many theorems which can not be handle by any of the latest existing real QE software.

There are four hierarchies of theorems of elementary geometry.

Definition 1 (**Hierarchies is elementary geometry**)
(1) A sentence of elementary geometry is called a theorem of *affine geometry* if it is true in a structure of any field with characteristic 0.
(2) A sentence of elementary geometry is called a theorem of *metric geometry* if it is true in a structure of any field with characteristic 0 which is closed under any two dimensional algebraic extension. Such a field is called a *metric field.*
(3) A sentence of elementary geometry is called a theorem of *Hilbert geometry* if it is true in a structure of any *ordered field* with characteristic 0 which is closed under any two dimensional algebraic extension. Such a field is called a *Hilbert field.*
(4) A sentence of elementary geometry is called a theorem of *Tarski geometry* if it is true in a structure of any *real closed field.*

We show how we can handle some of them without real QE.

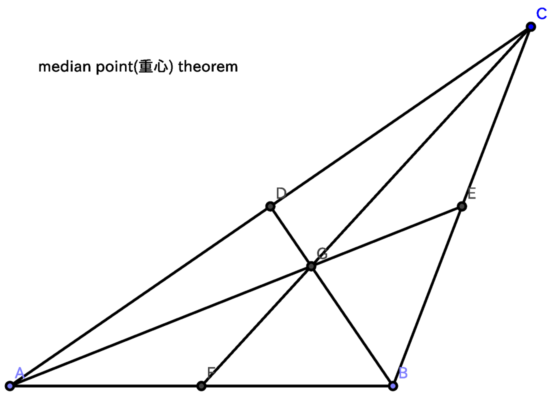
2 Affine geometry

Consider the following theorem.

*ysato@rs.kagu.tus.ac.jp

Theorem 2 The median point of a triangle is the intersection point of its three median lines.

Let G be the median point of a triangle △ABC, let D, E and F be the midpoints of the line segments AC, CB, AB respectively. Let the coordinates of A,B,C and G be A(a_1, a_2), B(b_1, b_2), C(c_1, c_2) and G(g_1, g_2).



Then the coordinate of D, E and F are D$(\frac{a_1+c_1}{2}, \frac{a_2+c_2}{2})$, E$(\frac{b_1+c_1}{2}, \frac{b_1+c_2}{2})$, F$(\frac{a_1+b_1}{2}, \frac{a_2+b_2}{2})$.
We have the following polynomial interpretations of geometric properties:

- The points A,B and C are not colinear $\Leftrightarrow \begin{vmatrix} c_1 - a_1 & c_2 - a_2 \\ c_1 - b_1 & c_2 - b_2 \end{vmatrix} \neq 0.$
- AG//AE $\Leftrightarrow g_1 - a_1 : g_2 - a_2 = \frac{b_1+c_1}{2} - a_1 : \frac{b_2+c_2}{2} - a_2$
  $\Leftrightarrow (g_1 - a_1) * (\frac{b_2+c_2}{2} - a_2) = (g_2 - a_2) * (\frac{b_1+c_1}{2} - a_1).$
- BG//BD $\Leftrightarrow g_1 - b_1 : g_2 - b_2 = \frac{a_1+c_1}{2} - b_1 : \frac{a_2+c_2}{2} - b_2$
  $\Leftrightarrow (g_1 - b_1) * (\frac{a_2+c_2}{2} - b_2) = (g_2 - b_2) * (\frac{a_1+c_1}{2} - b_1).$
- CG//CF $\Leftrightarrow g_1 - c_1 : g_2 - c_2 = \frac{a_1+b_1}{2} - c_1 : \frac{a_2+b_2}{2} - c_2$
  $\Leftrightarrow (g_1 - c_1) * (\frac{a_2+b_2}{2} - c_2) = (g_2 - c_2) * (\frac{a_1+b_1}{2} - c_1).$

The theorem is translated to the following polynomial sentence.

$$\forall a_1, a_2, b_1, b_2, c_1, c_2, g_1, g_2 \in \mathbb{R} \quad \begin{vmatrix} c_1 - a_1 & c_2 - a_2 \\ c_1 - b_1 & c_2 - b_2 \end{vmatrix} \neq 0 \quad \Rightarrow$$

$$\left(\begin{array}{l} g_1 = \frac{a_1+b_1+c_1}{3} \wedge g_2 = \frac{a_2+b_2+c_2}{3} \\ \quad \Leftrightarrow \\ (g_1 - a_1) * (\frac{b_2+c_2}{2} - a_2) = (g_2 - a_2) * (\frac{b_1+c_1}{2} - a_1) \wedge \\ (g_1 - b_1) * (\frac{a_2+c_2}{2} - b_2) = (g_2 - b_2) * (\frac{a_1+c_1}{2} - b_1) \wedge \\ (g_1 - c_1) * (\frac{a_2+b_2}{2} - c_2) = (g_2 - c_2) * (\frac{a_1+b_1}{2} - c_1) \end{array} \right)$$

We can *automatically* show that it is true by real QE.

Real QE is a heavy computation. We do not need real QE for proving the theorem.

We actually have the following property:

$$\forall a_1, a_2, b_1, b_2, c_1, c_2, g_1, g_2 \in K \quad \begin{vmatrix} c_1 - a_1 & c_2 - a_2 \\ c_1 - b_1 & c_2 - b_2 \end{vmatrix} \neq 0 \quad \Rightarrow$$

$$\left(\begin{array}{l} g_1 = \frac{a_1+b_1+c_1}{3} \wedge g_2 = \frac{a_2+b_2+c_2}{3} \\ \Leftrightarrow \\ (g_1 - a_1) * (\frac{b_2+c_2}{2} - a_2) = (g_2 - a_2) * (\frac{b_1+c_1}{2} - a_1) \wedge \\ (g_1 - b_1) * (\frac{a_2+c_2}{2} - b_2) = (g_2 - b_2) * (\frac{a_1+c_1}{2} - b_1) \wedge \\ (g_1 - c_1) * (\frac{a_2+b_2}{2} - c_2) = (g_2 - c_2) * (\frac{a_1+b_1}{2} - c_1) \end{array} \right)$$

Where K is any field with characteristic 0.

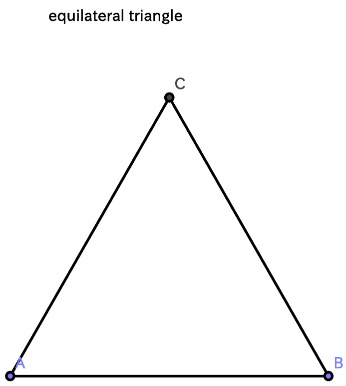
We can prove that this sentence is true by complex Quantifier Elimination (complex QE). In general, the computations of complex QE is much faster than the computation of real QE.

The above theorem belongs to affine geometry.

3 Metric geometry

Consider the following theorem.

Theorem 3 For any pair of distinct two points A and B, there exists another point C such that the triangle △ABC is equilateral.



Let the coordinates of A, B and C be A(a_1, a_2), B(b_1, b_2), C(c_1, c_2), then the theorem is translated to the following polynomial sentence.

$\forall a_1, a_2, b_1, b_2 \in \mathbb{R}\ (a_1 \neq b_1 \vee a_2 \neq b_2) \ \Rightarrow$
$\exists c_1, c_2 \in \mathbb{R}\ (a_1 - c_1)^2 + (a_2 - c_2)^2 = (b_1 - c_1)^2 + (b_2 - c_2)^2 = (a_1 - b_1)^2 + (a_2 - b_2)^2.$

Actually the following property holds.

$\forall a_1, a_2, b_1, b_2 \in \mathbb{C}\ (a_1 \neq b_1 \vee a_2 \neq b_2)\ \Rightarrow$
$\exists c_1, c_2 \in \mathbb{C}\ (a_1 - c_1)^2 + (a_2 - c_2)^2 = (b_1 - c_1)^2 + (b_2 - c_2)^2 = (a_1 - b_1)^2 + (a_2 - b_2)^2.$

But the following property may not be true for some field K.

$\forall a_1, a_2, b_1, b_2 \in K\ (a_1 \neq b_1 \vee a_2 \neq b_2)\ \Rightarrow$
$\exists c_1, c_2 \in K\ (a_1 - c_1)^2 + (a_2 - c_2)^2 = (b_1 - c_1)^2 + (b_2 - c_2)^2 = (a_1 - b_1)^2 + (a_2 - b_2)^2$

K must be closed under any two dimensional algebraic extension,
that is $a \in K \Rightarrow \sqrt{a} \in K$.

Hence, the theorem belongs to metric geometry but not affine geometry.

From a viewpoint of automated theorem proving, we only need to deal with the following type of sentence:

$$\forall \bar{X} \in \mathbb{R}\ \phi_1(\bar{X}) \Rightarrow \phi_2(\bar{X}).$$

When it belongs to metric geometry, we can show the stronger sentence:

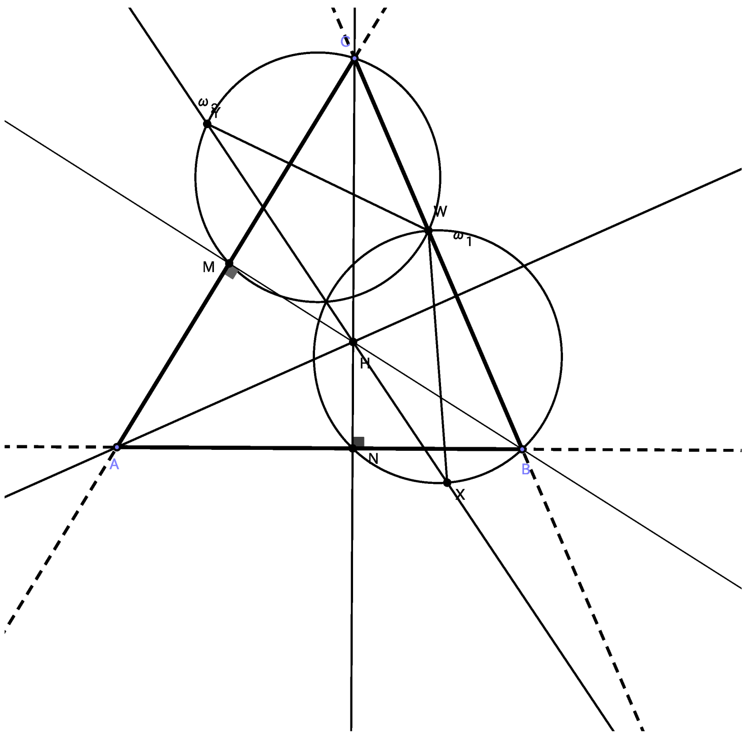
$$\forall \bar{X} \in \mathbb{C}\ \phi_1(\bar{X}) \Rightarrow \phi_2(\bar{X}).$$

It can be automatically proved by manipulation of underlying ideals. In case a theorem does not contain hidden non-degenerate assumptions, we can handle it by computation of a Gröbner basis for example. For a theorem of metric geometry with some hidden non-degenerate assumptions, we need complex QE for finding all hidden non-degenerate assumptions.

Problem(International Mathematical Olympiad 2013)

Let ABC be an acute-angled triangle with orthocentre H, and let W be a point on the side BC, lying strictly between B and C. The points M and N are the feet of the altitudes from B and C, respectively. Denote by ω_1 the circumcircle of BWN, and let X be the point on ω_1 such that WX is a diameter of ω_1. Analogously, denote by ω_2 the circumcircle of CWM, and let Y be the point on ω_2 such that WY is a diameter of ω_2. Prove that X, Y and H are collinear. Take the coordinates of the points A, B, C, M, X, Y by A$(0,0)$, B$(1,0)$, C(c_1, c_2), M(m_1, m_2), X(x_1, x_2), Y(y_1, y_2). We have the following.

1. An obvious non-degenerate assumption $c_2 \neq 0$ for the point C.
2. ABC is an acute-angled triangle $\Leftrightarrow 0 < c_1 < 1 \wedge (c_1 - 1/2)^2 + c_2^2 > 1/4$.
3. Since CN $\perp$ AB, the coordinate of N is $(c_1, 0)$.
4. Since H is on the line CN, its coordinate is (c_1, h_2) for some real number h_2.
5. Since W is on the line BC, its coordinate is $(1 + w(c_1 - 1), wc_2)$ for some real number w. Since W is strictly between B and C, we need $0 < w < 1$.
6. M is on the line AC $\Leftrightarrow m_1c_2 - m_2c_1 = 0$.
7. BH $\perp$ AC $\Leftrightarrow (c_1 - 1)c_1 + h_2c_2 = 0$.
8. BM $\perp$ AC $\Leftrightarrow$ H is on the line BM $\Leftrightarrow (m_1 - 1)c_1 + m_2c_2 = 0$.



9. WX is a diameter of $\omega_1 \Leftrightarrow$

$$((1+w(c_1-1))-x_1)^2+(wc_2-x_2)^2 = ((1+w(c_1-1))+x_1-2c_1)^2+(wc_2+x_2)^2$$
$$= ((1+w(c_1-1))+x_1-2)^2+(wc_2+x_2)^2.$$

10. WY is a diameter of $\omega_2 \Leftrightarrow$

$$((1+w(c_1-1))-y_1)^2+(wc_2-y_2)^2 = ((1+w(c_1-1))+y_1-2mc_1)^2+(wc_2+y_2-2mc_2)^2$$
$$= ((1+w(c_1-1))+y_1-2c_1)^2+(wc_2+y_2-2c_2)^2.$$

11. X, Y and H are collinear $\Leftrightarrow (y_1-c_1)(y_2-x_2)-(y_2-h_2)(y_1-x_1)=0$.

Let $F_1 = m_1c_2 - m_2c_1$, $F_2 = (c_1-1)c_1 + h_2c_2$, $F_3 = (m_1-1)c_1 + m_2c_2$,

$F_4 = ((1+w(c_1-1))-x_1)^2+(wc_2-x_2)^2 - (((1+w(c_1-1))+x_1-2c_1)^2+(wc_2+x_2)^2)$,

$F_5 = ((1+w(c_1-1))-x_1)^2+(wc_2-x_2)^2 - (((1+w(c_1-1))+x_1-2)^2+(wc_2+x_2)^2)$,

$F_6 = ((1+w(c_1-1))-y_1)^2+(wc_2-y_2)^2$
$\quad -(((1+w(c_1-1))+y_1-2mc_1)^2+(wc_2+y_2-2mc_2)^2)$,

$F_7 = ((1+w(c_1-1))-y_1)^2+(wc_2-y_2)^2$
$\quad -(((1+w(c_1-1))+y_1-2c_1)^2+(wc_2+y_2-2c_2)^2)$,

$P = (y_1-c_1)(y_2-x_2)-(y_2-h_2)(y_1-x_1)$.

The problem is nothing but proving the following sentence is true:

$\forall x_1, x_2, y_1, y_2, m_1, m_2, h_2, w, c_1, c_2 \in \mathbb{R}$
$c_2 \neq 0 \ \wedge \ 0 < c_1 < 1 \ \wedge \ (c_1-1/2)^2 + c_2^2 > 1/4 \ \wedge \ 0 < w < 1 \ \wedge$
$F_1 = 0 \ \wedge \ F_2 = 0 \ \wedge \ F_3 = 0 \ \wedge \ F_4 = 0 \ \wedge \ F_5 = 0 \ \wedge \ F_6 = 0 \ \wedge \ F_7 = 0$
$\quad \Rightarrow \quad P = 0.$

Unfortunately we can not handle it by any of existing real QE implementations such as [5, 4, 6, 7] except for the program of [8].

Note that we have the following obvious non-degenerate assumptions.

$c_2 \neq 0$ in order that the points A, B and C are not collinear.
$w \neq 0, 1$ in order that BWN and CWM have their circumcircle.

Using only these conditions, we can see the problem is actually a problem of metric geometry together with getting all hidden non-degenerate assumptions by applying complex QE to the following formula:

$$\forall x_1, x_2, y_1, y_2, m_1, m_2, h_2, w \in \mathbb{C}(w \neq 0 \wedge w \neq 1 \wedge F_1 = 0 \wedge F_2 = 0 \wedge F_3 = 0 \wedge F_4 = 0 \wedge \\ F_5 = 0 \wedge F_6 = 0 \wedge F_7 = 0 \Rightarrow P = 0).$$

The equivalent quantifier free formula is the following:

$$(c_1 = 1 \wedge c_2^2 + 1 = 0) \vee (c_1 = 0 \wedge c_2 = 0) \vee (c_1 - 1)((c_1 - 1/2)^2 + c_2^2 - 1/4) \neq 0.$$

The first formula $c_1 = 1 \wedge c_2^2 + 1 = 0$ is impossible for real values and the second formula $c_1 = 0 \wedge c_2 = 0$ is also impossible under the condition $c_2 \neq 0$. Hence, the following formula is true:

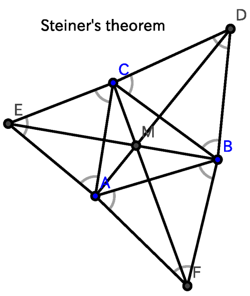
$$\forall x_1, x_2, y_1, y_2, m_1, m_2, h_2, w, c_1, c_2 \in \mathbb{R}(c_1 \neq 1 \wedge c_2 \neq 0 \wedge (c_1 - 1/2)^2 + c_2^2 \neq 1/4 \wedge \\ w \neq 0 \wedge w \neq 1 \wedge F_1 = 0 \wedge F_2 = 0 \wedge F_3 = 0 \wedge F_4 = 0 \wedge F_5 = 0 \wedge F_6 = 0 \wedge F_7 = 0 \\ \Rightarrow P = 0).$$

The condition $c_1 = 1$ implies N=B and the condition $(c_1 - 1/2)^2 + c_2^2 = 1/4$ implies M=C, both are degenerate cases. Note also that $c_1 = 1 \Leftrightarrow$ CB⊥BA and $(c_1 - 1/2)^2 + c_2^2 = 1/4 \Leftrightarrow$ AC⊥CB. Hence, necessary and sufficient conditions for the conclusion are ∠ABC$\neq \pi/2$, ∠ACB$\neq \pi/2$ and W≠B,W≠C.

4 Hilbert geometry

Consider the following theorem of Steiner.

Theorem 4 Steiner's Theorem
For an arbitrary triangle △ABC, let D, E and F be the points such that triangles △DBC, △ACE and △ABF are equilateral. Then the lines AD, BE and CF intersects at one point.



Let the coordinates of the points A,B,C,D,E,F,M be A$(0,0)$, B$(1,0)$, C(c_1,c_2), D(d_1,d_2), E(e_1,e_2), F$(\frac{1}{2},f_2)$, M$(m*d_1,m*d_2)$.

Note that we can assume $0<c_1<1$ and $0<c_2$ w.l.o. generality and the following relations hold.

AF=BF=AB $\Leftrightarrow f_2^2=\frac{3}{4}$
AC=AE=EC $\Leftrightarrow c_1^2+c_2^2=e_1^2+e_2^2=(e_1-c_1)^2+(e_2-c_2)^2$
BC=BD=DC $\Leftrightarrow (c_1-1)^2+c_2^2=(d_1-1)^2+d_2^2=(c_1-d_1)^2+(c_2-d_2)^2$
BE//BM $\Leftrightarrow (m*d_1-1)*e_2=m*d_2*(e_1-1)$
CF//MF $\Leftrightarrow (m*d_1-\frac{1}{2})*(f_2-c_2)=(m*d_2-f_2)*(\frac{1}{2}-c_1)$
D is on the upper side of the line CB $\Leftrightarrow d_2*(c_1-1)<c_2*(d_1-1)$
E is on the upper side of the line AC $\Leftrightarrow e_2*c_1>c_2*e_1$
F is on the lower side of the line AB $\Leftrightarrow f_2<0$
The theorem is translated to the following polynomial sentence.

$\forall c_1,c_2,d_1,d_2,e_1,e_2,f_2,m\in\mathbb{R}$

$0<c_1<1\ \wedge\ 0<c_2\ \wedge\ d_2*(c_1-1)<c_2*(d_1-1)\ \wedge\ e_2*c_1>c_2*e_1\ \wedge\ f_2<0$
$\wedge\ f_2^2=\frac{3}{4}\ \wedge\ c_1^2+c_2^2=e_1^2+e_2^2=(e_1-c_1)^2+(e_2-c_2)^2\ \wedge$
$(c_1-1)^2+c_2^2=(d_1-1)^2+d_2^2=(c_1-d_1)^2+(c_2-d_2)^2\ \wedge$
$(m*d_1-1)*e_2=m*d_2*(e_1-1)$

$\Rightarrow (m*d_1-\frac{1}{2})*(f_2-c_2)=(m*d_2-f_2)*(\frac{1}{2}-c_1)$

The theorem is translated to the following polynomial sentence.

$\forall c_1,c_2,d_1,d_2,e_1,e_2,f_2,m\in\mathbb{R}$

$0<c_1<1\ \wedge\ 0<c_2\ \wedge\ d_2*(c_1-1)<c_2*(d_1-1)\ \wedge\ e_2*c_1>c_2*e_1\ \wedge\ f_2<0$
$\wedge\ f_2^2=\frac{3}{4}\ \wedge\ c_1^2+c_2^2=e_1^2+e_2^2=(e_1-c_1)^2+(e_2-c_2)^2\ \wedge$

$(c_1 - 1)^2 + c_2^2 = (d_1 - 1)^2 + d_2^2 = (c_1 - d_1)^2 + (c_2 - d_2)^2 \wedge$
$(m * d_1 - 1) * e_2 = m * d_2 * (e_1 - 1)$

$\Rightarrow (m * d_1 - \frac{1}{2}) * (f_2 - c_2) = (m * d_2 - f_2) * (\frac{1}{2} - c_1)$

It can not be handled by most existing real QE implementation either except for the real QE programs of [8] and [5].

Note that we have an obvious non-degenerate condition $c_2 \neq 0$. If the following sentence holds, the theorem belongs to metric geometry.

$\forall c_1, c_2, d_1, d_2, e_1, e_2, f_2, m \in \mathbb{C}$

$c_2 \neq 0 \wedge f_2^2 = \frac{3}{4} \wedge c_1^2 + c_2^2 = e_1^2 + e_2^2 = (e_1 - c_1)^2 + (e_2 - c_2)^2 \wedge$
$(c_1 - 1)^2 + c_2^2 = (d_1 - 1)^2 + d_2^2 = (c_1 - d_1)^2 + (c_2 - d_2)^2 \wedge$
$(m * d_1 - 1) * e_2 = m * d_2 * (e_1 - 1)$

$\Rightarrow (m * d_1 - \frac{1}{2}) * (f_2 - c_2) = (m * d_2 - f_2) * (\frac{1}{2} - c_1)$

Unfortunately, we can check that it is false by computation of a Gröbner basis. Hence, the theorem does not belong to metric geometry.

We can check the theorem belongs to Hilbert geometry by manipulation of a suitable ideal as follows.

Let I be the following polynomial ideal.

$$I = \langle f_2^2 - \tfrac{3}{4},\ c_1^2 + c_2^2 - (e_1^2 + e_2^2),\ c_1^2 + c_2^2 - ((e_1 - c_1)^2 + (e_2 - c_2)^2),$$
$$(c_1 - 1)^2 + c_2^2 - ((d_1 - 1)^2 + d_2^2),\ (c_1 - 1)^2 + c_2^2 - ((c_1 - d_1)^2 + (c_2 - d_2)^2)\rangle$$

Primary decomposition of I contains the component.

$$\langle 4*f_2^2-3,\ c_1+2*f_2*c_2-2*e_1,\ 2*f_2*c_1-c_2+2*e_2,\ 2*f_2*c_1+c_2-2*d_2-2*f_2,\ c_1-2*f_2*c_2-2*d_1+1\rangle.$$

We can check the following sentence is true by computation of a Gröbner basis.

$\forall c_1, c_2, d_1, d_2, e_1, e_2, f_2, m \in \mathbb{C}$

$4 * f_2^2 - 3 = 0 \wedge c_1 + 2 * f_2 * c_2 - 2 * e_1 = 0 \wedge 2 * f_2 * c_1 - c_2 + 2 * e_2 = 0 \wedge 2 * f_2 * c_1 + c_2 - 2 * d_2 - 2 * f_2 =$
$0 \wedge c_1 - 2 * f_2 * c_2 - 2 * d_1 + 1 = 0 \wedge (m * d_1 - 1) * e_2 = m * d_2 * (e_1 - 1)$

$\Rightarrow (m * d_1 - \frac{1}{2}) * (f_2 - c_2) = (m * d_2 - f_2) * (\frac{1}{2} - c_1).$

The obtained primary component correspond to two cases that is the points D, E and F lei in outside or inside of the three lines BC, AC and AB simultaneously.

We can say such a theorem belongs to Hilbert geometry.

5 Tarski geometry

A theorem which does not belong to Hilbert geometry can not be handled by any of the above method. Intuitively, a theorem described by only inequalities is such a theorem. We need real QE for them.

6 Conclusion

We summarize the method of automated theorem proving of elementary geometry as follows.

1. Metric geometry with no hidden non-degenerate assumptions.

Simple ideal manipulations such as Gröbner bases computations suffice.

2. Metric geometry with some hidden non-degenerate assumptions.

Complex QE can handle it.

3. Hilbert geometry with no hidden non-degenerate assumptions.

Primary decomposition of an ideal can handle it.
(In most cases, factorizations are enough.)

4. Hilbert geometry with hidden non-degenerate assumptions.

Parametric decomposition of an ideal may handle it.

5. Tarski geometry.

We need real QE.

参 考 文 献

[1] Collins, G, E. : Quantifier elimination for real closed fields by cylindrical algebraic decomposition. Automata theory and formal languages (Second GI Conf., Kaiserslautern, 1975), pp. 134-183. Lecture Notes in Comput. Sci., Vol. 33, Springer, Berlin, 1975.

[2] Fukasaku, R.,Inoue, S. and Sato, Y. On QE Algorithms over Algebraically Closed Field based on Comprehensive Gröbner Systems. To appear in Mathematics in Computer Science.

[3] Fukasaku, R., Iwane, H. and Sato, Y. Real Quantifier Elimination by Computation of Comprehensive Gröbner Systems. Proceedings of International Symposium on Symbolic and Algebraic Computation, pp. 173-180, ACM, 2015.

[4] Mathematica Tutorial: tutorial/{ComplexPolynomialSystems,RealPolynomialSystems}

[5] The RegularChains Library. `http://www.regularchains.org/index.html`

[6] QEPCAD-Quantifier Elimination by Partial Cylindrical Algebraic Decomposition. `http://www.usna.edu/CS/qepcadweb/B/QEPCAD.html`

[7] Redlog: an integral part of the interactive computer algebra system Reduce. `http://www.redlog.eu/`

[8] SyNRAC: a software package for quantifier elimination. `http://jp.fujitsu.com/group/labs/en/techinfo/freeware/synrac/`

[9] Tarski, A. A Decision Method for Elementary Algebra and Geometry. Quantifier Elimination and Cylindrical Algebraic Decomposition, Texts & Monographs in Symbolic Computation, pp. 24-84, Springer, 1998.