On Applications of Technology to Understanding Hierarchies of Elementary Geometry

Yosuke Sato [1] *Ryoya Fukasaku* [2] *Katsusuke Nabeshima* [3]

[1] ysato@rs.kagu.tus.ac.jp [2] fukasaku@rs.tus.ac.jp
[3] nabeshima@tokushima-u.ac.jp

[1,2] Department of Applied Mathematics
Tokyo University of Science
1-3,Kagurazaka,Shinjukuku, Tokyo, Japan

[3] Graduate School of Technology, Industrial and Social Sciences
Tokushima University
2-1, Minamijosanjima, Tokushima, Japan

Abstract

Problems and theorems of elementary geometry are categorized roughly into four hierarchies, affine, metric, Hilbert and Tarski geometry. Difference between the latter three is especially hard to make out. In this paper, we give algorithmic descriptions for these hierarchies. Our descriptions together with sophisticated programs of computer algebra systems such as Gröbner basis computation, primary decomposition of a polynomial ideal and real quantifier elimination enable teachers to understand these hierarchies. They also could help teachers to make high quality problems of elementary geometry.

1 Introduction

Problems and theorems of elementary geometry are categorized roughly into four hierarchies, affine, metric, Hilbert and Tarski geometry. Affine geometry is what remains of Euclidean geometry when not using the metric notions of distance and angle. It is not difficult to check whether a given problem or theorem lies in this hierarchy. On the other hand, the difference between the latter three is very subtle and hard to make out. Though there exists a book which describes those hierarchies such as [1], it does not contain a complete algorithmic description for them and there are very few publications which contain thorough algorithmic treatment of those hierarchies. As a result, many mathematics teachers make problems of elementary geometry without recognizing them well. In fact, even in a high level competition such as International

Mathematical Olympiad, many problems containing unnecessary assumptions are given as is reported in [2].

In this paper, we give algorithmic descriptions for the three hierarchies in terms of computer algebra such as a Gröbner basis, primary decomposition of a polynomial ideal and real quantifier elimination. Using technology of the latest computer algebra systems which contain the implementations of these computations, we can decide the hierarchy of a given problem or a theorem of elementary geometry.

The paper is organized as follows. In section 2, we give a minimum description of the above-mentioned tools of computer algebra which is necessary to understand this paper. We deal with metric geometry in section 3, Hilbert geometry in section 4 and Tarski geometry in section 5 together with a typical computation example.

2 Preliminary

$\mathbb{Q}, \mathbb{R}$ and $\mathbb{C}$ denote the field of rational numbers, real numbers and complex numbers respectively, $\mathbb{N}$ denotes the set of natural numbers. For a capital letter such as X, $\bar{X}$ denotes some variables $X_1, \ldots, X_n$. $T(\bar{X})$ denotes a set of terms in $\bar{X}$. For an ideal $I \subset \mathbb{Q}[\bar{X}]$, $\mathbb{V}_{\mathbb{C}}(I)$ denotes its variety in $\mathbb{C}$.

2.1 Gröbner Basis

The following fundamental properties of Gröbner bases, found in most standard text books of Gröbner bases, play important roles in this paper.

Theorem 1 *Let I be an ideal in a polynomial ring $\mathbb{Q}[\bar{X}]$. For any admissible term order of $T(\bar{X})$, $\mathbb{V}_{\mathbb{C}}(I) = \emptyset$ if and only if the reduced Gröbner basis of I is equal to $\{1\}$.*

Corollary 2 *Let $f_1(\bar{X}), \ldots, f_l(\bar{X}), h(\bar{X}), g(\bar{X})$ be polynomials in $\mathbb{Q}[\bar{X}]$. For any admissible term order of $T(\bar{X}, Y)$, $\forall \bar{a} \in \mathbb{C}^n (f_1(\bar{a}) = 0 \wedge \cdots \wedge f_l(\bar{a}) = 0 \wedge h(\bar{a}) \neq 0 \Rightarrow g(\bar{a}) = 0)$ holds if and only if the reduced Gröbner basis of the ideal $\langle f_1, \ldots, f_l, hgY - 1\rangle$ in $\mathbb{Q}[\bar{X}, Y]$ is equal to $\{1\}$.*

Theorem 3 *For polynomials $f_1(\bar{X}), \ldots, f_l(\bar{X}), h(\bar{X}), g(\bar{X})$ in $\mathbb{Q}[\bar{X}]$, Let G be a Gröbner basis of the ideal $\langle f_1(\bar{X}), \ldots, f_l(\bar{X}), h(\bar{X})Y - 1\rangle$ in $\mathbb{Q}[\bar{X}, Y]$ w.r.t. an arbitrary admissible term order of $T(\bar{X}, Y)$. For any polynomial $g(\bar{X}) \in \mathbb{Q}[\bar{X}]$, the following relation holds:*

$$\forall \bar{a} \in \mathbb{C}^n \ (f_1(\bar{a}) = 0 \wedge \cdots \wedge f_l(\bar{a}) = 0 \wedge h(\bar{a}) \neq 0 \Rightarrow g(\bar{a}) = 0) \Leftrightarrow \exists s \in \mathbb{N} \ \overline{g(\bar{X})^s}^{G} = 0,$$

where $\overline{g(\bar{X})^s}^{G}$ denotes the remainder of the polynomial devision of $g(\bar{X})^s$ by G.

2.2 Primary Decomposition

A primary decomposition of a polynomial ideal in a multivariate polynomial ring corresponds to a factorization of a univariate polynomial. When the given ideal is not a radical ideal, we need to discuss some technical issues concerning isolated and embedded components. Since we need the decomposition of only radical ideals in this paper, we only deals with radical ideals.

Definition 4 *For an ideal I of $\mathbb{Q}[\bar{X}]$, its radical denoted $\sqrt{I}$ is an ideal $\{f \in \mathbb{Q}[\bar{X}] : \exists l \in \mathbb{N} \ f^l \in I\}$ of $\mathbb{Q}[\bar{X}]$. We say I is radical if $I = \sqrt{I}$.*

When I is an ideal in a univariate polynomial ring $\mathbb{Q}[X]$, $I = \langle f \rangle$ for some polynomial f. Let $f = f_1^{n_1} \cdots f_l^{n_l}$ where each f_i is irreducible in $\mathbb{Q}[X]$, then $\sqrt{I} = \langle f_1 \cdots f_l \rangle = \langle f_1 \rangle \cap \cdots \cap \langle f_l \rangle$.

Theorem 5 *The radical of an arbitrary ideal I of $\mathbb{Q}[\bar{X}]$ can be represented as an intersection of prime ideals, that is $\sqrt{I} = I_1 \cap \cdots \cap I_l$ with prime ideals $I_1, \ldots, I_l$ of $\mathbb{Q}[\bar{X}]$ such that $\sqrt{I} \neq I_1 \cap \cdots \cap I_{i-1} \cap I_{i+1} \cap \cdots \cap I_l$ for any i. Furthermore, $I_1, \ldots, I_l$ are determined unique.*

Definition 6 *The representation $\sqrt{I} = I_1 \cap \cdots \cap I_l$ in the above theorem is called the the primary decomposition of $\sqrt{I}$.*

Given an arbitrary ideal $I = \langle f_1, \ldots, f_s \rangle$ of $\mathbb{Q}[\bar{X}]$, we can always compute the primary decomposition of $\sqrt{I}$. The primary decomposition $\sqrt{I} = I_1 \cap \cdots \cap I_l$ gives an irreducible decomposition $V_{\mathbb{C}}(I) = V_{\mathbb{C}}(I_1) \cup \cdots \cup V_{\mathbb{C}}(I_l)$, where each variety $V_{\mathbb{C}}(I_i)$ is irreducible, that is $V_{\mathbb{C}}(I_i)$ cannot be represented as a union of two varieties, such that each of them is smaller than $V_{\mathbb{C}}(I_i)$.

2.3 Real Quantifier Elimination

Quantifier elimination(QE) means the following procedure:

> *For a given first order formula, compute an equivalent quantifier free formula by eliminating all quantifiers.*

We can handle QE in many types of domains. In this paper, however, we deal with QE only in the domain of real numbers, where any first order formula consists from atomic formulas of polynomial equations and inequalities with real coefficients. The following examples are real QE computations using Mathematica's real QE implementations **Resolve** ([4]).

```
In[1]:= F[x_]:= x^3 - x + 1;
In[2]:= Resolve[Exists[epsilon, epsilon > 0 &&
        ForAll[x1, Implies[-epsilon < x - x1 < 0 || 0 < x - x1 < epsilon,
        F[x] > F[x1]]] && M == F[x]], {x, M}, Reals]
Out[2]:= x == -(1/Sqrt[3]) && M == 1 - x + x^3
```

3 Metric Geometry

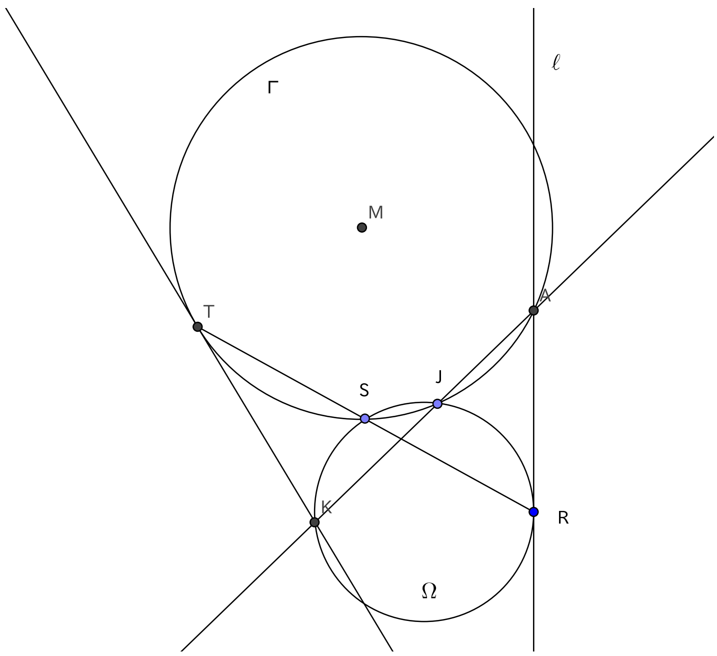
A problem or a theorem of elementary geometry in the hierarchy of metric geometry is roughly speaking a problem or a theorem which does not need a description of inequality.

Algorithmically we can say that a problem or a theorem of metric geometry is a problem which can be automatically solved using computation of a Gröbner basis.

The following problem does not seem to be in this hierarchy since it contains the descriptions "the shorter arc" and "is closer to". It will turn out that the problem actually belongs to metric geometry. The conclusion also holds even when J is on the longer arc R or A is not closer to R.

Problem 4 (International Mathematical Olympiad 2017)

Let R and S be different points on a circle Ω such that RS is not a diameter. Let ℓ be the tangent line to Ω at R. Point T is such that S is the midpoint of the line segment RT . Point J is chosen on the shorter arc RS of Ω so that the circumcircle Γ of triangle JST intersects ℓ at two distinct points. Let A be the common point of Γ and ℓ that is closer to R. Line AJ meets Ω again at K. Prove that the line KT is tangent to Γ.



We can assume that Ω is a unit circle with its center $(0,0)$, the coordinate of R is $\mathrm{R}(1,0)$ and ℓ is the line perpendicular to x-axis at R w.o.l. of generality. Let the coordinates of S, J, A be $\mathrm{S}(s_1,s_2)$, $\mathrm{J}(j_1,j_2)$, $\mathrm{A}(1,a_2)$. Hence the coordinates of T and K are $\mathrm{T}(2s_1-1,2s_2)$ and $\mathrm{K}(k(j_1-1)+1,k(j_2-a_2)+a_2)$ for some real number k. Let $\mathrm{M}(m_1,m_2)$ be the center of Γ. We have the following relations.

S is on $\Omega \Leftrightarrow s_1^2+s_2^2=1$, J is on $\Omega \Leftrightarrow j_1^2+j_2^2=1$, K is on $\Omega \Leftrightarrow (k(j_1-1)+1)^2+(k(j_2-a_2)+a_2)^2=1$, Γ is the circumcircle of triangle JST $\Leftrightarrow (m_1-s_1)^2+(m_2-s_2)^2=(m_1-j_1)^2+(m_2-j_2)^2=(m_1-(2s_1-1))^2+(m_2-2s_2)^2$, A is on $\Gamma \Leftrightarrow (m_1-s_1)^2+(m_2-s_2)^2=(m_1-1)^2+(m_2-a)^2$, $\mathrm{J}\neq\mathrm{R}\Leftrightarrow j_1\neq 1$, $\mathrm{S}\neq\mathrm{R}\Leftrightarrow s_1\neq 1$, $\mathrm{K}\neq\mathrm{J}\Leftrightarrow k\neq 1$, RS is not a diameter $\Leftrightarrow s_1\neq -1$.
We can also assume $s_2>0$ w.l.o. generality which implies J is on the shorter arc RS $\Leftrightarrow j_1>s_1$.

KT is tangent to $\Gamma \Leftrightarrow \mathrm{KT}\perp\mathrm{TM}\Leftrightarrow ((k(j_1-1)+1)-(2s_1-1))(m_1-(2s_1-1))+(k(j_2-a_2)+a_2-2s_2)(m_2-2s_2)=0$.

Hence the theorem is translated to the following first order sentence.

$\forall s_1,s_2,j_1,j_2,m_1,m_2,k,a_2\in\mathbb{R}$
$s_1^2+s_2^2=1 \wedge j_1^2+j_2^2=1 \wedge (k(j_1-1)+1)^2+(k(j_2-a_2)+a2)^2=1 \wedge (m_1-s_1)^2+(m_2-s_2)^2=(m_1-j_1)^2+(m_2-j_2)^2=(m_1-(2s_1-1))^2+(m_2-2s_2)^2=(m_1-1)^2+(m_2-a)^2 \wedge j_1\neq 1 \wedge s_1\neq 1 \wedge s_1\neq -1 \wedge k\neq 1 \wedge s_2>0 \wedge j_1>s_1$
$\Rightarrow ((k(j_1-1)+1)-(2s_1-1))(m_1-(2s_1-1))+(k(j_2-a_2)+a_2-2s_2)(m_2-2s_2)=0$

Actually, we can prove that the following much stronger sentence holds.

$\forall s_1,s_2,j_1,j_2,m_1,m_2,k,a_2\in\mathbb{C}$
$s_1^2+s_2^2=1 \wedge j_1^2+j_2^2=1 \wedge (k(j_1-1)+1)^2+(k(j_2-a_2)+a_2)^2=1 \wedge (m_1-s_1)^2+(m_2-s_2)^2=(m_1-j_1)^2+(m_2-j_2)^2=(m_1-(2s_1-1))^2+(m_2-2s_2)^2=(m_1-1)^2+(m_2-a)^2 \wedge j_1\neq 1 \wedge s_1\neq 1 \wedge s_1\neq -1 \wedge k\neq 1 \wedge j_1\neq s_1$
$\Rightarrow ((k(j_1-1)+1)-(2s_1-1))(m_1-(2s_1-1))+(k(j_2-a_2)+a_2-2s_2)(m_2-2s_2)=0$

There are two ways to check the above sentence holds. One is the way using **Corollary 2**. What we have to do is the computation of the reduced Gröbner basis of the following ideal $\langle f_1, f_2, f_3, f_4, f_5, f_6, hgy - 1\rangle$ in $\mathbb{Q}[s_1, s_2, j_1, j_2, m_1, m_2, k, a_2, y]$. Where, $f_1 = s_1^2 + s_2^2 - 1$, $f_2 = j_1^2 + j_2^2 - 1$,$f_3 = (k(j_1 - 1) + 1)^2 + (k(j_2 - a_2) + a_2)^2 - 1$, $f_4 = (m_1 - s_1)^2 + (m_2 - s_2)^2 - ((m_1 - j_1)^2 + (m_2 - j_2)^2)$, $f_5 = (m_1 - s_1)^2 + (m_2 - s_2)^2 - ((m_1 - (2s_1 - 1))^2 + (m_2 - 2s_2)^2)$, $f_6 = (m_1 - s_1)^2 + (m_2 - s_2)^2 - ((m_1 - 1)^2 + (m_2 - a)^2)$, $h = (j_1 - 1)(s_1 - 1)(s_1 + 1)(k - 1)(j_1 - s_1)$ and $g = ((k(j_1 - 1) + 1) - (2s_1 - 1))(m_1 - (2s_1 - 1)) + (k(j_2 - a_2) + a_2 - 2s_2)(m_2 - 2s_2)$.

The following picture is the computation of its reduced Gröbner basis w.r.t. lexicographic order such that $s_1 > s_2 > j_1 > j_2 > m_1 > m_2 > k > a_2 > y$ using the Gröbner basis computation program `GroebnerBasis` of Mathematica. The program produces $\{1\}$ as is desired.

```
In[1]:= f1:=s1^2+s2^2-1;f2:=j1^2+j2^2-1;
      f3:=(k(j1-1)+1)^2+(k(j2-a2)+a2)^2-1;
      f4:=(m1-s1)^2+(m2-s2)^2-((m1-j1)^2+(m2-j2)^2);
      f5:=(m1-s1)^2+(m2-s2)^2-((m1-(2*s1-1))^2+(m2-2*s2)^2);
      f6:=(m1-s1)^2+(m2-s2)^2-((m1-1)^2+(m2-a2)^2);
      h:=(s1-1)*(s1+1)*(j1-1)*(j1-s1)*(k-1);
      g:=((k(j1-1)+1)-(2*s1-1))*(m1-(2*s1-1))+(k(j2-a2)+a2-2*s2)*(m2-2*s2);
In[9]:= GroebnerBasis[{f1,f2,f3,f4,f5,f6,h*g*y-1},{s1,s2,j1,j2,m1,m2,k,a2,y}]
Out[9]= {1}
```

The another way is by **Theorem 3**. The following picture is also by Mathematica. It produces $\overline{g}^G = 0$ for the reduced Gröbner basis G of the ideal $\langle f_1, f_2, f_3, f_4, f_5, f_6, hy - 1\rangle$ w.r.t. degree reverse lexicographic order such that $s_1 > s_2 > j_1 > j_2 > m_1 > m_2 > k > a_2 > y$ as is desired.

```
In[10]:= G:=GroebnerBasis[{f1,f2,f3,f4,f5,f6,h*y-1},
 {s1,s2,j1,j2,m1,m2,k,a2,y},MonomialOrder->DegreeReverseLexicographic];
In[11]:= Last[PolynomialReduce[g,G,{s1,s2,j1,j2,m1,m2,k,a2,y},
                               MonomialOrder->DegreeReverseLexicographic]]
Out[11]= 0
```

4 Hilbert Geometry

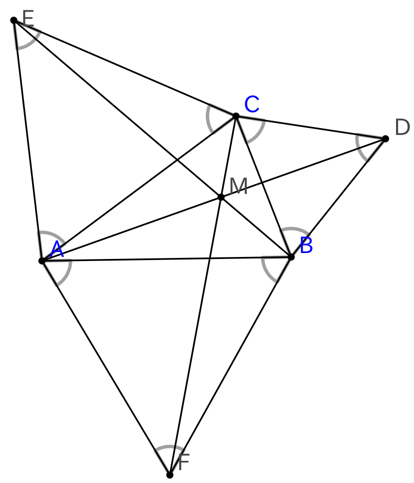
A problem or a theorem of elementary geometry in the hierarchy of Hilbert geometry is roughly speaking a problem or a theorem which needs descriptions of inequality only in the assumption but not in the conclusion.

Algorithmically we can say that a problem or a theorem of Hilbert geometry is a problem or a theorem which cannot be automatically solved by only computation of a Gröbner basis, but can be solved with computation of primary decomposition of a radical ideal.

Consider the following theorem of Steiner.

Steiner's Theorem

For an arbitrary triangle ABC, let D, E and F be the points lying in its outside 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 be $A(0,0)$, $B(1,0)$ w.l.o. generality and C,D,E,F,M be $C(c_1,c_2)$, $D(d_1,d_2)$, $E(e_1,e_2)$, $F(\frac{1}{2},f_2)$, $M(m\,d_1,m\,d_2)$. We can assume $0<c_1<1$ and $0<c_2$ w.o.l. of generality since at least two angles are acute. Then 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 $\Leftrightarrow f_2<0$.

Hence the theorem is translated to the following first order sentence.

$$\forall c_1,c_2,d_1,d_2,e_1,e_2,f_2,m\in\mathbb{R}$$
$$0<c_1<1\ \wedge\ 0<c_2\ \wedge\ d_2(c_1-1)<c_2(d_1-1)\ \wedge\ e_2\,c_1>c_2\,e_1\ \wedge\ f_2<0\ \wedge\ f_2^2=\tfrac{3}{4}\ \wedge$$
$$c_1^2+c_2^2=e_1^2+e_2^2=(e_1-c_1)^2+(e_2-c_2)^2\ \wedge\ (c_1-1)^2+c_2^2=(d_1-1)^2+d_2^2=(c_1-d_1)^2+(c_2-d_2)^2\ \wedge$$
$$(m\,d_1-1)e_2=m\,d_2(e_1-1)$$
$$\Rightarrow (m\,d_1-\tfrac{1}{2})(f_2-c_2)=(md_2-f_2)(\tfrac{1}{2}-c_1)$$

If the following sentence holds, the theorem belongs to metric geometry.

$$\forall c_1,c_2,d_1,d_2,e_1,e_2,f_2,m\in\mathbb{C}$$
$$c_1\neq 0\ \wedge\ c_1\neq 1\ \wedge\ c_2\neq 0\ \wedge\ d_2(c_1-1)\neq c_2(d_1-1)\ \wedge\ e_2\,c_1\neq c_2\,e_1\ \wedge\ f_2^2=\tfrac{3}{4}\ \wedge$$
$$c_1^2+c_2^2=e_1^2+e_2^2=(e_1-c_1)^2+(e_2-c_2)^2\ \wedge(c_1-1)^2+c_2^2=(d_1-1)^2+d_2^2=(c_1-d_1)^2+(c_2-d_2)^2\ \wedge$$
$$(m\,d_1-1)e_2=m\,d_2(e_1-1)$$
$$\Rightarrow (m\,d_1-\tfrac{1}{2})(f_2-c_2)=(m\,d_2-f_2)(\tfrac{1}{2}-c_1)$$

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 that the theorem belongs to Hilbert geometry by manipulation of a suitable ideal as follows. Let I be the following polynomial ideal generated by the polynomials which appear in the equations of the above sentence.

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

Unfortunately most computer algebra systems including Mathematica do not have a primary decomposition program. We use the primary decomposition program `primedec` of Risa/Asir ([3]) for the computation of the primary decomposition of $\sqrt{I}$, which is one of the fastest implementations we can use for a primary decomposition of a polynomial ideal.

```
[1905] primedec([f2^2-3/4,c1^2+c2^2-(e1^2+e2^2),
c1^2+c2^2-((e1-c1)^2+(e2-c2)^2),(c1-1)^2+c2^2-((d1-1)^2+d2^2),
(c1-1)^2+c2^2-((c1-d1)^2+(c2-d2)^2)],[d1,d2,e2,e1,c1,c2,f2]);
[
[2*c2*f2-2*e1+c1,2*c1*f2+2*e2-c2,(2*c1-2)*f2-c2+2*d2,2*c2*f2+c1-2*d1+1,
 4*f2^2-3],
[2*c2*f2+2*e1-c1,2*c1*f2-2*e2+c2,(2*c1-2)*f2+c2-2*d2,2*c2*f2-c1+2*d1-1,
 4*f2^2-3],
[2*c2*f2-2*e1+c1,2*c1*f2+2*e2-c2,(2*c1-2)*f2+c2-2*d2,2*c2*f2-c1+2*d1-1,
 4*f2^2-3],
[2*c2*f2+2*e1-c1,2*c1*f2-2*e2+c2,(2*c1-2)*f2-c2+2*d2,2*c2*f2+c1-2*d1+1,
 4*f2^2-3],
[2*c1-1,2*c2*e1-e2,2*d2*c2-d1+1,4*f2^2-3,4*c2^2+1],
[4*f2^2-3,(2*c1-2)*f2+c2-2*d2,2*c2*f2-c1+2*d1-1,c1^2+c2^2,c1*e1+c2*e2,
c2*e1-c1*e2,e1^2+e2^2],
[4*f2^2-3,(2*c1-2)*f2-c2+2*d2,2*c2*f2+c1-2*d1+1,c1^2+c2^2,c1*e1+c2*e2,
 c2*e1-c1*e2,e1^2+e2^2],
[4*f2^2-3,2*c2*f2-2*e1+c1,2*c1*f2+2*e2-c2,c1^2-2*c1+c2^2+1,
 d2*c1+(-d1+1)*c2-d2,(d1-1)*c1+d2*c2-d1+1,d1^2-2*d1+d2^2+1],
[4*f2^2-3,2*c2*f2+2*e1-c1,2*c1*f2-2*e2+c2,c1^2-2*c1+c2^2+1,
 d2*c1+(-d1+1)*c2-d2,(d1-1)*c1+d2*c2-d1+1,d1^2-2*d1+d2^2+1]]
```

The obtained decomposition contains 9 components. Among them, a valid component is only the third one $\langle 2c_2f_2-2e_1+c_1, 2c_1f_2+2e_2-c_2, (2c_1-2)f_2+c_2-2d_2, 2c_2f_2-c_1+2d_1-1, 4f_2^2-3\rangle$. That is the following sentence is true.

$\forall c_1, c_2, d_1, d_2, e_1, e_2, f_2, m \in \mathbb{C}$
$2c_2f_2-2e_1+c_1 = 0 \wedge 2c_1f_2+2e_2-c_2 = 0 \wedge (2c_1-2)f_2+c_2-2d_2 = 0 \wedge 2c_2f_2-c_1+2d_1-1 = 0 \wedge 4f_2^2-3 = 0 \wedge (m\,d_1-1)e_2 = m\,d_2(e_1-1)$
$\Rightarrow (m\ d_1 - \frac{1}{2})(f_2-c_2) = (m\ d_2 - f_2)(\frac{1}{2}-c_1)$.

We can also check it by suitable Gröbner basis computation as is described in the previous section. The following picture is its computation by Mathematica.

```
In[1]:= GroebnerBasis[{2*c2*f2-2*e1+c1,2*c1*f2+2*e2-c2,(2*c1-2)*f2+c2-2*d2,
 2*c2*f2-c1+2*d1-1,4*f2^2-3,(m*d1-1)*e2-m*d2*(e1-1),
 ((m*d1-1/2)(f2-c2)-(m*d2-f2)(1/2-c1))*y-1}, {d1,d2,e2,e1,c1,c2,f2,m,y}]
Out[1]= {1}
```

Note that the obtained primary component correspond to two cases that is the points D, E and F lie in the outside or inside of the triangle ABC simultaneously. It also can be automatically checked by real QE computation. The following picture is the computation of Mathematica's real QE program `Resolve`.

```
In[1]:= Resolve[ForAll[{d1, d2, e2, e1, c1, c2, f2},
  f2 < 0 && c2 > 0 && 1 > c1 > 0&& f2^2-3/4==0,
```

```
  Implies[ c1 + 2*f2*c2 - 2*e1 == 0 && 2*f2*c1 - c2 + 2*e2 == 0 &&
   2*f2*c1 + c2 - 2*d2 - 2*f2 == 0 && c1 - 2*f2*c2 - 2*d1 + 1 == 0,
  d2 (c1 - 1) < c2 (d1 - 1) && e2 c1 > c2 e1]], Reals]
Out[1]= True
In[2]:= Resolve[ForAll[{d1, d2, e2, e1, c1, c2, f2},
  f2 > 0 && c2 > 0 && 1 > c1 > 0&& f2^2-3/4==0,
  Implies[ c1 + 2*f2*c2 - 2*e1 == 0 && 2*f2*c1 - c2 + 2*e2 == 0 &&
   2*f2*c1 + c2 - 2*d2 - 2*f2 == 0 && c1 - 2*f2*c2 - 2*d1 + 1 == 0,
  d2 (c1 - 1) > c2 (d1 - 1) && e2 c1 < c2 e1]], Reals]
Out[2]= True
```

Note that each of the first 4 components also contains 2 different cases of the position of the points D, E, F. For example the first component contains two cases such that F is outside, D is inside, E is outside of the triangle or F is inside, D is outside, E is inside of the triangle. We can also check it by real QE computation as above. Note also that the other 5 components contains conditions which are not satisfiable by real numbers, which can also be checked by real QE computation.

We can give a more precise algorithmic description of Hilbert geometry as follows.

Let $f_1 = 0, \dots, f_l = 0$ be all equations and $h_1 \neq 0, \dots, h_m \neq 0$ be all dis-equations contained in the assumption of a theorem, let $g = 0$ be the conclusion of a theorem. The theorem belongs to Hilbert geometry, if $\forall \bar{c} \in V_{\mathbb{C}}(I_i)\, g(\bar{c}) = 0$ holds on some component I_i of the ideal $\langle f_1, \dots, f_l, h_1 h_2 \cdots h_m\, g\, y - 1\rangle$.

Of course we have to check that any $\bar{c} \in V_{\mathbb{C}}(I_i)$ satisfies all inequalities contained in the assumption of the theorem. We need a real QE computation for it, but such a computation is not very heavy in general as the above example.

5 Tarski Geometry

A problem or a theorem of elementary geometry in the hierarchy of Tarski geometry is roughly speaking a problem or a theorem which needs descriptions of inequality in the conclusion.

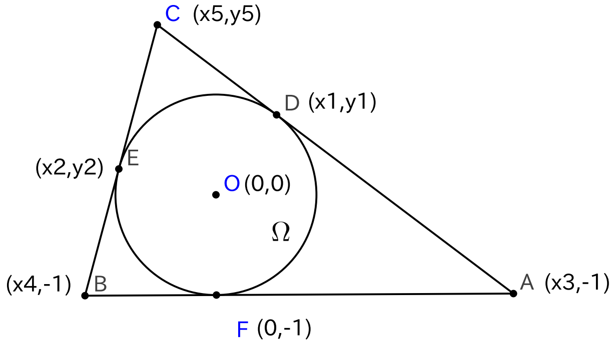
Algorithmically we can say that a problem or a theorem of Tarski geometry is a problem or a theorem which cannot be automatically solved by the method described in the previous sections but needs computation of real QE.

Consider the following problem of elementary geometry.

A problem given in an entrance examination of some Japanese university 2018

For a unit circle Ω, consider all possible triangles whose inscribed circle is Ω.
(1) Compute the possible range of the area of such triangles.
(2) What is the shape of a triangle which has the minimum area ?

Let the center of the unit circle Ω be the origin $\mathrm{O}(0,0)$. We can assume that two points of the triangle are $\mathrm{A}(x_3, -1)$ and $\mathrm{B}(x_4, -1)$ with $x_3 > 0 > x_4$ and the tangent point of Ω and AB is $\mathrm{F}(0, -1)$ w.o.l. of generality. Let the third point of the triangle be $\mathrm{C}(x_5, y_5)$ and the tangent point of Ω and CA be $\mathrm{D}(x_1, y_1)$ and the other tangent point by CB be $\mathrm{E}(x_2, y_2)$. We can assume that $y_1, y_2 > 0$ and $x_1 > 0 > x_2$.



Since $x_1 > 0 > x_2$ implies $x_3 > 0 > x_4$ and $y_1, y_2 > 0$ implies $y_5 > 0$, we have the following conditions.

OE⊥CE ⇔ $x_2(x_5 - x_2) + y_2(y_5 - y_2) = 0$, OE⊥BE ⇔ $x_2(x_2 - x_4) + y_2(y_2 + 1) = 0$, OD⊥CD ⇔ $x_1(x_5 - x_1) + y_1(y_5 - y_1) = 0$, OD⊥AD ⇔ $x_1(x_1 - x_3) + y_1(y_1 + 1) = 0$.

Using the variable s to represent the area of the triangle ABC, a necessary and sufficient condition for s can be represented by the following first order formula:

$\exists x_1, x_2, y_1, y_2, x_3, x_4, x_5, y_5$
$x_1 > 0 > x_2 \wedge y_1 > 0 \wedge y_2 > 0 \wedge x_2(x_5 - x_2) + y_2(y_5 - y_2) = 0 \wedge x_2(x_2 - x_4) + y_2(y_2 + 1) = 0 \wedge x_1(x_5 - x_1) + y_1(y_5 - y_1) = 0 \wedge x_1(x_1 - x_3) + y_1(y_1 + 1) = 0 \wedge 2s = (x_3 - x_4)(y_5 + 1)$.

The following picture is a computation of the real QE program **Resolve** of Mathematica, which automatically produces the solution $s \geq 3\sqrt{3}$ of (1).

```
In[1]:= Resolve[Exists[{x1,x2,y1,y2,x3,x4,x5,y5},x1>0>x2&&y1>0&&y2>0&&
 x2*(x5-x2)+y2*(y5-y2)==0&&x2*(x2-x4)+y2*(y2+1)==0&&x1*(x5-x1)+y1*(y5-y1)==0
 &&x1*(x1-x3)+y1*(y1+1)==0
 &&x1^2+y1^2==1&&x2^2+y2^2==1&&2*s==(x3-x4)*(y5+1)],
 Reals]
Out[1]= s >= 3 Sqrt[3]
```

we can also compute the solution of (2) by real QE as follows.

```
In[2]:= Resolve[Exists[{x3,x4,x5},Resolve[Exists[{x1,x2,y1,y2},
 x1>0>x2&&y1>0&&y2>0&&x2*(x5-x2)+y2*(y5-y2)==0&&x2*(x2-x4)+y2*(y2+1)==0&&
 x1*(x5-x1)+y1*(y5-y1)==0&&
 x1*(x1-x3)+y1*(y1+1)==0&&x1^2+y1^2==1&&x2^2+y2^2==1
 &&108==(x3-x4)^2*(y5+1)^2],Reals]],Reals]
Out[2]= y5 == 2
In[3]:= Resolve[Exists[{x3,x4,x1,x2,y1,y2,y5},
 x1>0>x2&&y1>0&&y2>0&&y5==2&&x2*(x5-x2)+y2*(y5-y2)==0&&
 x2*(x2-x4)+y2*(y2+1)==0&&x1*(x5-x1)+y1*(y5-y1)==0&&x1*(x1-x3)+y1*(y1+1)==0
 &&x1^2+y1^2==1&&x2^2+y2^2==1&&108==(x3-x4)^2*(y5+1)^2],Reals]
```

```
Out[3]= x5 == 0
In[4]:= Resolve[Exists[{x1,x2,y1,y2,y5,x5},
 x1>0>x2&&y1>0&&y2>0&&y5==2&&x5==0&&x2*(x5-x2)+y2*(y5-y2)==0&&
 x2*(x2-x4)+y2*(y2+1)==0&&x1*(x5-x1)+y1*(y5-y1)==0&&x1*(x1-x3)+y1*(y1+1)==0
 &&x1^2+y1^2==1&&x2^2+y2^2==1&&108==(x3-x4)^2*(y5+1)^2],Reals]
Out[4]= -3 + x4^2 == 0 && x3 + x4 == 0 && x4/2 < 0
```

From the above output, we know that the triangle has the minimum area when $x_5 = 0, y_5 = 2, x_3 = \sqrt{3}$ and $x_4 = -\sqrt{3}$ that is the triangle is a equilateral.

6 Conclusion and Remarks

A problem of a lower level hierarchy also belongs to a higher level hierarchy. Hence, any problem in affine, metric or Hilbert geometry can be solved by computation of real QE. However, computation of real QE is much heavier than Gröbner basis computation in general. The problems of metric and Hilbert geometry we treated in section 3,4 can not be handled by any of the existing real QE implementations. Real QE program can handle only easy part of the problem obtained by the computation of primary decomposition. Since real QE computation is a very heavy computation, there are many problems which can be handled theoretically but not in realistic computation time. The first real QE computation presented in section 5 needs more than half a minute with a standard laptop computer. We also use some technique in the next computation. We divide the QE computation into two QE computations, if we simply use `Resolve[Exists[x1,x2,y1,y2,x3,x4,x5],...]` the computation does not terminate within one hour.

We should mention that the program `primedec` of Risa/Asir we use in this paper is now a sort of legacy program, Risa/Asir has much faster program, nevertheless it satisfactorily works even for our rather non-trivial example.

References

[1] Chou, SC. Mechanical Geometry Theorem Proving. Mathematics and Its Applications, Springer, 1988.

[2] Sato, Y. and Fukasaku, R. Detecting unnecessary assumptions of elementary geometry problems by CAS. Proceedings of the 20th Asian Technology Conference in Mathematics, pp. 316-325, 2015.

[3] Noro, M. et al.: Risa/Asir — A computer algebra system for polynomial computations. http://www.math.kobe-u.ac.jp/Asir/asir.html (2018).

[4] Mathematica Tutorial: tutorial/RealPolynomialSystems

[5] 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.