Geometric theorem proving

Ulrik Buchholtz

March 3, 2010

Outline

Defining geometry

There are two approaches to geometry:

Algebraic approach

Start with a field k, define geometric objects and relations in k^n or $\mathrm{k}^n/\mathrm{k}^\times$.

Axiomatic geometric approach

Define a geometry as a formal system in first-order logic.

Affine geometry

Two sorts: points and lines. One relation: $p \in l$ (The point p is on the line l, or alternatively, l passes through p.)
Affine geometry (including the axiom of infinity) models exactly the structures $\Omega_K \equiv (K^2, L_K)$, where K is any field of characteristic zero,

$$L_K = \{ (a, b, c) \in K^3 \mid a \neq 0 \vee b \neq 0 \} / \sim,$$

and $(a, b, c) \sim (a', b', c')$ iff there is a $k \in K$ such that

$$a' = \lambda a \quad \wedge \quad b' = \lambda b \quad \wedge \quad c' = \lambda c.$$

Metric geometry

Metric geometry adds two new relations, perpendicularity of lines, $\mathrm{l} \perp \mathrm{m}$, and congruence of segments, $\mathrm{AB} = \mathrm{CD}$, together with corresponding axioms.

Definition

A *Hilbert field* is a field K, of characteristic zero, such that every sum of two squares has a square root.

Theorem

The models of Metric geometry correspond to structures Ω_{K} *for Hilbert fields* K.

Hilbert geometry

Hilbert geometry adds the betweenness relations for three points, $\mathrm{B}(\mathrm{A}, \mathrm{B}, \mathrm{C})$, to mean that A, B, and C are distinct points on the same line with B lying between A and C.

Theorem

The models of Hilbert geometry correspond to structures Ω_{K} for ordered Hilbert fields K.

Note

This concerns a first-order version of Hilbert's axioms (according to Chou). Hilbert's original axioms are second-order, and include the Archimedean property and line completeness.

Tarski geometry

Tarski's axioms are first-order, and similar to the ones for Hilbert geometry, but narrow the range of possible fields.

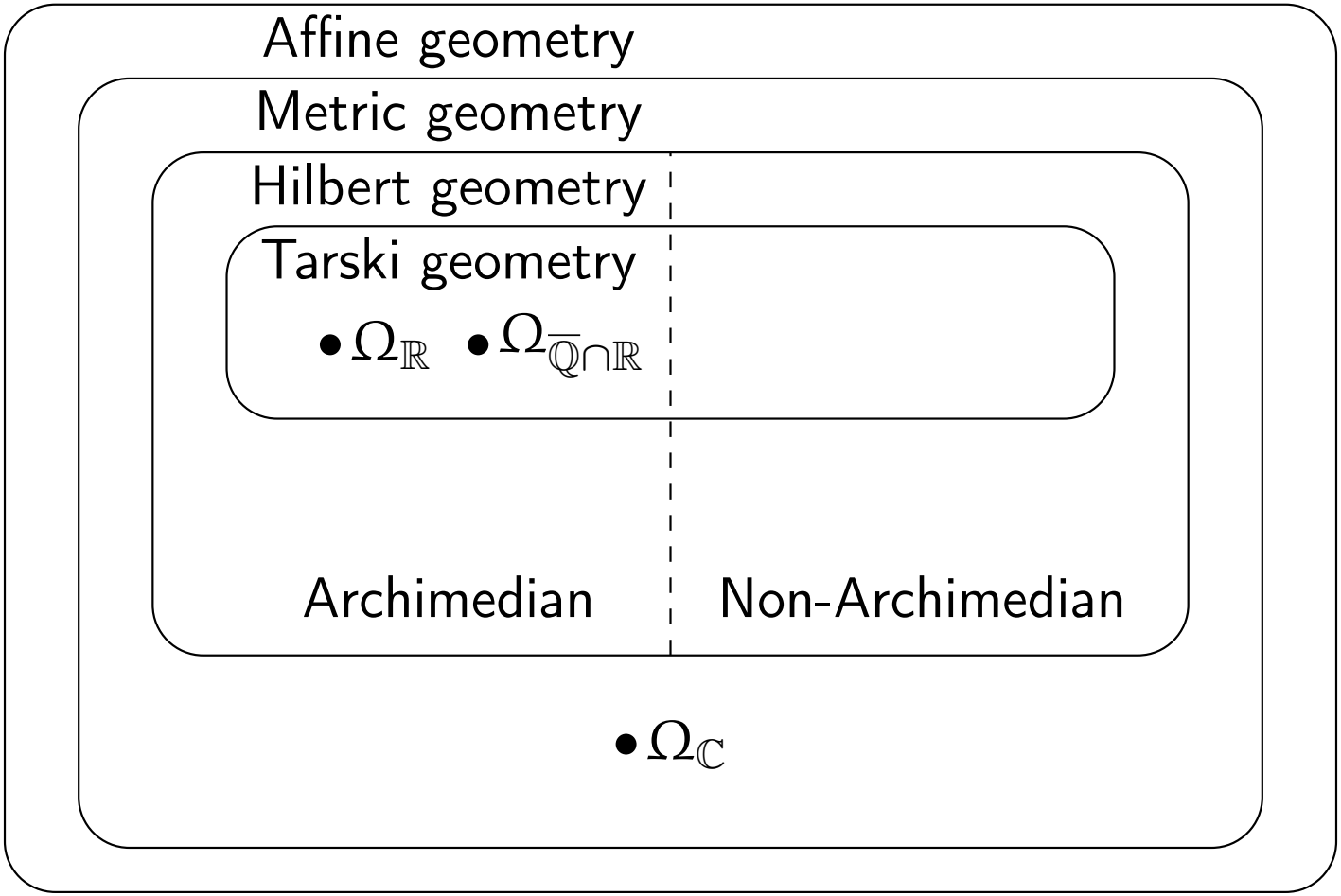
Definition

A *real closed field* is a field K that is elementarily equivalent to $\mathbb{R}$. Equivalently, it is an ordered field where positive elements have square roots and odd-degree polynomials have roots.

Theorem

The models of Tarski geometry correspond to structures Ω_{K} *for real closed fields* K.

Geometries and models

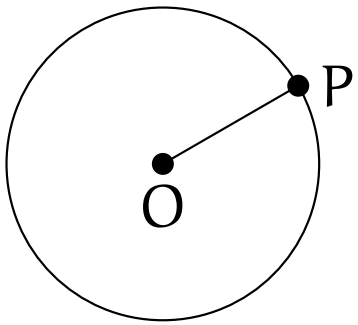


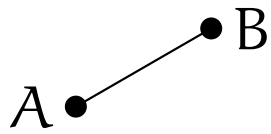
Circles

Circles can be defined in metric geometry using congruence:

Definition

A *circle* is a triple of points (O, A, B) where O is the center and the segment AB gives the radius. Two circles are *congruent* if they have the same center and congruent radii. A point P lies on the circle (O, A, B) iff OP is congruent to AB.





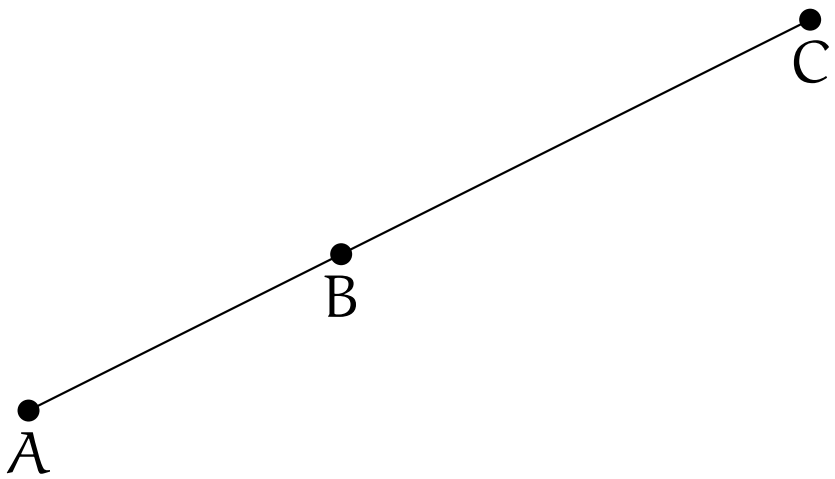
Translating geometry into algebra

In each of these geometries, we have the option of proving geometric theorems by translation into algebra, and showing that the translated statement holds in all models. Let us recall how this translation happens:

Translating geometry into algebra, II

Consider points $A = (a_x, a_y)$, $B = (a_x, b_y)$ and $C = (c_x, c_y)$.
Points A, B and C are collinear iff:

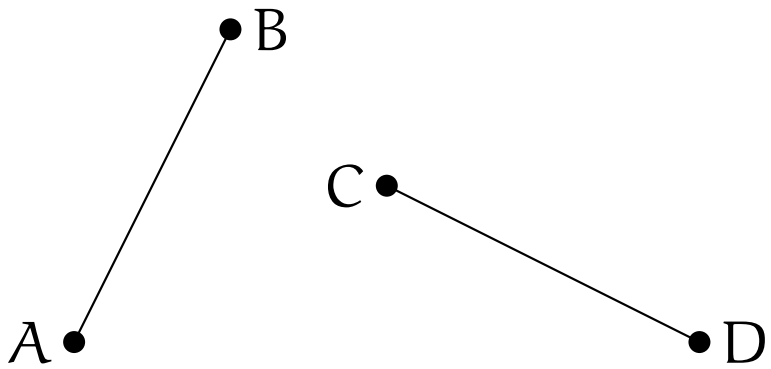
$$(a_x - b_x)(b_y - c_y) = (a_y - b_y)(b_x - c_x).$$



Translating geometry into algebra, III

Consider points $A = (a_x, a_y)$, $B = (a_x, b_y)$, $C = (c_x, c_y)$ and $D = (d_x, d_y)$.
Segments AB and CD are perpendicular iff:

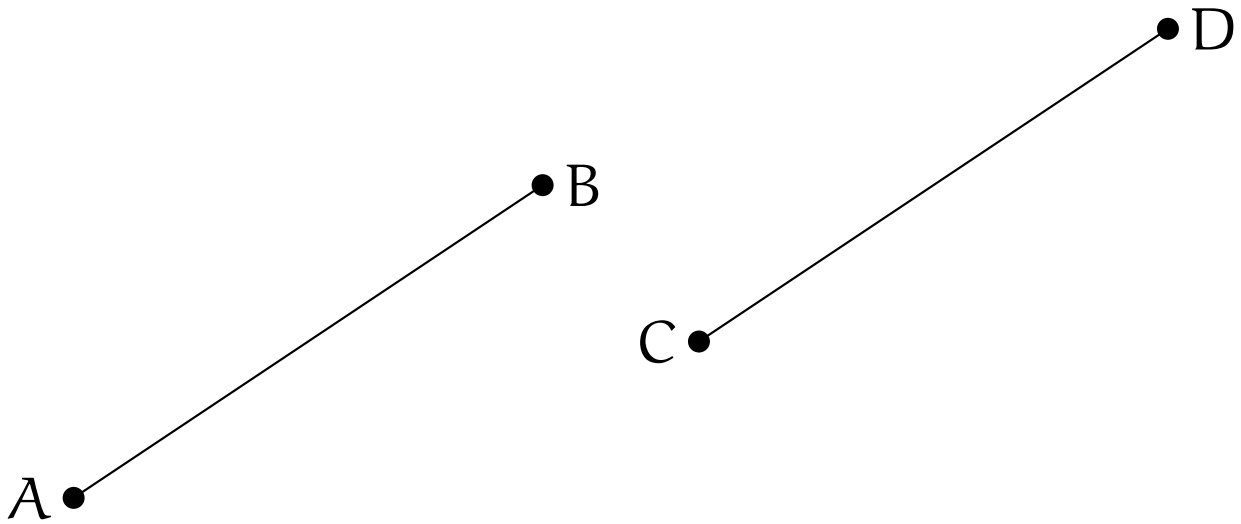
$$(a_x - b_x)(c_x - d_x) + (a_y - b_y)(c_y - d_y) = 0.$$



Translating geometry into algebra, IV

Consider points $A = (a_x, a_y)$, $B = (a_x, b_y)$, $C = (c_x, c_y)$ and $D = (d_x, d_y)$.
Segments AB and CD are parallel iff:

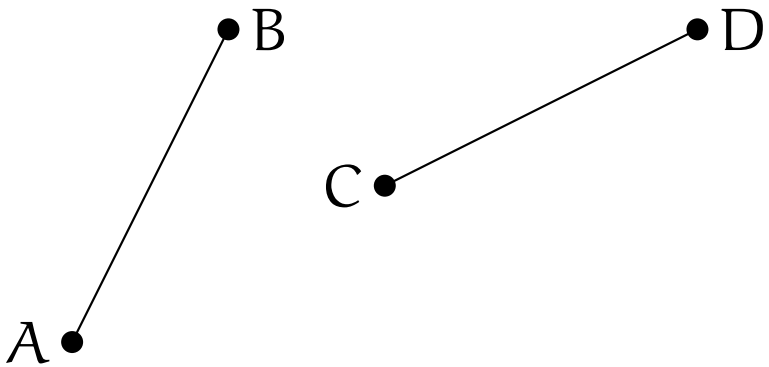
$$(a_x - b_x)(c_y - d_y) = (a_y - b_y)(c_x - d_x).$$



Translating geometry into algebra, V

Consider points $A = (a_x, a_y)$, $B = (a_x, b_y)$, $C = (c_x, c_y)$ and $D = (d_x, d_y)$.
Segments AB and CD are congruent (have same length) iff:

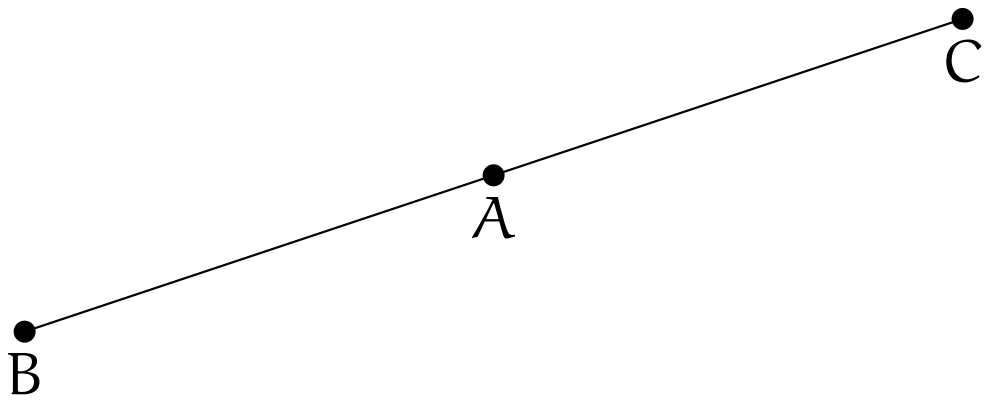
$$(a_x - b_x)^2 + (a_y - b_y)^2 = (c_x - d_x)^2 + (c_y - d_y)^2.$$



Translating geometry into algebra, VI

Consider points $A = (a_x, a_y)$, $B = (a_x, b_y)$ and $C = (c_x, c_y)$.
Point A is the midpoint of segment BC iff:

$$2a_x = b_x + c_x \quad \wedge \quad 2a_y = b_y + c_y.$$



Theorem proving

We know from the class that quantifier elimination gives us decision procedures for metric geometry and Tarski geometry.
But quantifier elimination has horrible algorithmic complexity and doesn't give satisfactory results when applied to geometry.
Therefore, we will restrict our attention to geometric statements of *constructive type*.

Statements of constructive type

We consider statements of metric geometry that translate into algebraic sentences of the form:

$$\forall \bar{u} \forall \bar{x},\ \bigwedge_i f_i(\bar{u}, \bar{x}) = 0 \wedge \bigwedge_j h_j(\bar{u}, \bar{x}) \neq 0 \Rightarrow g(\bar{u}, \bar{x}) = 0,$$

where the f_i, the h_j, and g are polynomials in $\mathbb{Q}[\bar{u}, \bar{x}]$.

Note

We know from Harrison that such a sentence is true over $\mathbb{C}$ iff it is true over all fields of characteristic zero.

Statements of constructive type

We consider statements of metric geometry that translate into algebraic sentences of the form:

$$\forall \bar{u} \forall \bar{x}, \bigwedge_i f_i(\bar{u}, \bar{x}) = 0 \wedge \bigwedge_j h_j(\bar{u}, \bar{x}) \neq 0 \Rightarrow g(\bar{u}, \bar{x}) = 0,$$

where the f_i, the h_j, and g are polynomials in $\mathbb{Q}[\bar{u}, \bar{x}]$.

Note

We know from Harrison that such a sentence is true over $\mathbb{C}$ iff it is true over all fields of characteristic zero.
Question: Why?

Gröbner bases

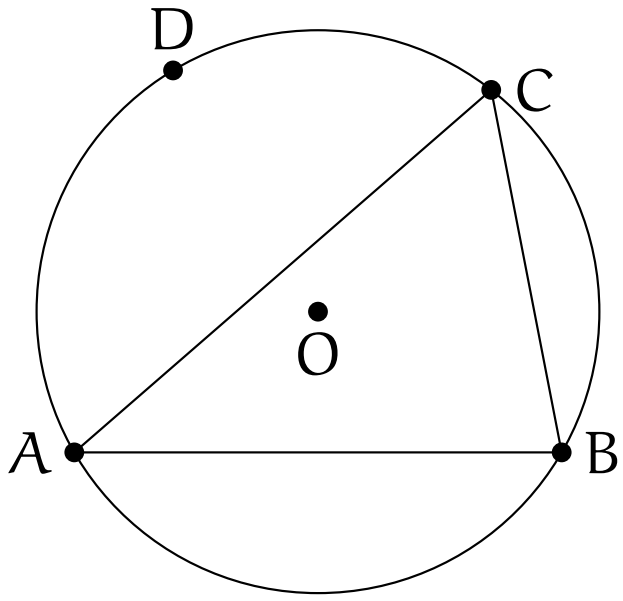
Recall that such statements can be decided effectively using the method of Gröbner bases.
However, geometric statements often do not include the necessary non-degeneracy conditions $h_j \neq 0$. We would like to generate these automatically. Especially since some of them are unfamiliar from Euclidean geometry, where all lines are nonisotropic (not perpendicular to themselves).

Wu's method

After Wu Wen-Tsün.

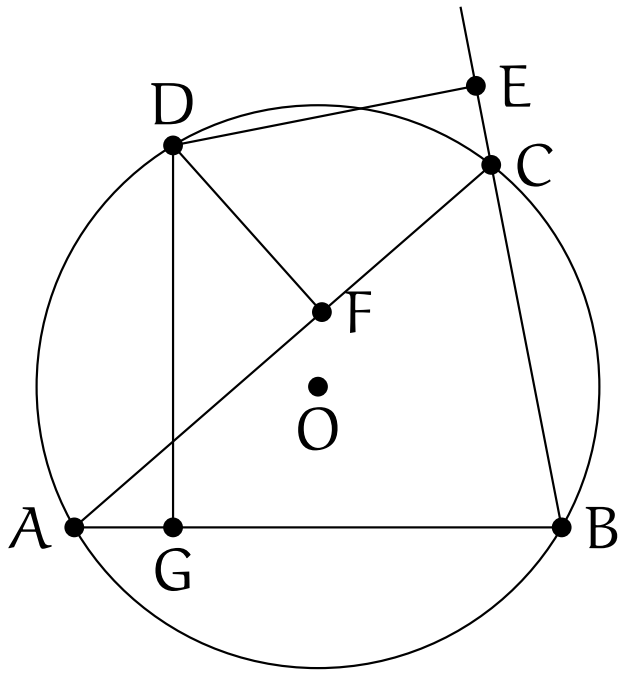
1. Translate problem into algebra.
2. Put hypothesis equations in triangular form.
3. Decompose into irreducible components.
4. Pseudo-divide and find remainder.
5. If remainder is zero, the theorem is *generically true*, that is, it holds under some extra *non-degeneracy conditions*, and these are provided by the method.

Example: Simson's Theorem



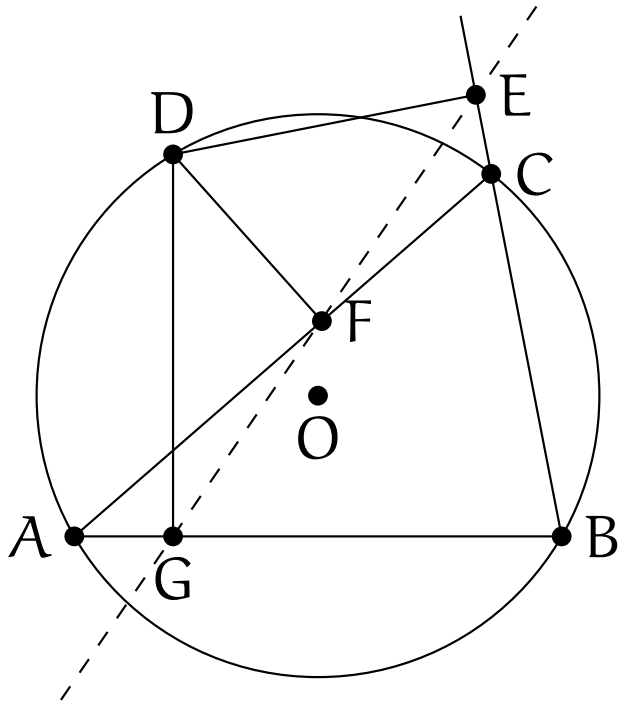
Let D be a point on the circumcircle of triangle ABC. From D are drawn perpendiculars to the sides BC, AC, and AB. Let the feet be E, F, and G, respectively. Show that E, F and G are collinear.

Example: Simson's Theorem



Let D be a point on the circumcircle of triangle ABC. From D are drawn perpendiculars to the sides BC, AC, and AB. Let the feet be E, F, and G, respectively. Show that E, F and G are collinear.

Example: Simson's Theorem



Let D be a point on the circumcircle of triangle ABC. From D are drawn perpendiculars to the sides BC, AC, and AB. Let the feet be E, F, and G, respectively. Show that E, F and G are collinear.

Example: Simson's Theorem, II

Translating to algebra, let $A = (0, 0)$, $B = (u_1, 0)$, $C = (u_2, u_3)$, $O = (x_2, x_1)$, $D = (x_3, u_4)$, $E = (x_5, x_4)$, $F = (x_7, x_6)$, $G = (x_3, 0)$.
The hypotheses are:

$$h_1 = 2u_2x_2 + 2u_3x_1 - u_3^2 - u_2^2 = 0 \qquad OA = OC$$
$$h_2 = 2u_1x_2 - u_1^2 = 0 \qquad OA = OB$$
$$h_3 = -x_3^2 + 2x_2x_3 + 2u_4x_1 - u_4^2 = 0 \qquad OA = OD$$
$$h_4 = u_3x_5 + (-u_2 + u_1)x_4 - u_1u_3 = 0 \qquad \mathrm{coll}(E, B, C)$$
$$h_5 = (u_2 - u_1)x_5 + u_3x_4 + (-u_2 + u_1)x_3 - u_3u_4 = 0 \qquad DE \perp BC$$
$$h_6 = u_3x_7 - u_2x_6 = 0 \qquad \mathrm{coll}(F, A, C)$$
$$h_7 = u_2x_7 + u_3x_6 - u_2x_3 - u_3u_4 = 0 \qquad DF \perp AC$$

Example: Simson's Theorem, III

The conclusion, coll(E, F, G), translates into

$$g = x_4x_7 + (-x_5 + x_3)x_6 - x_3x_4 = 0.$$

The first step of Wu's method is to triangulate the hypothesis system:

Example: Simson's Theorem, IV

Triangulation:

$$
\begin{aligned}
h_1 &= 2u_2x_2 + 2u_3x_1 - u_3^2 - u_2^2 = 0 \\
h_2 &= 2u_1x_2 - u_1^2 = 0 \\
h_3 &= -x_3^2 + 2x_2x_3 + 2u_4x_1 - u_4^2 = 0 \\
h_4 &= u_3x_5 + (-u_2 + u_1)x_4 - u_1u_3 = 0 \\
h_5 &= (u_2 - u_1)x_5 + u_3x_4 + (-u_2 + u_1)x_3 - u_3u_4 = 0 \\
h_6 &= u_3x_7 - u_2x_6 = 0 \\
h_7 &= u_2x_7 + u_3x_6 - u_2x_3 - u_3u_4 = 0
\end{aligned}
$$

Example: Simson's Theorem, IV

Triangulation:

$$
\begin{aligned}
h_1 &= 2u_2x_2 + 2u_3x_1 - u_3^2 - u_2^2 = 0 \\
h_2 &= 2u_1x_2 - u_1^2 = 0 \\
h_3 &= -x_3^2 + 2x_2x_3 + 2u_4x_1 - u_4^2 = 0 \\
h_4 &= u_3x_5 + (-u_2 + u_1)x_4 - u_1u_3 = 0 \\
h_5 &= (u_2 - u_1)x_5 + u_3x_4 + (-u_2 + u_1)x_3 - u_3u_4 = 0 \\
h_6 &= u_3x_7 - u_2x_6 = 0 \\
h_7 &= u_2x_7 + u_3x_6 - u_2x_3 - u_3u_4 = 0
\end{aligned}
$$

First, we pseudo-divide h_1 by h_2 using the variable x_2, replacing h_1 by the remainder, $2u_1u_3x_1 - u_1u_3^2 - u_1u_2^2 + u_1^2u_2$.

Example: Simson's Theorem, IV

Triangulation:

$$
\begin{aligned}
h_1 &= 2u_1u_3x_1 - u_1u_3^2 - u_1u_2^2 + u_1^2u_2 = 0 \\
h_2 &= 2u_1x_2 - u_1^2 = 0 \\
h_3 &= -x_3^2 + 2x_2x_3 + 2u_4x_1 - u_4^2 = 0 \\
h_4 &= u_3x_5 + (-u_2 + u_1)x_4 - u_1u_3 = 0 \\
h_5 &= (u_2 - u_1)x_5 + u_3x_4 + (-u_2 + u_1)x_3 - u_3u_4 = 0 \\
h_6 &= u_3x_7 - u_2x_6 = 0 \\
h_7 &= u_2x_7 + u_3x_6 - u_2x_3 - u_3u_4 = 0
\end{aligned}
$$

Example: Simson's Theorem, IV

Triangulation:

$$
\begin{aligned}
h_1 &= 2u_1u_3x_1 - u_1u_3^2 - u_1u_2^2 + u_1^2u_2 = 0\\
h_2 &= 2u_1x_2 - u_1^2 = 0\\
h_3 &= -x_3^2 + 2x_2x_3 + 2u_4x_1 - u_4^2 = 0\\
h_4 &= u_3x_5 + (-u_2 + u_1)x_4 - u_1u_3 = 0\\
h_5 &= (u_2 - u_1)x_5 + u_3x_4 + (-u_2 + u_1)x_3 - u_3u_4 = 0\\
h_6 &= u_3x_7 - u_2x_6 = 0\\
h_7 &= u_2x_7 + u_3x_6 - u_2x_3 - u_3u_4 = 0
\end{aligned}
$$

Next, we pseudo-divide h_4 by h_5 using the variable x_5, replacing h_5 by h_4 and h_4 by the remainder,
$(-u_3^2-u_2^2+2u_1u_2-u_1^2)x_4+(u_2-u_1)u_3x_3+u_3^2u_4+(-u_1u_2+u_1^2)u_3$.

Example: Simson's Theorem, IV

Triangulation:

$$
\begin{aligned}
h_1 &= 2u_1u_3x_1 - u_1u_3^2 - u_1u_2^2 + u_1^2u_2 = 0 \\
h_2 &= 2u_1x_2 - u_1^2 = 0 \\
h_3 &= -x_3^2 + 2x_2x_3 + 2u_4x_1 - u_4^2 = 0 \\
h_4 &= (-u_3^2 - u_2^2 + 2u_1u_2 - u_1^2)x_4 + \cdots + (-u_1u_2 + u_1^2)u_3 \\
h_5 &= u_3x_5 + (-u_2 + u_1)x_4 - u_1u_3 = 0 \\
h_6 &= u_3x_7 - u_2x_6 = 0 \\
h_7 &= u_2x_7 + u_3x_6 - u_2x_3 - u_3u_4 = 0
\end{aligned}
$$

Example: Simson's Theorem, IV

Triangulation:

$$
\begin{aligned}
h_1 &= 2u_1u_3x_1 - u_1u_3^2 - u_1u_2^2 + u_1^2u_2 = 0 \\
h_2 &= 2u_1x_2 - u_1^2 = 0 \\
h_3 &= -x_3^2 + 2x_2x_3 + 2u_4x_1 - u_4^2 = 0 \\
h_4 &= (-u_3^2 - u_2^2 + 2u_1u_2 - u_1^2)x_4 + \cdots + (-u_1u_2 + u_1^2)u_3 \\
h_5 &= u_3x_5 + (-u_2 + u_1)x_4 - u_1u_3 = 0 \\
h_6 &= u_3x_7 - u_2x_6 = 0 \\
h_7 &= u_2x_7 + u_3x_6 - u_2x_3 - u_3u_4 = 0
\end{aligned}
$$

Finally, we pseudo-divide h_6 by h_7 using the variable x_7, replacing h_6 by the remainder, $(-u_3^2 - u_2^2)x_6 + u_2u_3x_3 + u_3^2u_4$.

Example: Simson's Theorem, IV

Triangulation:

$$
\begin{aligned}
h_1 &= 2u_1u_3x_1 - u_1u_3^2 - u_1u_2^2 + u_1^2u_2 = 0 \\
h_2 &= 2u_1x_2 - u_1^2 = 0 \\
h_3 &= -x_3^2 + 2x_2x_3 + 2u_4x_1 - u_4^2 = 0 \\
h_4 &= (-u_3^2 - u_2^2 + 2u_1u_2 - u_1^2)x_4 + \cdots + (-u_1u_2 + u_1^2)u_3 \\
h_5 &= u_3x_5 + (-u_2 + u_1)x_4 - u_1u_3 = 0 \\
h_6 &= (-u_3^2 - u_2^2)x_6 + u_2u_3x_3 + u_3^2u_4 = 0 \\
h_7 &= u_2x_7 + u_3x_6 - u_2x_3 - u_3u_4 = 0
\end{aligned}
$$

Example: Simson's Theorem, IV

Triangulation:

$$
\begin{aligned}
h_1 &= 2u_1u_3x_1 - u_1u_3^2 - u_1u_2^2 + u_1^2u_2 = 0 \\
h_2 &= 2u_1x_2 - u_1^2 = 0 \\
h_3 &= -x_3^2 + 2x_2x_3 + 2u_4x_1 - u_4^2 = 0 \\
h_4 &= (-u_3^2 - u_2^2 + 2u_1u_2 - u_1^2)x_4 + \cdots + (-u_1u_2 + u_1^2)u_3 \\
h_5 &= u_3x_5 + (-u_2 + u_1)x_4 - u_1u_3 = 0 \\
h_6 &= (-u_3^2 - u_2^2)x_6 + u_2u_3x_3 + u_3^2u_4 = 0 \\
h_7 &= u_2x_7 + u_3x_6 - u_2x_3 - u_3u_4 = 0
\end{aligned}
$$

Now the system is in triangular form. Successive pseudo-division of the goal polynomial g by these polynomials:

Example: Simson's Theorem, V

Pseudo-division: divide g by h_7 using x_7, we get

$$R_6 = (-u_2x_5 - u_3x_4 + u_2x_3)x_6 + u_3u_4x_4.$$

We then divide this polynomial by h_6 using x_6 and so on, and continuing in this way, the final remainder is indeed zero, so the theorem is true, under the non-degeneracy conditions:

$$\begin{aligned} 0 &\neq u_1u_3 \\ 0 &\neq -u_3^2 - u_2^2 + 2u_1u_2 - u_1^2 \\ 0 &\neq -u_3^2 - u_2^2 \\ 0 &\neq u_2 \end{aligned}$$

Triangulation procedure

Recursively, eliminate a variable x_r from all but one out of r equations in $x_1, \ldots, x_r$. There are four cases:

Case 1. No equation contains x_r. Something went wrong.

Case 2. Exactly one equation contains x_r. OK!

Case 3. One equation $f = 0$ has $\deg_{x_r} f = 1$. Easy to eliminate x_r from other equations.

Case 4. Take two equations $f_1 = 0$ and $f_2 = 0$ with minimal degrees in x_r. Pseudodivide.

Decomposition into irreducible components

Given a geometric configuration given by a set of hypothesis equations $h_i(\bar{u}, \bar{x}) = 0$, with $\bar{u} = u_1, \ldots, u_d$ and $\bar{x} = x_1, \ldots, x_r$, we form a variety in $\mathbb{C}^{d+r}$, $V = V(h_i)$. From algebraic geometry, we know that this splits into irreducible components:

$$V = V_1 \cup \cdots \cup V_c \cup W_1 \cup \cdots \cup W_l,$$

where the V_i have dimension d where the u_i are algebraically independent, and are the nondegenerate components, and the W_i, the other components, and are the degenerate components.

Generical truth

Given a polynomial $g \in \mathbb{Q}[\bar{u}, \bar{x}]$, we say $g = 0$ is *generically true* on V, if g vanishes on all the nondegenerate components.

Theorem

Given hypothesis equations h_i *in triangular form, the variety* V *is irreducible if each* h_i *is irreducible in* $\mathbb{Q}(\bar{u})[x_1, \ldots, x_i]/(h_1, \ldots, h_{i-1})$.

This gives us the Ritt-Wu Characteristic Set method for determining the irreducible components.

Pseudodivision

Given polynomials $g, h \in \mathbb{Z}[\bar{x}, y] = \mathbb{Z}[\bar{x}][y]$. We write

$$g = a_n y^n + \cdots + a_1 y + a_0$$
$$h = b_m y^m + \cdots + b_1 y + b_0,$$

where the a_i and b_j are polynomials in $\mathbb{Z}[\bar{x}]$.

Theorem

There exists an integer $k \geqslant 0$ *and polynomials* $p, q \in \mathbb{Z}[\bar{x}, y]$ *with* $\deg_y r < \deg_y h$ *such that*

$$b_m^k g = qh + r.$$

Furthermore, there is an algorithm to find k, p *and* q.

The subsidiary conditions

Given hypothesis equations h_j in triangular form, and given a goal polynomial g. Form successive pseudo-divisions g by h_r using x_r, remainder of that by h_{r-1} using x_{r-1}, and so on until we pseudo-divide by h_1 using x_1, getting final remainder r. We get

$$s_1^{k_1} \dots s_r^{k_r} g = q_1 h_1 + \dots q_r h_r + r,$$

where s_i is the leading coefficient in h_i.
Thus, the corresponding geometric statement is generically true if $r = 0$.

Real geometry

Wu's method gives a decision method for geometric statements of constructive type over algebraically closed fields.
What about Euclidean geometry? Luckily, most statements of constructive type in Euclidean geometry are *generic*, which means that the real nondegenerate varieties for the configuration are of real dimension d. This happens in maybe 95% of interesting statements (Chou).

Theorem

A generic statement is generically true over $\mathbb{R}$ iff it is generically true over $\mathbb{C}$.

The area method

The algebraic methods are good to decide the validity of geometric theorems, but they are not suitable to generate human-understandable proofs.
Here, approaches based on geometric invariants (area, inner and exterior products, etc.) have been more successful.
Notable, the area method, and the full-angle method.

Differential geometry

Work over a differential field such as $\mathbb{Q}(t)$ with differential operator $(-)'$ satisfying

$$(f+g)' = f' + g'$$
$$(fg)' = f'g + fg' \qquad \text{Leibniz's law}$$

Pseudo-division, the CS method, and the decomposition algorithm can be extended to work in this setting.
Example: the Kepler-Newton problem: show Newton's Law of Gravitation follows from Kepler's Laws.

References I


Shang-Ching Chou.
An introduction to Wu's method for mechanical theorem proving in geometry.
J. Automat. Reason., 4(3):237–267, 1988.


Shang-Ching Chou.
Mechanical geometry theorem proving, volume 41 of *Mathematics and its Applications*.
D. Reidel Publishing Co., Dordrecht, 1988.
With a foreword by Larry Wos.


Shang-Ching Chou and Xiao-Shan Gao.
Automated reasoning in geometry.
In Robinson and Voronkov [5], pages 707–749.

References II


David Cox, John Little, and Donal O'Shea.
Ideals, varieties, and algorithms.
Undergraduate Texts in Mathematics. Springer, New York, third edition, 2007.
An introduction to computational algebraic geometry and commutative algebra.


John Alan Robinson and Andrei Voronkov, editors.
Handbook of Automated Reasoning (in 2 volumes).
Elsevier and MIT Press, 2001.