Automatic Geometric Theorem Proving: Turning Euclidean Geometry into Algebra to Prove Theorems

Dr. Heather Coughlin
California State University, Stanislaus

Overview:

- polynomials, “zeros” of polynomials - varieties
- polynomial rings, ideals in polynomial rings, ideals of varieties
- translating Euclidean geometry into commutative algebra
- proving Euclidean geometry theorems with commutative algebra software
- troubles with the process: degenerate cases and how to handle them

Polynomials:

Examples:

1. $f(x, y) = x^2 + y^2 - 4$

2. $g(x, y) = xy - x^3 + 1$

3. $h(x, y, z) = z - x^2 - y^2$

4. $j(x, y, z) = z^2 - x^2 - y^2$

(Algebraic Geometry) Varieties:

Let k be a field, e.g. $\mathbb{R}$ (real numbers), or $\mathbb{C}$ (complex numbers).

Definition: Let $f(x_1, x_2, \ldots, x_n)$ be a polynomial in $x_1, x_2, \ldots, x_n$ with coefficients in k. Then set

$$V(f) = \{(a_1, a_2, \ldots, a_n) \in k^n \mid f(a_1, a_2, \ldots, a_n) = 0\}$$

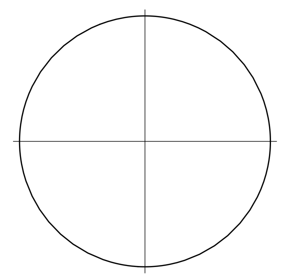
We call $V(f)$ the **affine variety** defined by f.

Note: $V(f)$ is the set of all solutions of $f = 0$

Examples:

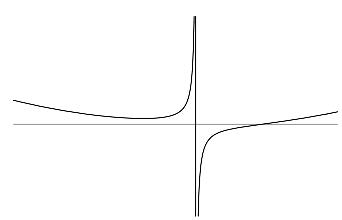
1. $f(x,y) = x^2 + y^2 - 4 = 0$

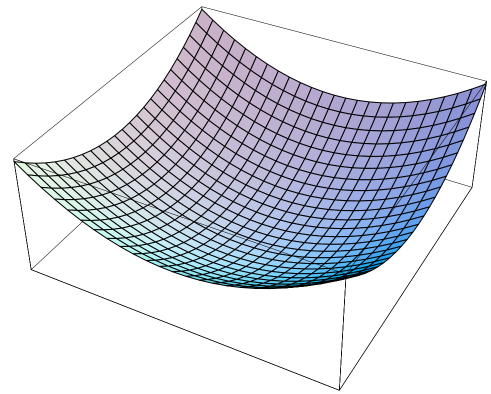
   $x^2 + y^2 = 4$ ($V(f)$ is a circle of radius 2)



2. $g(x,y) = xy - x^3 + 1 = 0$

   $$y = \frac{x^3 - 1}{x}$$





3. $h(x, y, z) = z - x^2 - y^2 = 0$

$z = x^2 + y^2$ ($V(f)$ is the parabola $z = x^2$ rotated about the z-axis)

4. $j(x, y, z) = z^2 - x^2 - y^2 = 0$

$z^2 = x^2 + y^2$ ($V(g)$ is a cone)

Notes:

- $V(f_1, \ldots, f_s) = \{(a_1, a_2, \ldots, a_n) \in k^n \mid f_i(a_1, a_2, \ldots, a_n) = 0$ for all $1 \leq i \leq s\}$

- $V(f_1, \ldots, f_s) = V(f_1) \cap V(f_2) \cap \cdots \cap V(f_s)$

(Commutative Algebra) Polynomial Rings:

Definition: Let k be a field, e.g. $\mathbb{R}$ or $\mathbb{C}$. A **polynomial ring** in n-variables over k, denoted $k[x_1, \ldots, x_n]$ is the collection of all polynomials with coefficients from k under polynomial addition and multiplication.

Definition: Let I be a non-empty subset of $k[x_1, \ldots, x_n]$. We say I is an **ideal** of $k[x_1, \ldots, x_n]$ if

- $0 \in I$,
- if $f, g \in I$, then $f + g \in I$,
- if $f \in I$ and $h \in k[x_1, \ldots, x_n]$, then $hf \in I$.

Example: Consider $\mathbb{R}[x]$, the polynomial ring consisting of all polynomials in x with real coefficients. Define the **ideal generated by** x to be

$$I = \langle x \rangle = \{g(x) \cdot x \mid g(x) \in \mathbb{R}[x]\}.$$

Then I, the set of all polynomials with zero constant terms, is an ideal of $\mathbb{R}[x]$.

Example: Let $f_1, \ldots, f_s \in k[x_1, \ldots, x_n]$. Then the **ideal generated by** $f_1, \ldots, f_s$ is

$$\langle f_1, \ldots, f_s \rangle = \{h_1 f_1 + \ldots + h_s f_s \mid h_1, \ldots, h_s \in k[x_1, \ldots, x_n]\}.$$

Example: $I = \langle x, 2 \rangle$ in $\mathbb{R}[x]$ is the set of all polynomials with even constant term. Indeed,

$$I = \langle x, 2 \rangle = \{g(x) \cdot x + h(x) \cdot 2 \mid g, h \in \mathbb{R}[x]\}$$

Example/Defn: Let $W \subset k^n$, a set of n-tuples. We want to consider the set of all polynomials which vanish on W. Define this set of polynomials as

$$I(W) = \{f \in k[x_1, \ldots, x_n] \mid f(w) = 0 \text{ for all } w \in W\}.$$

Note:

1. $I(W)$ is an ideal of $k[x_1, \ldots, x_n]$
2. $W \subset B$ if and only if $I(W) \supset I(B)$

Recall:
$$\begin{aligned} V(f_1, \ldots, f_s) &= \{(a_1, a_2, \ldots, a_n) \in k^n \mid f_i(a_1, a_2, \ldots, a_n) = 0 \\ &\qquad\qquad\qquad\qquad\qquad \text{for all } 1 \leq i \leq s\} \\ &= V(\langle f_1, \ldots, f_s \rangle) \end{aligned}$$

The Big Deal: So $I(-)$ takes a set of n-tuples and gives an ideal, and $V(-)$ takes an ideal and gives a set of n-tuples. This relationship is inclusion reversing.

Even Bigger Deal: Now $V(I(W)) = W$. However, in general $I(V(\langle f_1, \ldots, f_s \rangle)) \supseteq \langle f_1, \ldots, f_s \rangle$. Hilbert's Nullstellensatz will save the day!

Theorem: (Hilbert's Nullstellensatz) Let k be an algebraically closed field. For any ideal $J \subset k[x_1, \ldots, x_n]$,

$$I(V(J)) = \sqrt{J} = \{f \mid f^m \in J \text{ for some integer } m \geq 1\}.$$

Note:

- $V(\langle x \rangle) = V(\langle x^2 \rangle)$

- Over $\mathbb{R}$, $V(\langle x^2 + 1 \rangle) = V(\langle 1 \rangle) = \emptyset$

Biggest Deal:

Computational Commutative Algebra allows us to compute examples.
If we know what elements generate an ideal I, i.e. $I = \langle f_1, \ldots, f_s \rangle$, then we can program a computer to

- compute $\sqrt{I}$,

- (more importantly) determine if any given polynomial g is in I. That is, if we can find polynomials $h_1, \ldots, h_s$ such that

  $$g = h_1 f_1 + h_2 f_2 + \cdots + h_s f_s.$$

  In fact, if such a decomposition exists, we can actually compute $h_1, \ldots, h_s$.

- determine if any given polynomial g is in $\sqrt{I}$.

Translating a Euclidean Geometry Theorem into Algebra

Example: Consider a circle with points O, A, B on the circle. Suppose the line segment OA is a diameter of the circle. Then line determined by OB is perpendicular to line determined by BA.

Automatic Proof: Place a coordinate system so that

$$O = (0, 0),\ A = (a_1, a_2),\ B = (b_1, b_2).$$

We must translate the theorem into commutative algebra/algebraic geometry.

- Let r be the radius of the circle.
- (hypothesis 1) OA is a diameter of the circle. By the distance formula:

$$2r = \sqrt{a_1^2 + a_2^2}.$$

  This gives our first hypothesis equation:

$$h_1 := a_1^2 + a_2^2 - 4r^2 = 0$$

- (hypothesis 2) B is a point on the circle with radius r and center $\left(\frac{a_1}{2}, \frac{a_2}{2}\right)$.

The equation of the circle is: $\left(x - \frac{a_1}{2}\right)^2 + \left(y - \frac{a_2}{2}\right)^2 = r^2$.

Then $\left(b_1 - \frac{a_1}{2}\right)^2 + \left(b_2 - \frac{a_2}{2}\right)^2 = r^2$.

So $\left(\frac{2b_1 - a_1}{2}\right)^2 + \left(\frac{2b_2 - a_2}{2}\right)^2 - r^2 = 0$,

which gives our second hypothesis equation:

$$h_2 := (2b_1 - a_1)^2 + (2b_2 - a_2)^2 - 4r^2 = 0.$$

- (conclusion) Finally, we must translate the thesis statement (i.e. what we are trying to prove): line OB is perpendicular to line BA.

  The equation of line OB is

  $$y = \left(\frac{b_2}{b_1}\right) x.$$

  The equation of line BA is

  $$y - a_2 = \frac{b_2 - a_2}{b_1 - a_1}(x - a_1).$$

  The lines are perpendicular if the product of their slopes is -1:

  $$\frac{b_2}{b_1}\left(\frac{b_2 - a_2}{b_1 - a_1}\right) = -1$$

  So $b_2(b_2 - a_2) = -b_1(b_1 - a_1)$.

  Thus, our thesis equation is:

  $$t := b_2(b_2 - a_2) + b_1(b_1 - a_1) = 0.$$

Main Idea

We have the following polynomials equations in the variables a_1, a_2, b_1, b_2, s:

$$\begin{aligned} h_1 &:= a_1^2 + a_2^2 - 4r^2 = 0 \\ h_2 &:= (2b_1 - a_1)^2 + (2b_2 - a_2)^2 - 4r^2 = 0 \\ t &:= b_2(b_2 - a_2) + b_1(b_1 - a_1) = 0. \end{aligned}$$

To prove the theorem, it is enough to show that the values of a_1, a_2, b_1, b_2, s which make $h_1 = h_2 = 0$ also make $t = 0$. That is the points which make the hypothesis polynomials vanish also make the thesis polynomial vanish.

Set H to be the "hypotheses ideal," $H = \langle h_1, h_2 \rangle$.

Set T to be the "thesis ideal," $T = \langle t \rangle$.

We must show $V(h_1, h_2) \subseteq V(t)$, or equivalently $I(V(H)) \supseteq I(V(T))$.

That is $\sqrt{T} \subseteq \sqrt{H}$.

It is enough to show that the generators of T (for this example, t) are elements of $\sqrt{H}$.

For this example, it happens to turn out that $t \in H \subseteq \sqrt{H}$.

We may use a computer algebra system, such as CoCoA to determine this. The code (with output) looks like:

```
Use R::=Q[a[1..2],b[1..2],r];
I:=Ideal(a[1]^2+a[2]^2-4r^2, (2b[1]-a[1])^2+(2b[2]-a[2])^2-4r^2);
T:=b[1](b[1]-a[1])+b[2](b[2]-a[2]);
NFsAreZero([T],I);
TRUE
```

Hence the theorem is true.

Degenerate Cases

The previous example was very nice in that the degenerate situation did not hinder the algebra. However, this is not always the case.

Example: Theorem: The diagonals of a parallelogram bisect each other.

Let A, B, C, D be the vertices of the parallelogram, and N be the point of intersection of the diagonals.

We must prove $AN = DN$ and $BN = CN$.

Automatic Proof: Introduce a coordinate system with

$$A = (0, 0),\ B = (u_1, 0),\ C = (u_2, u_3).$$

Inherent in this setup, we need $u_1 \neq 0$ and $u_3 \neq 0$.

Let $D = (x_1, x_2)$. To require that we indeed have a parallelogram, we need:

$$\overline{AB} \parallel \overline{CD} : \quad 0 = \frac{x_2 - u_3}{x_1 - u_2}$$

$$\overline{AC} \parallel \overline{BD} : \ \frac{u_3}{u_2} = \frac{x_2}{x_1 - u_1}.$$

Clear denominators to get the hypothesis equations:

$$\begin{aligned} h_1 &:= x_2 - u_3 = 0 \\ h_2 &:= (x_1 - u_1)u_3 - x_2 u_2 = 0. \end{aligned}$$

Now for $N = (x_3, x_4)$. It must satisfy

$$A, N, D \text{ are collinear } : \qquad \frac{x_4}{x_3} = \frac{u_3}{x_1}$$

$$B, N, C \text{ are collinear } : \frac{x_4}{x_3 - u_1} = \frac{u_3}{u_2 - u_1}.$$

Clear denominators to get the hypothesis equations:

$$\begin{aligned} h_3 &:= x_4 x_1 - x_3 u_3 = 0 \\ h_4 &:= x_4(u_2 - u_1) - (x_3 - u_1)u_3 = 0. \end{aligned}$$

To create the thesis polynomials, we use the distance formula, then square each side.

$$\begin{aligned} AN = ND: &\quad x_3^2 + x_4^2 = (x_3 - x_1)^2 + (x_4 - x_2)^2 \\ BN = NC: &\quad (x_3 - u_1)^2 + x_4^2 = (x_3 - u_2)^2 + (x_4 - u_3)^2. \end{aligned}$$

Cancel like terms, then write the thesis equations as

$$\begin{aligned} t_1 &:= x_1^2 - 2x_1x_3 - 2x_4x_2 + x_2^2 = 0 \\ t_2 &:= 2x_3u_1 - 2x_3u_2 - 2x_4u_3 - u_1^2 + u_2^2 + u_3^2 = 0. \end{aligned}$$

Again, we create the "hypothesis ideal" $H = \langle h_1, h_2, h_3, h_4 \rangle$ in the polynomial ring $\mathbb{R}[u_1, u_2, u_3, x_1, x_2, x_3, x_4]$.

We must show $t_1, t_2 \in \sqrt{H}$.

If we run to a computer algebra system (like CoCoA) and do some computations which involve Gröbner bases, we will find the inclusion is false.

Why? The variety $V = V(h_1, h_2, h_3, h_4)$ is reducible, that is it is the union of other affine varieties.

With the use of Gröbner bases computations, it turns out that

$$V = V' \cup U_1 \cup U_2 \cup U_3,$$

where

$$\begin{aligned} V' &= V\left(x_1 - u_1 - u_2, x_2 - u_3, x_3 - \frac{u_1 + u_2}{2}, x_4 - \frac{u_3}{2}\right), \\ U_1 &= V(x_2, x_4, u_3), \\ U_2 &= V(x_1, x_2, u_1 - u_2, u_3), \\ U_3 &= V(x_1 - u_2, x_2 - u_3, x_3u_3 - x_4u_2, u_1). \end{aligned}$$

Notice that on U_1, U_2, U_3, we have $u_1 = 0$ or $u_3 = 0$, which were the degenerate cases. So we may restrict to V'. Using our computer algebra system, we conclude $t_1, t_2 \in I(V')$, thus proving the theorem.

The Process of Automatic Proofs

1. Translate the hypotheses into the vanishing of a set of polynomials, $h_1, \ldots, h_n \in \mathbb{R}[u_1, \ldots, u_m, x_1, \ldots x_n]$, with $u_1, \ldots, u_m$ being the parameters of the geometric problem (and the variables x_i depend upon the u_j's.
2. Translate the conclusion into the vanishing of a set of polynomials, $t_j,\ j = 1, \ldots, s$.
3. Compare $V(t_1, \ldots, t_s)$ and $V(h_1, \ldots, h_n)$, that is $t_1, \ldots, t_s$ and $\sqrt{H}$, where $H = \langle h_1, \ldots, h_n \rangle$.
   (a) We say a conclusion t *follows strictly* from the hypotheses if $t \in \sqrt{H}$.
   (b) We say a conclusion t *follows generically* from the hypotheses if $t \in I(V')$, where V' is the union of irreducible components of $V(h_1, \ldots, h_n)$ on which the u_i are algebraically independent.

Proposition: g follows generically from $h_1, \ldots h_n$ when there is some nonzero polynomial $c(u_1, \ldots, u_m) \in \mathbb{R}[u_1, \ldots, u_m]$ such that $c \cdot g \in \sqrt{H}$.

Note: There is an algorithm to find such a polynomial c.

References

[1] Cox, Little, O'Shea, *Ideals, Varieties, and Algorithms, Second Edition*,Undergraduate Texts in Mathematics, Springer, 1997.

[2] Bazzotti, Dalzotto, Robbiano, *Remarks on Geometric Theorem Proving*, Proceedings of the CoCoA Conference, Kingston, Ontario, 2001.

[3] Recio, Vélez-Melón, *Automatic Discovery of Theorems in Elementary Geometry*, Proceedings of the CoCoA Conference, Kingston, Ontario, 2001.

[4] Roozemond, *2J008 Bachelorproject: Automatic Geometric Theorem Proving*, Eindhoven University of Technology, 2003

[5] Giovini, Niesi, Capani, *http://cocoa.dima.unige.it*