Automatic Geometric Theorem Proving

Markus Tran

Contents

1. Introduction

Doing mathematics often requires a "touch of intuition" which is thought to be uniquely human. We are able to reason about mathematical problems, and progress forwards towards a reasonable solution. On the contrary, computer machines are confined to their own rigid system of rules, and can only make deductions "within a system", which often isn't sufficient for general problems which require "out of the box" thinking. This difference seems to create an impenetrable wall between human and computer thought.

In *Gödel, Escher, Bach*, Douglas Hofstadter presents the MU puzzle to highlight the difference between modes of thought. The goal of the puzzle is to begin with the string MI and construct the string MU by applying any of the four formal rules any number of times. There is no solution, but to a robot operating in the "Mechanical Mode," will only be able to apply rule after rule hoping that MU will be reached in time. But a human can operate in the "Intelligent Mode" and make deductions *about* the puzzle to conclude that MU is impossible. Gödel takes it a step further and concludes in his Incompleteness Theorems that any such formal system, no matter how complex, is subject a similar flaw. There will always be MU-like theorems that a robot simply cannot solve, but humans can solve by somehow reasoning about the *meaning* of purely mathematical statements (e.g. the Gödel sentence).

Still, the use of computers in mathematics is far from futile. Computers are still able to solve a wide variety of problems, and in 1976, computers were able to solve the infamous Four color theorem (despite controversy revolving around the usefulness of such a proof). It is interesting to consider problems that computers are able to provide insight to. One such field is geometry. I've previously attempted to use a program to check for the existence of a perfect cuboid (https://pf-n.co/blog/perfect-cuboid), so this area of research interests me and hopefully will provide me with a deeper understanding of computer-assisted proofs.

2. Geometric Statements as Polynomials

Automatic Geometric Theorem Proving begins with a translations of geometric statements into a system of polynomial equations. A statement such as "$\overline{AB}$ is parallel to $\overline{CD}$" asserts some numerical relationship between the coordinates of the points A, B, C, D. After translating a geometric question into polynomial equations, we can use theorems we've studied to analyze the relationship between a given conclusion and several hypotheses. Several translations are given in this section for general points on a plane.

(i) $\overline{AB}$ is parallel to $\overline{CD}$

$$\frac{B_y - A_y}{B_x - A_x} = \frac{D_y - C_y}{D_x - C_x} \implies$$
$$B_yD_x - B_yC_x - A_yD_x + A_yC_x - B_xD_y + B_xC_y + A_xD_y - A_xC_y = 0$$

(ii) $\overline{AB}$ is perpendicular to $\overline{CD}$

$$\frac{B_y - A_y}{B_x - A_x} = -\frac{D_x - C_x}{D_y - C_y} \implies$$
$$B_yD_y - B_yC_y - A_yD_y + A_yC_y + D_xB_x - D_xA_x - C_xB_x + C_xA_x = 0$$

(iii) A, B, C are collinear

$$\overline{AB} \parallel \overline{AC} \implies$$
$$B_yC_x - B_yA_x - A_yC_x + A_yA_x - B_xC_y + B_xA_y + A_xC_y - A_xA_y = 0 \implies$$
$$B_yC_x - B_yA_x - A_yC_x - B_xC_y + B_xA_y + A_xC_y = 0$$

(iv) The distance from A to B is equal to the distance from C to D: $AB = CD$

$$(B_x - A_x)^2 + (B_y - A_y)^2 = (D_x - C_x)^2 + (D_y - C_y)^2 \implies$$
$$B_x^2 - 2B_xA_x + A_x^2 + B_y^2 - 2B_yA_y + A_y^2 - D_x^2 + 2D_xC_x - C_x^2 - D_y^2 + 2D_yC_y - C_y^2 = 0$$

(v) The cross ratio of (A, B, C, D) is equal to $\rho \in \mathbb{R}$

$$\frac{\sqrt{(C_x - A_x)^2 + (C_y - A_y)^2} \cdot \sqrt{(D_x - B_x)^2 + (D_y - B_y)^2}}{\sqrt{(D_x - A_x)^2 + (D_y - A_y)^2} \cdot \sqrt{(C_x - B_x)^2 + (C_y - B_y)^2}} = \rho \implies$$
$$\frac{\left(C_x^2 - 2C_xA_x + A_x^2 + C_y^2 - 2C_yA_y + A_y^2\right) \cdot \left(D_x^2 - 2D_xB_x + B_x^2 + D_y^2 - 2D_yB_y + B_y^2\right)}{\left(D_x^2 - 2D_xA_x + A_x^2 + D_y^2 - 2D_yA_y + A_y^2\right) \cdot \left(C_x^2 - 2C_xB_x + B_x^2 + C_y^2 - 2C_yB_y + B_y^2\right)} = \rho^2 \implies$$

$$
\left(\begin{array}{rrrrrrrrrrrr}
 & C_x^2 D_x^2 & - & 2C_x^2 D_x B_x & + & C_x^2 B_x^2 & + & C_x^2 D_y^2 & - & 2C_x^2 D_y B_y & + & C_x^2 B_y^2 \\
- & 2C_x A_x D_x^2 & + & 4C_x A_x D_x B_x & - & 2C_x A_x B_x^2 & - & 2C_x A_x D_y^2 & + & 4C_x A_x D_y B_y & - & 2C_x A_x B_y^2 \\
+ & A_x^2 D_x^2 & - & 2A_x^2 D_x B_x & + & A_x^2 B_x^2 & + & A_x^2 D_y^2 & - & 2A_x^2 D_y B_y & + & A_x^2 B_y^2 \\
+ & C_y^2 D_x^2 & - & 2C_y^2 D_x B_x & + & C_y^2 B_x^2 & + & C_y^2 D_y^2 & - & 2C_y^2 D_y B_y & + & C_y^2 B_y^2 \\
- & 2C_y A_y D_x^2 & + & 4C_y A_y D_x B_x & - & 2C_y A_y B_x^2 & - & 2C_y A_y D_y^2 & + & 4C_y A_y D_y B_y & - & 2C_y A_y B_y^2 \\
+ & A_y^2 D_x^2 & - & 2A_y^2 D_x B_x & + & A_y^2 B_x^2 & + & A_y^2 D_y^2 & - & 2A_y^2 D_y B_y & + & A_y^2 B_y^2 \\
- & \rho^2 D_x^2 C_x^2 & + & 2\rho^2 D_x^2 C_x B_x & - & \rho^2 D_x^2 B_x^2 & - & \rho^2 D_x^2 C_y^2 & + & 2\rho^2 D_x^2 C_y B_y & - & \rho^2 D_x^2 B_y^2 \\
+ & 2\rho^2 D_x A_x C_x^2 & - & 4\rho^2 D_x A_x C_x B_x & + & 2\rho^2 D_x A_x B_x^2 & + & 2\rho^2 D_x A_x C_y^2 & - & 4\rho^2 D_x A_x C_y B_y & + & 2\rho^2 D_x A_x B_y^2 \\
- & \rho^2 A_x^2 C_x^2 & + & 2\rho^2 A_x^2 C_x B_x & - & \rho^2 A_x^2 B_x^2 & - & \rho^2 A_x^2 C_y^2 & + & 2\rho^2 A_x^2 C_y B_y & - & \rho^2 A_x^2 B_y^2 \\
- & \rho^2 D_y^2 C_x^2 & + & 2\rho^2 D_y^2 C_x B_x & - & \rho^2 D_y^2 B_x^2 & - & \rho^2 D_y^2 C_y^2 & + & 2\rho^2 D_y^2 C_y B_y & - & \rho^2 D_y^2 B_y^2 \\
+ & 2\rho^2 D_y A_y C_x^2 & - & 4\rho^2 D_y A_y C_x B_x & + & 2\rho^2 D_y A_y B_x^2 & + & 2\rho^2 D_y A_y C_y^2 & - & 4\rho^2 D_y A_y C_y B_y & + & 2\rho^2 D_y A_y B_y^2 \\
- & \rho^2 A_y^2 C_x^2 & + & 2\rho^2 A_y^2 C_x B_x & - & \rho^2 A_y^2 B_x^2 & - & \rho^2 A_y^2 C_y^2 & + & 2\rho^2 A_y^2 C_y B_y & - & \rho^2 A_y^2 B_y^2
\end{array}\right) = 0
$$

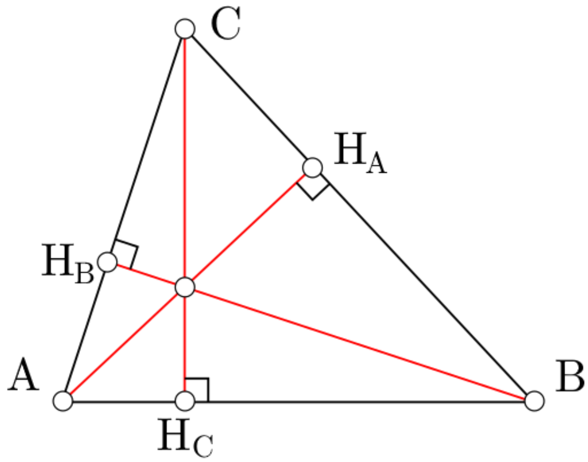
Most geometric statements can be expressed by one ore more polynomial equations.

3. Orthocenter Theorem

An application of Automatic Geometric Theorem Proving is applied for the following well-known theorem.

> **Theorem.** Let $\triangle ABC$ be a triangle in the plane. The three altitudes of a triangle meet at a single point H, often called the *orthocenter* of the triangle.

The first step is to translate the hypotheses into polynomial equations. Let $\triangle ABC$ be a triangle such that A lies on the origin and B lies on the x-axis as in the following diagram:



This gives us the independent variables

$$
\begin{aligned}
A &= (0,0), \\
B &= (u_1, 0), \\
C &= (u_2, u_3).
\end{aligned}
$$

Next, we construct the feet of the 3 altitudes with coordinates $H_A = (x_1, x_2)$, $H_B = (x_3, x_4)$, and $H_C = (x_5, 0)$. The requirement that $\overline{AH_A}$ forms an altitude with A is given by the two hypotheses

$$\begin{aligned} B, C, H_A \text{ are collinear:} \quad & h_1 = u_3x_1 - u_3u_1 - u_2x_2 + u_1x_2 = 0, \\ AH_A \perp BC\text{:} \quad & h_2 = x_2u_3 + u_2x_1 - u_1x_1 = 0. \end{aligned}$$

Doing the same for H_B and H_C gives a total of 5 hypotheses. (Note that the collinearity of A, B, H_C is omitted, since $A_y = B_y = (H_C)_y = 0$ by construction).

$$\begin{aligned} B, C, H_A \text{ are collinear:} \quad & h_1 = u_3x_1 - u_3u_1 - u_2x_2 + u_1x_2 = 0, \\ AH_A \perp BC\text{:} \quad & h_2 = x_2u_3 + u_2x_1 - u_1x_1 = 0, \\ A, C, H_B \text{ are collinear:} \quad & h_3 = u_3x_3 - u_2x_4 = 0, \\ BH_B \perp AC\text{:} \quad & h_4 = x_4u_3 + u_2x_3 - u_2u_1 = 0, \\ CH_C \perp AB\text{:} \quad & h_5 = u_1x_5 - u_1u_2 = 0. \end{aligned}$$

The conclusion that the three altitude intersects at a single point can be restated as follows: Let O be the point where $\overline{AH_A}$ and $\overline{BH_B}$ intersect; then C, H_C, O are collinear. This admits two additional hypotheses regarding $O = (x_6, x_7)$,

$$\begin{aligned} A, H_A, O \text{ are collinear:} \quad & h_6 = x_2x_6 - x_1x_7 = 0, \\ B, H_B, O \text{ are collinear:} \quad & h_7 = x_4x_6 - x_4u_1 - x_3x_7 + u_1x_7 = 0, \end{aligned}$$

and the final conclusion is

$$C, H_C, O \text{ are collinear:} \quad g = -u_3x_6 - x_5x_7 + x_5u_3 + u_2x_7 = 0.$$

Now we can use Maple to compute the Gröbner basis of the ideal

$$\langle h_1, \ldots, h_7, 1 - yg \rangle \subseteq \mathbb{R}(u_1, u_2, u_3)[x_1, \ldots, x_7, y].$$

```
> h_1 := u_3·x_1 − u_3·u_1 − u_2·x_2 + u_1·x_2 :
> h_2 := x_2·u_3 + u_2·x_1 − u_1·x_1 :
> h_3 := u_3·x_3 − u_2·x_4 :
> h_4 := x_4·u_3 + u_2·x_3 − u_2·u_1 :
> h_5 := u_1·x_5 − u_1·u_2 :
> h_6 := x_2·x_6 − x_1·x_7 :
> h_7 := x_4·x_6 − x_4·u_1 − x_3·x_7 + u_1·x_7 :
> g := −u_3·x_6 − x_5·x_7 + x_5·u_3 + u_2·x_7 :
> Groebner[Basis]([h_1, h_2, h_3, h_4, h_5, h_6, h_7, 1 − y·g], plex(x_1, x_2, x_3, x_4, x_5, x_6, x_7, y))
                                   [1]                                   (1)
```

Since the Gröbner basis is $\{1\}$, by Propositions 8 and 9, the conclusion g follows generally.

But it is also possible to see how g follows by computing the Gröbner basis for

$$\langle h_1, \ldots, h_7 \rangle \subseteq \mathbb{R}[u_1, u_2, u_3, x_1, \ldots, x_7],$$

which Maple gives as

$$\text{Groebner[Basis]}([h_1, \ldots, h_7], \text{lex}) = [-u_1^3 u_2 u_3 + u_1^2 u_2^2 u_3 + u_1^2 u_3^2 x_7, \ldots].$$

There are 30 elements in this basis, but we can see already that the first term factors into

$$-u_1^3 u_2 u_3 + u_1^2 u_2^2 u_3 + u_1^2 u_3^2 x_7 = u_1^2(-u_1 u_2 u_3 + u_2^2 u_3 + u_3^2 x_7)$$

which means that the variety defined by this ideal can be decomposed further. The following procedure can be used to recursively decompose the variety into (possibly non-distinct) irreducible varieties:

```
DecomposeVarieties := proc(polys)
  local i, j, f, groebnerBasis, polyFactors, splits, newBasis:
  groebnerBasis := Groebner[Basis](polys, porder):
  for i, f in groebnerBasis do
    polyFactors := factors(f)[2]:
    if numelems(polyFactors) > 1 then
      splits := [0 $ numelems(polyFactors)]:
      for j from 1 to numelems(polyFactors) do
        newBasis := copy(groebnerBasis):
        newBasis[i] := polyFactors[j][1]:
        splits[j] := DecomposeVarieties(newBasis):
      end do:
      return ListTools[Flatten](splits, 1):
    end if:
  end do:
return [groebnerBasis]:
end proc:
```

This procedure decomposes the original variety into 234 elements, but most of them contain either u_1 or u_3 as a basis polynomial. When either of these polynomials are in the basis, it results in the degenerate case of either $B = A$ or A, B, C collinear, so these varieties can be excluded.

```
> f := Groebner[Basis]([h_1, h_2, h_3, h_4, h_5, h_6, h_7], porder) :
> V := select(n → not u_1 in n and not u_3 in n, DecomposeVarieties(f, 1))
```

$$V := [[u\_2, x\_7, x\_6, x\_5, x\_4, x\_3, -u\_1^2 u\_3 + u\_1^2 x\_2 + u\_3^2 x\_2, -u\_1 u\_3 + u\_1 x\_2 + u\_3 x\_1, u\_1 x\_1 - u\_3 x\_2], [-u\_1 u\_2 + u\_2^2 + u\_3 x\_7, -u\_2 + x\_6, -u\_2 + x\_5, -u\_1 u\_2 u\_3 + u\_2^2 x\_4 + u\_3^2 x\_4, -u\_1^2 u\_2 + u\_1 u\_2^2 + u\_1 u\_3 x\_4 - u\_2 u\_3 x\_4 + u\_2 x\_4 x\_7, -u\_2 x\_4 + u\_3 x\_3, -u\_1 u\_2 + u\_2 x\_3 + u\_3 x\_4, u\_1 x\_4 - u\_1 x\_7 - u\_2 x\_4 + x\_3 x\_7, -u\_1^2 u\_3 + u\_1^2 x\_2 + u\_1 u\_2 u\_3 - 2 u\_2 u\_1 x\_2 + u\_2^2 x\_2 + u\_3^2 x\_2, -u\_1^2 u\_2 + u\_1 u\_2^2 + u\_1 x\_2 x\_7 + u\_2 u\_3 x\_2 - u\_2 x\_2 x\_7, -u\_1^2 u\_2 u\_3 - u\_1^2 u\_2 x\_4 + 2 u\_1 u\_2^2 u\_3 - 3 u\_1 u\_2^2 x\_2 - u\_1 u\_3^2 x\_4 + 2 u\_3 u\_1 x\_2 x\_4 + u\_1 x\_2 x\_3^2 + u\_1 x\_2 x\_4^2 + 2 u\_2^3 x\_2 + 2 u\_2 u\_3^2 x\_2, -u\_1 u\_3 + u\_1 x\_2 - u\_2 x\_2 + u\_3 x\_1, u\_1 x\_1 - u\_2 x\_1 - u\_3 x\_2, -u\_2 x\_2 + x\_1 x\_7, -u\_2 u\_1 x\_2 - u\_1 u\_2 x\_4 + u\_1 x\_2 x\_3 + u\_2 x\_1 x\_4 + u\_3 x\_2 x\_4]] \quad (7)$$

We are left with 2 varieties, V_1 and V_2. Since $u_2 \in V_1$, V_1 corresponds to the case where $\angle CAB$ forms a right angle. Regardless, Maple shows that g vanishes on both these varieties.

```
> PolynomialIdeals[IdealMembership](g, PolynomialIdeals[PolynomialIdeal](V[1]))
                                   true                                          (5)
> PolynomialIdeals[IdealMembership](g, PolynomialIdeals[PolynomialIdeal](V[2]))
                                   true                                          (6)
```

4. Centroid Theorem

The previous section is repeated here for a similar theorem.

> **Theorem.** Let $\triangle ABC$ be a triangle in the plane. If we let M_1 be the midpoint of $\overline{BC}$, M_2 be the midpoint of $\overline{AC}$ and M_3 be the midpoint of $\overline{AB}$, then the segments $\overline{AM_1}$, $\overline{BM_2}$ and $\overline{CM_3}$ meet at a single point M, often called the *centroid* of the triangle.

Let $\triangle ABC$ be defined as in the previous section:

$$\begin{aligned} A &= (0, 0), \\ B &= (u_1, 0), \\ C &= (u_2, u_3). \end{aligned}$$

Then the 3 midpoints $M_1 = (x_1, x_2)$, $M_2 = (x_3, x_4)$, and $M_3 = (x_5, 0)$ are constructed.

$$\begin{aligned} M_1 \text{ is the midpoint of } \overline{BC}: \quad & h_1 = 2x_1 - u_1 - u_2 = 0, \\ & h_2 = 2x_2 - u_3 = 0; \\ M_2 \text{ is the midpoint of } \overline{AC}: \quad & h_3 = 2x_3 - u_2 = 0, \\ & h_4 = 2x_4 - u_3 = 0; \\ M_3 \text{ is the midpoint of } \overline{AB}: \quad & h_5 = 2x_5 - u_1 = 0. \end{aligned}$$

The conclusion that the 3 medians intersect at a single point is translated to the fact that the intersection of $\overline{AM_1}$ and $\overline{BM_2}$ is collinear with C and M_3. Let $O = (x_6, x_7)$ be the intersection of $\overline{AM_1}$ and $\overline{BM_2}$.

$$\begin{aligned}
&A, M_1, O \text{ are collinear:} \quad h_6 = x_2x_6 - x_1x_7 = 0, \\
&B, M_2, O \text{ are collinear:} \quad h_7 = x_4x_6 - x_4u_1 - x_3x_7 + u_1x_7 = 0.
\end{aligned}$$

The final conclusion is

$$C, M_3, O \text{ are collinear:} \quad g = -u_3x_6 - x_5x_7 + x_5u_3 + u_2x_7 = 0.$$

Using Maple to compute the Gröbner basis of the ideal

$$\langle h_1, \ldots, h_7, 1 - yg \rangle \subseteq \mathbb{R}(u_1, u_2, u_3)[x_1, \ldots, x_7, y],$$

```
> h_1 := 2x_1 − u_1 − u_2:
> h_2 := 2x_2 − u_3:
> h_3 := 2x_3 − u_2:
> h_4 := 2x_4 − u_3:
> h_5 := 2x_5 − u_1:
> h_7 := x_4·x_6 − x_4·u_1 − x_3·x_7 + u_1·x_7:
> g := −u_3·x_6 − x_5·x_7 + x_5·u_3 + u_2·x_7:
> Groebner[Basis]([h_1, h_2, h_3, h_4, h_5, h_6, h_7, 1 − y·g], plex(x_1, x_2, x_3, x_4, x_5, x_6, x_7, y))
                                   [1]                                         (1)
```

The Gröbner basis is $\{1\}$, and the conclusion g follows generally. Addtionally, decomposing the variety defined by

$$\langle h_1, \ldots, h_7 \rangle \subseteq \mathbb{R}[u_1, u_2, u_3, x_1, \ldots, x_7]$$

results in 3 varieties.

```
> V := DecomposeVarieties(Groebner[Basis]([h_1, h_2, h_3, h_4, h_5, h_6, h_7], porder))
V := [[u_1, −u_2 x_7 + u_3 x_6, x_5, 2 x_4 − u_3, 2 x_3 − u_2, 2 x_2 − u_3, 2 x_1 − u_2], [u_3, x_7, 2 x_5 − u_1, x_4,      (8)
    2 x_3 − u_2, x_2, 2 x_1 − u_1 − u_2], [−u_3 + 3 x_7, −u_1 − u_2 + 3 x_6, 2 x_5 − u_1, 2 x_4 − u_3, 2 x_3 − u_2,
    2 x_2 − u_3, 2 x_1 − u_1 − u_2]]
> PolynomialIdeals[IdealMembership](g, PolynomialIdeals[PolynomialIdeal](V[3]))
                                   true                                        (9)
```

V_1 and V_2 correspond to the same degenerate cases as before, and $g \in V_3$ so the conclusion g follows. Curiously, g also follows strictly since $g \in \langle h_1, \ldots, h_7 \rangle$.

5. Exploration

Gröbner bases have shown that we have algorithmic methods for conclusively determining whether certain geometric theorems are true. This technique can be used for more general systems and theorems in those systems. “Using the Groebner basis algorithm to find proofs of unsatisfiability" by Clegg et al. shows how a modification of the technique can be used for proofs in a propositional calculus.

The general strategy is similar:

1. Translate axioms, hypotheses, and rules of inference into polynomial equations.
2. Use Gröbner bases to determine the relationship between hypotheses and conclusion.

The paper continues by offering a proof-proving algorithm similar to the Gröbner basis algorithm, then examining its efficacy and algorithmic complexity alongside other known algorithms.

What I find most interesting about this is how more natural statements of logic can be codified as "meaningless" assertions about numbers. Even if a computer can be used to solve any theorem or question we might pose, there is a disconnect between what the computer asserts is true and how we interpret it.

6. References

Clegg, M., Edmonds, J., & Impagliazzo, R. (1996, July). Using the Groebner basis algorithm to find proofs of unsatisfiability. In *Proceedings of the twenty-eighth annual ACM symposium on Theory of computing* (pp. 174-183).

Cox, D. A. (2016). *Ideals, Varieties, and Algorithms* (4th ed.). Springer.