Geometry via Algebra

Andrew Zhao

Research paper

1 A New Perspective

In high school, we tend to think of geometry as being composed of lines, circles and triangles. We also tend to think about algebra as composed of polynomials. We can actually combine polynomials and properties of space into a field of study: algebraic geometry. Algebraic geometry studies the set of zeros of polynomials using algebraic structures such as rings. One might be thinking that algebraic geometry has no resemblance to what we would call Euclidean geometry: what do polynomials have to do with circles? Turns out we can use techniques from algebraic geometry to verify theorems in Euclidean geometry, a method known as automatic theorem proving. There are two main steps involved:

1. Encode each geometrical property of the configuration into a polynomial (Shout out for coordinate bashing). One way to accomplish this is to use Cartesian coordinates to represent points. For example, consider two lines, one generated by the points (a_1, a_2) and (b_1, b_2) and the other one generated by (c_1, c_2) and (d_1, d_2). Thanks to Algebra 1, we note that the two lines are perpendicular if and only if the equation $(a_2 - b_2)(c_1 - d_1) + (a_1 - b_1)(c_2 - d_2) = 0$ holds. If done right, we should get a set of polynomials that correspond to the information we are given in the configuration, and at "theorem" polynomial which encodes the theorem we want to prove. In terms of algebraic geometry, the theorem is equivalent to having the algebraic set generated by the "theorem" polynomial contains every single algebraic set generated by the hypothesis polynomials (Remember that $V(I)$ is inclusion reversing).

2. Solve the algebraic problem. We can show that the above condition is equivalent to showing that the theorem polynomial is part of the ideal generated by the hypothesis polynomial, reducing the problem to the Ideal Membership Problem. This problem is solved using Grobner bases, which is Gaussian elimination on steroids.

2 Grobner Basis

To solve the polynomial portion, we need to introduce the Grobner basis. Due to their properties, Grobner basis are useful in fields such as solving linear equations and linear programming. But to define what a Grobner basis actually is, we need some more background information.
Definition: A monomial ordering $<$ is a total ordering on the monomial terms x^p such that if $x^a < x^b$, than $x^a x^c < x^b x^c$.
Note that for this paper, we will use the lexicographic ordering for monomials. The ordering is given by $1 < x < x^2 < x^3$ ... $y < xy < x^2y < x^3y$ ... $z < xz < x^2z$ ... $zy < zyx < zyx^2$, etc.
Given a monomial ordering on a polynomial, if the polynomial is finite, than there exists a term of the polynomial such that it is the "biggest" monomial in the ordering. We denote this term by $LT_<(p)$. Now lets denote the ideal generated by the leading terms of all of the polynomials contained in the ideal I by $LT_<(I)$.
Definition: A Grobner Basis G is a subset $\{g_1, g_2, g_3...\}$ of an ideal I such that the ideal formed by taking the leading terms of elements in G can generate the ideal formed by $LT_<(I)$.
That's a pretty heavy definition, so let's look at a concrete example. Consider the ideal generated by $I = (x + y^2, xy + 1)$. If we set the monomial ordering $<$ such that $y < x$, this ideal by itself is not a Grobner basis. For example, the polynomial $y^3 - 1$ is contained in I. But if we look at the definition of a Grobner

basis, we note that (xy, x) must contain y^3, which is obviously false. However, the set $x + y^2, xy + 1, y^3 - 1$ can be shown to be a Grobner basis.
Now let's look at how Grobner basis can help us solve the Ideal Membership Problem.
Theorem: Let G be a Grobner basis of I, and let $f \in F[x_1, x_2, x_3 ...]$. Then there exists a unique polynomial $r \in F[x_1, x_2, x_3 ...]$. satisfying two conditions:

1. For every $g \in G$, $LT_< g$ is not a divisor of any term in r.
2. $f - r \in I$.

We sketch a proof. r is defined as the remainder of the General Division Algorithm using f as the dividend and G as the divisors. By definition, r satisfies both the 1st and 2nd conditions. We also need to show that r is unique, which can be done by assuming there exists another value of r and showing that the leading term of their difference violates the first condition, a contradiction.
This gives us an easy way to solve the Ideal Membership Problem: compute the Grobner basis of an ideal I and then apply Generalized Division to the function f: if $r = 0$, $f \in I$. Only problem is, we need to figure out how to form a Grobner basis.
Let's go over an algorithm that can allow us to compute a Grobner basis. First we need to define a special polynomial
Definition: An S-polynomial of polynomials f and g is defined by $S(f, g) = \frac{LT_<(g)f - LT_<(f)g}{GCD(LT_<(f), LT_<(g))}$.
We now state a theorem that will give us a way to test if a subset is a Grobner basis.
Theorem: A subset G is a Grobner basis if and only if $S(f, g)$ for $f, g \in G$ can all be represented by the ideal generated by G. Using this theorem as our testing condition, we can create an algorithm that generates a Grobner basis from any ideal I. This algorithm takes in a generator for an ideal I and outputs a Grobner basis of I.

1. Initialize a set G to be F, and initialize a set P which contains all pairs such that there elements are not identical and both elements are in F.
2. Check if $|P| > 0$: if it is, continue, if it is not, return G.
3. Choose a pair (a, b), and delete it from P. Now apply the Generalized Divisor Algorithm to $S(a, b)$.
4. Check if the remainder of Division Algorithm is 0. If it is nonzero, add $S(a, b)$ to G and add all pairs $(S(a, b), g)$, $g \in G$
5. Repeat step 2.

(This algorithm is also known as Buchberger's algorithm) Combining this algorithm with the Division Algorithm gives us a way to solve the algebraic portion of this problem.

3 Back to Geometry

Let's assume I have created a computer program that implements what I have discussed earlier. We can use this program to test if the theorem polynomial is in the ideal generated by the hypothesis polynomial. For example, consider the following theorem: If AB is a circle's diameter and C is any point on the circle, than $\angle ABC$ is a right angle.
To verify the theorem with our methods, we first put the configuration into the coordinate plane. Let $A = (0, 0)$, $B = (2r, 0)$ and $C = (p, q)$. The condition that C is on the circle is equivalent to the equation $A_1 = (p - r)^2 + q^2 - r^2$. Using perpendicular lines, we can show that the hypothesis polynomial is equivalent to $H_1 = q^2 + p(p - 2r)$. If we ask our machine whether $H_1 \in (A_1)$ in the ring $Q[p, q, r]$, it will return true. We can confirm this by hand.
Let's look at a more complicated theorem, the existence of the orthocenter. Let's have $C = (0, 0)$, $B = (b_1, 0)$, $A = (a_1, a_2)$. In addition, let's have $D = (d_1, d_2)$, where AD is perpendicular to BC. Similarly, we have $E = (e_1, e_2)$, $F = (f_1, f_2)$, where BE and CF are perpendicular to AC and AB respectively. Note that $D = (a_1, 0)$. Finally, we define $H = (h_1, h_2)$ to be the point that is the intersection of AD and CF. We

want to show that CF passes through H.
The hypothesis polynomials are

- $A_1 = a_2e_2 - a_1(e_1 - b_1)$ (AC perpendicular to BE)
- $A_2 = a_2e_1 - a_1e_2$ (E lies on AC)
- $A_3 = a_2f_2 - b_1f_1 + a_1f_1$ (CF perpendicular to AB)
- $A_4 = -a_2f_1 + a_2(b_1 - a_1) + a_2a_1 - l_2(b_1 - a_1)$ (F lies on AB)
- $A_5 = f_2h_1 - f_1h_2$ (H is on CF)
- $A_6 = h_1 - d_1$ (H is on AD)

Finally we have the theorem polynomial, which states that BE and H are collinear: (input later)
However if we check if H is contained in the ideal generated by the theorem polynomials, the machine will return false. This is due to the existence of degenerate cases. For example, the altitudes are not well defined if A and C are the same point. We have an ad-hoc solution to this problem: we look at whether the polynomial $Ha_1b_1a_2$ is in the ideal, which is true. This is due to the fact that the polynomial now factors in degenerate cases.

4 Works Used

http://www.math.kun.nl/ bosma/Students/KenMadlenerBscthesis.pdf
https://www.math.ucdavis.edu/ deloera/MISC/LA-BIBLIO/trunk/RecioTomas/Recio1.pdf
https://math.berkeley.edu/ lpachter/239/$02_04_2008_math239.pdf$
$http://people.csail.mit.edu/madhu/ST12/scribe/lect15.pdf$