Proof and Computation in Geometry

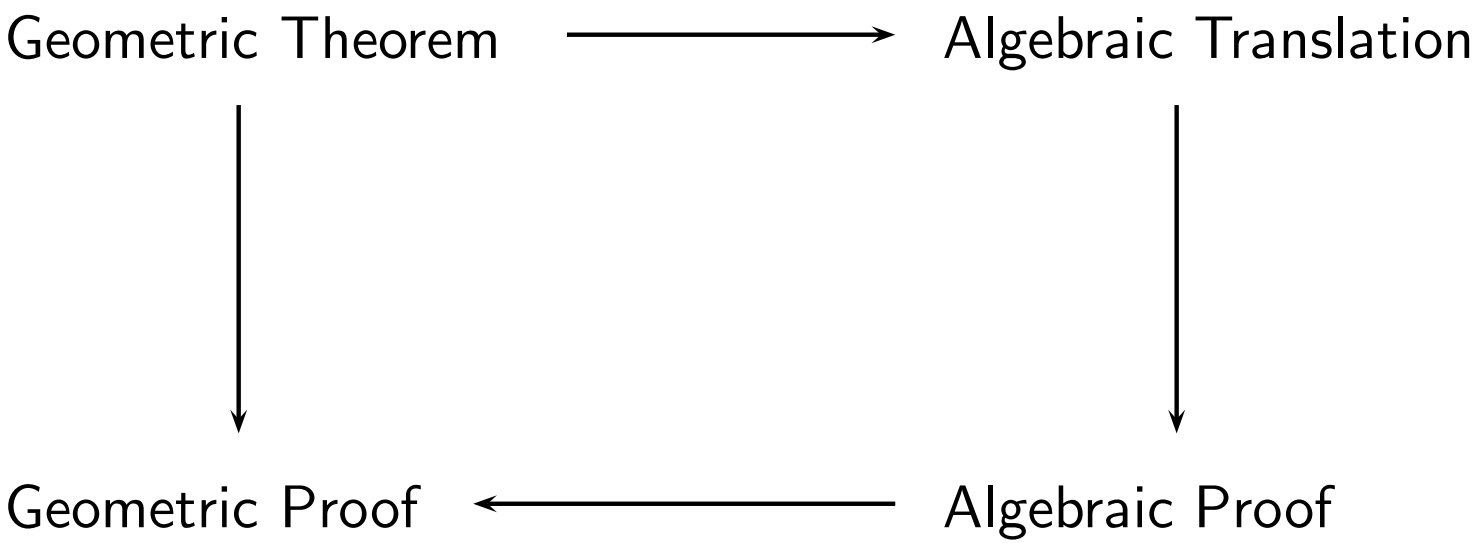
Michael Beeson

September 17, 2012

Proof and Computation

- Analytic geometry is more systematic than Euclid. It reduces geometry to calculation.
- First-order proofs are objects of beauty in their own right, but they are hard to come up with.
- A computation tells you *that* something is true.
  A proof tells you *why* it's true.
- We will study the reduction(s) of proof to computation, and then try to reverse the process, getting proofs from computations.

A commutative diagram, in theory

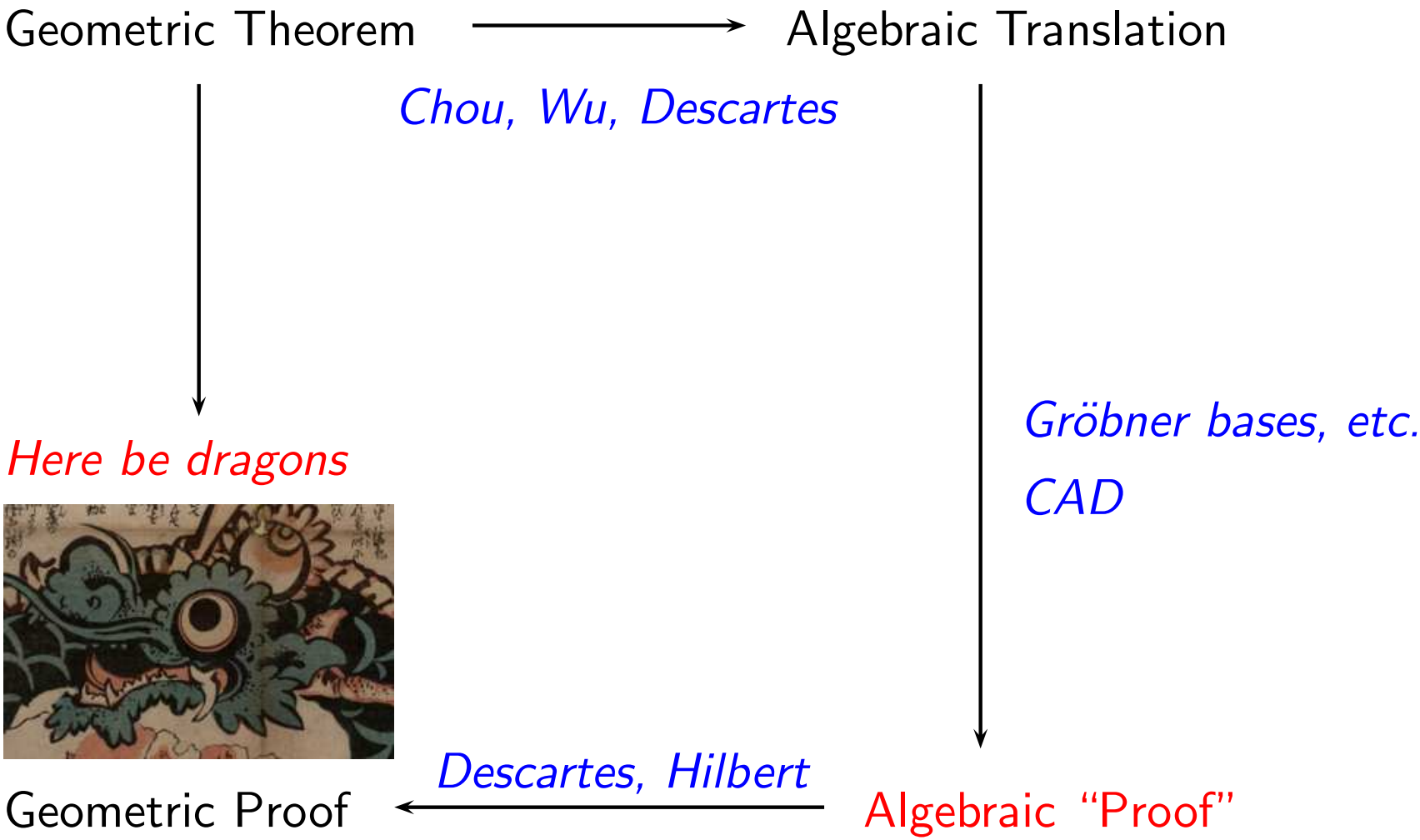


Yogi Berra said

In theory, there is no difference between theory and practice.

In practice, there is.

That commutative diagram, in practice



Let's get around the dragons by going across the bottom.

Outline of the talk

- We will focus on Euclidean ruler-and-compass geometry EG.
- We want to know if a given theorem is provable in EG, and to find a proof if it is.
- How far can we get proving geometry theorems with a theorem prover? (left side of the diagram, fight the dragons directly!)
- How far can we get by computations towards deciding such problems? (right side of the diagram)
- How can we convert computations into verified computations? (right side of the diagram)
- How can we convert verified computations into geometrical proofs? (bottom of the diagram)

First order theories of geometry

- Angles can be treated as ordered triples of points.
- Rays and segments are needed only for visual effect; for theory we need only points, lines, and circles.
- We don't even need lines and circles; every theorem comes down to constructing some points from given points, so that the constructed points bear certain relations to the original points.
- The relations in question can be expressed in terms of *betweenness* and *equidistance*.

Tarski geometry and Hilbert geometry

Just to avoid confusion: today we are concerned with "elementary" geometry in the sense that only line-circle and circle-circle continuity are used. Hilbert's geometry included a second-order continuity axiom; we may compare it to requiring that Dedekind cuts be filled, although Hilbert formulated it differently.

"Tarski geometry" is a first-order theory with a continuity schema, essentially requiring that first-order definable Dedekind cuts be filled. Sometimes "elementary" means first-order, and Tarski wrote a famous paper, *What is Elementary Geometry*, in which "elementary geometry" meant Tarski geometry. But "elementary" can also refer to the *Elements* of Euclid, which is a weaker theory.

Issues in the axiomatization of geometry

- What are the primitive sorts of the theory?
- What are the primitive relations?
- What (if any) are the function symbols?
- What are the continuity axioms?
- How is congruence of angles defined?
- How is the SAS principle built into the axioms?
- How close are the axioms to Euclid?
- Are the axioms few and elegant, or numerous and powerful?
- Are the axioms strictly first-order?

Various axiomatizations of geometry

Axiomatizations have been given by Veblen, Pieri, Hilbert, Tarski, Borsuk and Szmielew, and Szmielew, and that list is by no means comprehensive. Nearly every possible combination of answers to the "issues" has something to recommend it. For example, Hilbert has several sorts, and his axioms are not strictly first-order; Tarski has only one sort (points) and ten axioms. My theories ECG and EG have points, lines, and circles, and function symbols so that their axioms are quantifier-free and disjunction-free.

It is a lot of work to develop geometry constructively from ten or so axioms about points, but very elegant. In the experiments I describe today, I used Tarski's axioms. (Fewer primitives is easier for a theorem-prover; but it may be harder to get started.)

The model-theoretic view

A euclidean field is an ordered field in which every square has a square root; equivalently, a field in which every element is a square or minus a square, every element of the form $1 + x^2$ is a square, and -1 is not a square.

If $\mathbb{F}$ is a euclidean field, then using analytic geometry we can expand $\mathbb{F}^2$ to a model of geometry.

Descartes and Hilbert showed, by giving geometric definitions of addition and multiplication, that every model of Euclidean geometry is of the form $\mathbb{F}^2$, where $\mathbb{F}$ is a euclidean field.

Similarly every model of Tarski geometry is $\mathbb{F}^2$, where $\mathbb{F}$ is real-closed.

The Tarski field $\mathbb{T}$

- $\mathbb{T}$ is the least subfield of the reals closed under square roots of positive elements.
- T^2 is the minimal model of ruler-and-compass, or Euclidean, geometry EG.
- T consists of all real algebraic numbers whose degree over $\mathbb{Q}$ is a power of 2. It is not of finite degree over $\mathbb{Q}$.

Decidability issues

- Gödel: Proof can't always be reduced to computation
- Tarski: But in algebra and geometry, it can.
- Rabin-Fischler: But not efficiently. Any decision procedure is at least double-exponential (in the number of variables).
- Julia Robinson: $\mathbb{Q}$ is undecidable.
- Ziegler: any finitely axiomatizable extension of field theory is undecidable–in particular the theory of euclidean fields. His proof shows the AEA fragment is undecidable.
- Tarski's conjecture: The minimal model of ruler-and-compass geometry, $\mathbb{T}^2$, is undecidable.
- Conjecture: Euclidean geometry (the AE fragment of Tarski geometry) is decidable.

Euclid lies in the AE fragment

Euclid's theorems have the form,

- Given some points bearing certain relations to each other, there exist (one can construct) certain other points bearing specified relations to the original points and to each other.
- The case where no additional points are constructed is allowed.
- The points are to be constructed with ruler and compass, by constructing a series of auxiliary points.
- Constructed points are given by terms of EG, built up from $IntersectLines$, $IntersectLineCircle1$, etc.
- The auxiliary points are their subterms.
- Such theorems translate into the AE fragment of field theory.

Decidability of Euclidean geometry

- Although Tarski geometry (with first-order full continuity) is decidable, it does not follow that ruler-and-compass geometry (with only line-circle continuity), which we are here calling Euclidean geometry, or even its AE fragment, is decidable.
- The AEA fragment is undecidable, by Ziegler's proof.
- Is there an algorithm for deciding of an AE statement whether it is a theorem of Euclidean geometry?
- This is equivalent to asking if there is an algorithm for deciding whether an AE statement of field theory is provable in euclidean field theory (i.e. true in all euclidean fields).

An *a priori* bound on the number of auxiliary points?

Consider the class of geometrical problems of the form, given n points and some relations between them, can you construct k more points satisfying some relations with each other and the original points? If you can do so, you may need to construct a number of auxiliary points to achieve the desired result.

- Can one give an *a priori* bound on the number of auxiliary points that will suffice? The bound should depend only on n and k.
- Such a bound $f(n, k)$ would give us a decision procedure, because there are a finite number of ways to construct at most $f(n, k)$ points, and we can "just try them all", and test whether the result is achieved.
- Conversely, if we have such a decision procedure, we can apply it, and if it says the problem is solvable, we count the number of auxiliary points; and if it says the problem is not solvable, we can take any number for the bound.

Decision procedures for a theory *versus* for $\mathbb{R}^2$

A decision procedure for the AE fragment gives us an a priori *bound on the number of auxiliary points needed for a Euclidean construction, and vice versa.*

The proof of that equivalence is a straightforward application of the following well-known theorems:

- cut elimination
- Artin's theorem that every ordered field has a real closure
- Tarski's theorem that all real closed fields are elementary equivalent.

Even though the proof is short, each of these three theorems is a "big gun", so the equivalence is in some sense a deep result.

Recall the road map of this talk

Geometric Theorem → Algebraic Translation

Chou, Wu, Descartes

Here be dragons

Gröbner bases, etc.

CAD

Geometric Proof ← *Descartes, Hilbert* ← Algebraic "Proof"

Coming up with proofs

Down the left side of the diagram (and fight the dragons)

- Pencil and paper
- Proof checkers
- Theorem provers

Around the dragons to the right

- translate geometry to algebra (across the top)
- Decision methods, Gröbner bases, etc. (down the right side)
- Back-translation from calculation (left across the bottom)

Proofs in Geometry

Thales	600 BC
Euclid	300 BC
Descartes	1637
Pieri	1899
Hilbert	1899-1908
Borsuk-Szmielew	1960
Tarski	1941-65
Gupta	1965
Szmielew	1965-1976
Gelernter	1960
Quaife	1990
Narboux	2006
Avigad, Dean, and Mumma	2006

Computation

Descartes	1637
Wu	1976-88
Chou	1988–93
Chou, Gao, and Zhang	1993
Kapur	1986–1990
Ko	1988–89
Kutzler and Stifter	1986–88

A challenge

Get first-order proofs of geometrical theorems:

- Those in Szmielew's work and Quaife's work
- Those in Euclid
- Those in Chou's book

Tarski's language

There is only one sort of variables, for points.

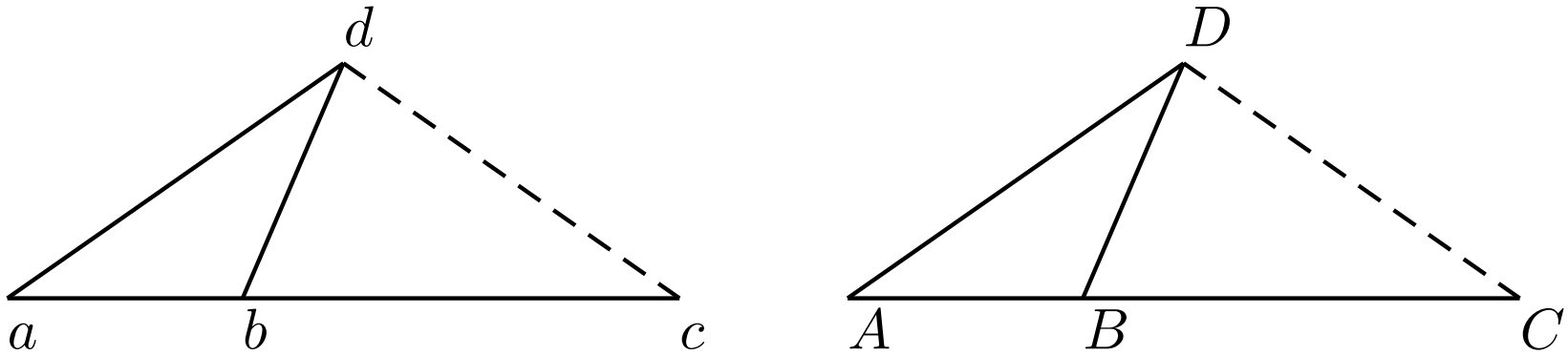
The primitive notions are betweenness and equidistance.

$T(a,b,c)$	b is non-strictly between a and c
$E(a,b,c,d)$	segment ab is congruent to segment cd
$ab \equiv cd$	human notation for $E(a,b,c,d)$

Hilbert, Pasch, Veblen, and I used strict betweenness $B(a,b,c)$.

Eliminating angle congruence

- Hilbert treated angles as primitive objects and angle congruence as a primitive relation.
- The idea to define these notions (instead of take them as primitive) goes back (at least) to J. Mollerup (1903), but he attributes it to Veronese.
- The key idea is the "five-segment axiom" (A5):



If the four solid segments are pairwise congruent then the fifth (dotted) segments are congruent too. This is essentially SAS for triangles dbc and DBC.

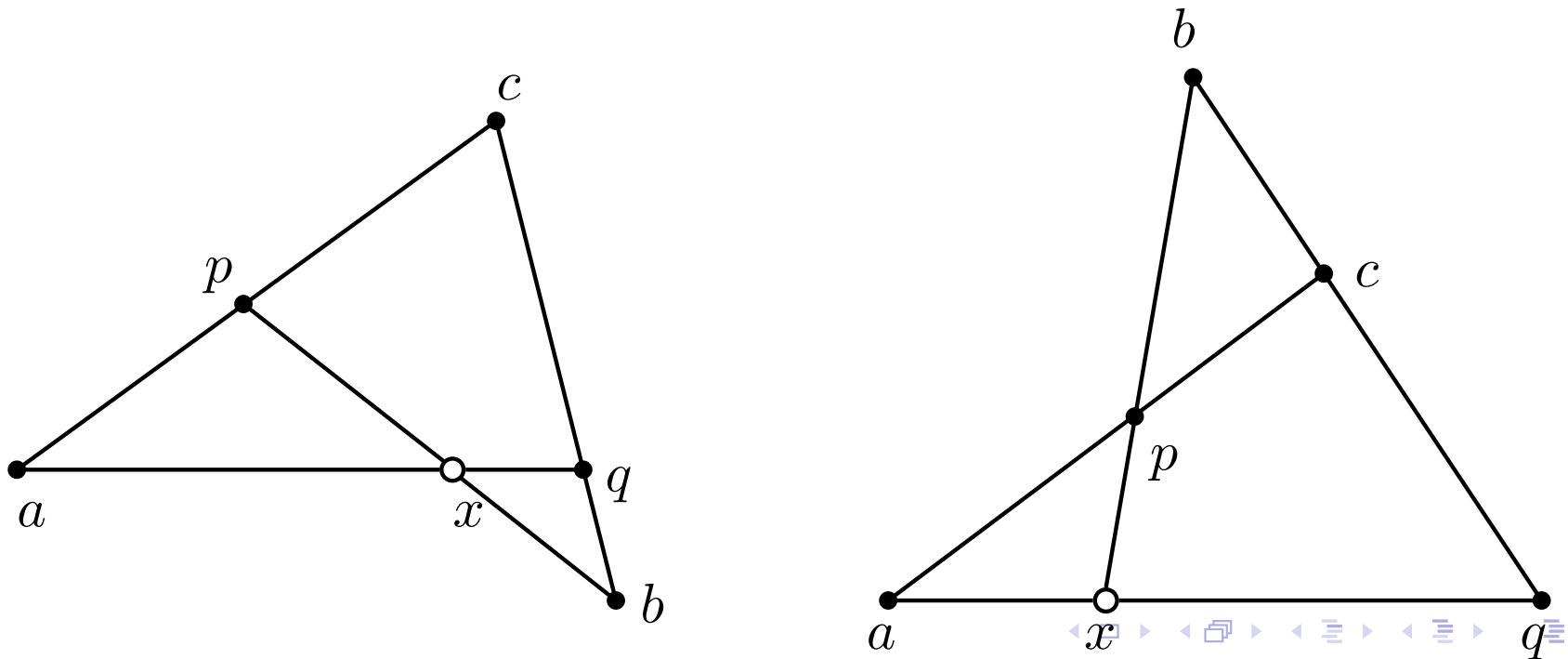
Tarski's first six axioms

$uv \equiv vu$	(A1)
$uv \equiv wx \wedge uv \equiv yz \rightarrow wx \equiv yz$	(A2)
$uv \equiv ww \rightarrow u = v$	(A3)
$T(u, v, ext(u, v, w, x))$	(A4), segment extension
Five-segment axiom	(A5), a form of SAS
$T(u, v, u) \rightarrow u = v$	(A6)

Pasch's axiom (1882)

As Pasch formulated it, it is not in AE form. There are two AE versions that go back to Veblen (1904), who proved outer Pasch implies inner Pasch. Gupta (1965) proved inner Pasch implies outer Pasch. After that Tarski's system used inner Pasch as axiom (A7) and dropped outer Pasch.

Figure: Inner Pasch (left) and Outer Pasch (right). Line pb meets triangle acq in one side. The open circles show the points asserted to exist on the other side.



Gupta's 1965 thesis

In his 1965 thesis under Tarski, H. N. Gupta proved two great theorems:

- Inner Pasch implies outer Pasch.
- Connectivity of Betweenness:

$$a \neq b \wedge T(a,b,c) \wedge T(a,b,d) \Rightarrow T(a,c,d) \vee T(a,d,c).$$

- That is, betweenness determines a linear order of points on a line. Points d and c, both to the right of b on $Line(a,b)$, must be comparable.
- Taken as an axiom by Tarski before Gupta.
- The proof is complicated. It uses 8 auxiliary points and more than 70 inferences, and uses all the axioms A1-A7.
- Gupta got his Ph. D. sixteen years after his second master's degree.

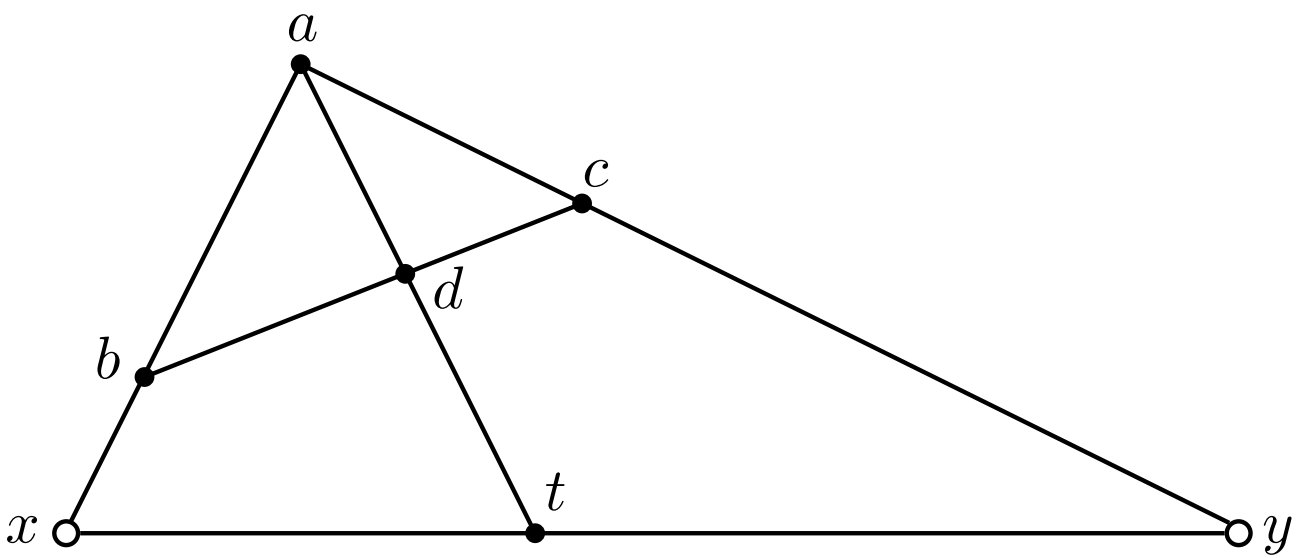
Dimension Axioms

(A8) (lower dimension axiom) says there are three non collinear points (none of them is between the other two)

(A9) (upper dimension axiom) says that any three points equidistant from two distinct points must be collinear. In other words, the locus of points equidistant from a and b is a line (not a plane as it would be in $\mathbb{R}^3$).

(A1) through (A9) are the axioms for "Hilbert planes."

Tarski's Parallel Axiom (A10)



- Open circles indicate points asserted to exist.
- There are many other equivalent forms, including at least one with no existential quantifiers.

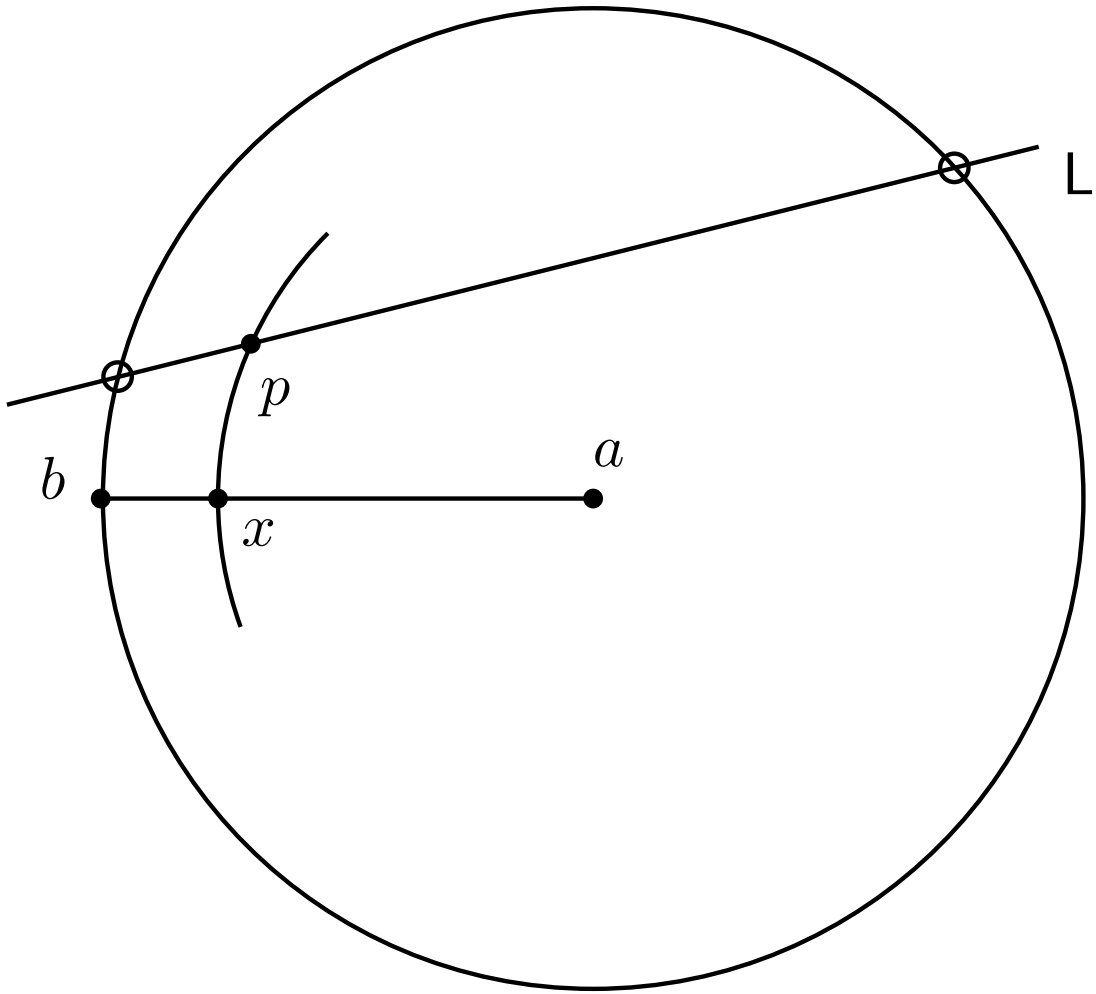
Continuity

- Tarski took the full first-order continuity scheme, similar to definable Dedekind cuts.
- We consider "Euclidean" continuity axioms, though Euclid didn't notice he needed them.
- Line-circle continuity says that if line L has a point inside circle C then L meets C.
- Circle-circle continuity says that if circle K has a point inside, and a point outside, circle C then it meets C.

But what is "inside" in Tarski's theory?

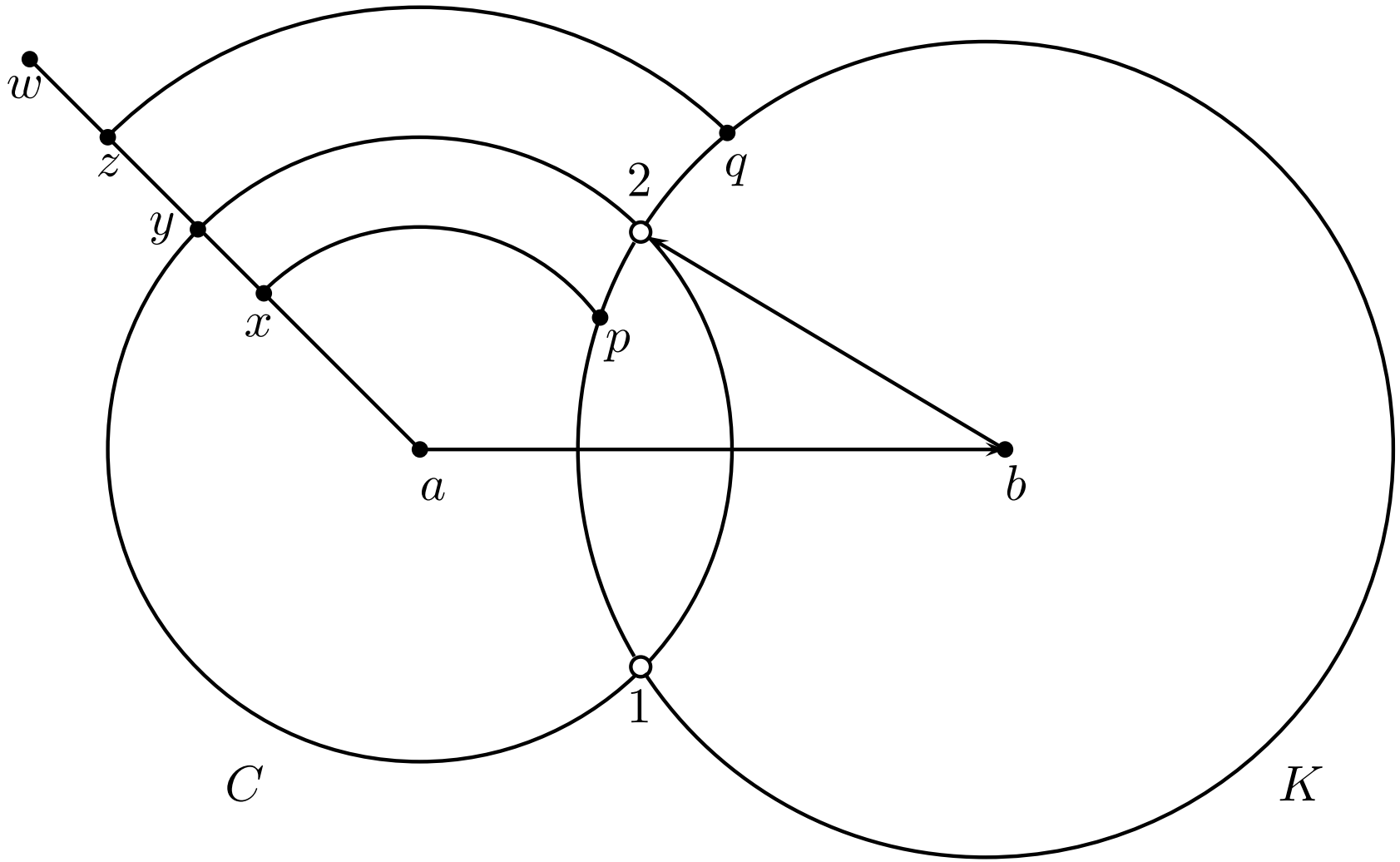
Line-circle continuity

Figure: Line-circle continuity



Circle-circle continuity

Figure: Circle-circle continuity. p is inside C and q is outside C, as witnessed by x, y, and z, so the intersection points 1 and 2 exist.



Line-circle *versus* Circle-circle

- Circle-circle continuity implies line-circle continuity using A1-A9.
- Line-circle continuity implies circle-circle continuity using A1-A9 *but no first-order proof is known*!
- *There is a challenge for automated deduction in geometry!*
- With the aid of the parallel postulate (A10), the proof by analytic geometry could, in theory, be used with back-translation to get a first-order proof.
- Without (A10) that method is not even in theory available.
- The known proof is model-theoretic, via the Pejas classification of Hilbert planes.

Szmielew's Development from Tarski's Axioms

- The formal development of geometry in Tarski's theory was carried out by Szmielew in her course at UC Berkeley, 1965.
- Important contributions were made by Gupta in his 1965 Ph. D. thesis, which was never published.
- Szmielew's lectures were finally published in 1983 in Part I of the book by Schwabhäuser, Szmielew, and Tarski (recently reprinted by Ishi Press). Chapters 2 through 16 contain theorems.
- Narboux (2006) checked the proofs through Chapter 12 in Coq. So we have first-order proofs in that sense.

A direct attack

How far can one get in 2012 using a modern resolution theorem prover? Larry Wos and I conducted three (still continuing) experiments using Otter and Prover 9:

- Szmielew's development from Tarski's axioms
- Quaife's work and challenge problems from 1990
- Euclid

Szmielew in Otter

- Larry Wos and I experimented with going through Szmielew's development, making each theorem into an Otter file, giving Otter the previously proved theorems to use. The hypothesis to be tested was
- A good theorem prover can prove most of those theorems, at least it can if you give it the diagram as well as the statement of the theorem.
- You give it the diagram by defining a name for each of the points that need to be constructed.
- Then those terms get the same weight as an atom and formulas involving them are more likely to be used.)
- That amounts to giving the prover the statement of the theorem, and the diagram.

What happened (so far–we're still working on this)

- We had to tell Otter the names of constructed points.
- Then we roared through Chapters 2 and 3.
- We hit a snag at Satz 4.2. An argument by cases according as $a = c$ or $a \neq c$ is used. Otter could do each case, but not the whole theorem!
- Prover 9 could do it without help, but it took 67,000 seconds! (1 day = 86,400 sec.)
- The inability to argue by cases is a well-known problem in resolution theorem-proving. On five or six (out of many) subsequent theorems, we had to help Otter with arguments by cases.
- We did that by putting in the case split explicitly, and giving the cases low weights. For example we would put in `b=c | b!=c` and then give both literals a negative weight. With this trick, if the cases can be done in separate runs, then we can get a proof in a single run.

Gupta's theorem proved using Otter

- Chapter 5 contains a difficult theorem from Gupta's thesis, the connectivity of betweenness.
- Recall: $a \neq b \wedge Babc \wedge Babd \rightarrow Bacd \vee Badc$.
- Otter and Prover9 could not prove Gupta's theorem without help.
- We put Gupta's proof steps (about thirty of them) in as preliminary goals. We got proofs of some of them. We gave the steps of those proofs low weight, so similar formulas would be kept and used. Wos calls this technique "resonators".
- We got a 122-step proof of Gupta's theorem.
- By continued efforts, we eventually got a 73-step proof.

Otter's new proof of Gupta's theorem

- Otter did not just find Gupta's proof whose steps we had used as resonators.
- Otter's proof contains only about half of those proof steps, and it contains some steps that are not in Gupta's proof.
- It even contains some congruences between segments that are not considered in Gupta's proof.
- By the way, Gupta's proof mentions a total of twelve points, forming a complicated diagram that cannot even be sensibly drawn as one diagram, because it diagrams an impossible situation for proof by contradiction.
- Both proofs are hard for a human to "understand", although they are not too long to check line-by-line.

Work in Progress

- After Gupta's theorem, we had no further difficulties with the rest of Chapters 5 and 6; Otter required no help except a couple of case splits.
- We intend to continue this project in October.
- In Chapter 7 we will prove the existence of a midpoint (without using circles) *a la* Gupta.

Quaife revisited in 2012

- Quaife made it approximately to where Wos and I hit our first snag in Szmielew.
- His most difficult example was that the diagonals of a "rectangle" bisect each other. But here a "rectangle" is a quadrilateral with two opposite sides equal and the diagonals equal.
- Most of Quaife's theorems are in Szmielew Chapters 2 and 3, or the first part of 4, or are similar to such theorems, but use some defined notions such as "reflection."
- Wos and I could easily prove them all.

Quaife's first challenge problem

Quaife left four challenge problems. One of them is the connectivity of betweenness, Satz 5.1 in Szmielew. So, in 2012 we can do what Quaife could not do in 1990. There are two factors that might be suggested to account for that:

- Computers run faster and have larger memories in 2012 than in 1990.
- We know some techniques for using Otter that Quaife didn't know, specifically resonators, hints, and the hot list. We used these techniques both for proof discovery and for proof shortening.
- Which factor is more important?
- Maybe we could have found the proofs we found with 1990 computers and 2012 techniques, but we're glad we didn't have to.
- We didn't find the proof with a 2012 computer and a 1990 technique.

Quaife's other challenge problems

Two of them are Gupta's other theorems:

- midpoint without using circles
- inner Pasch implies outer Pasch

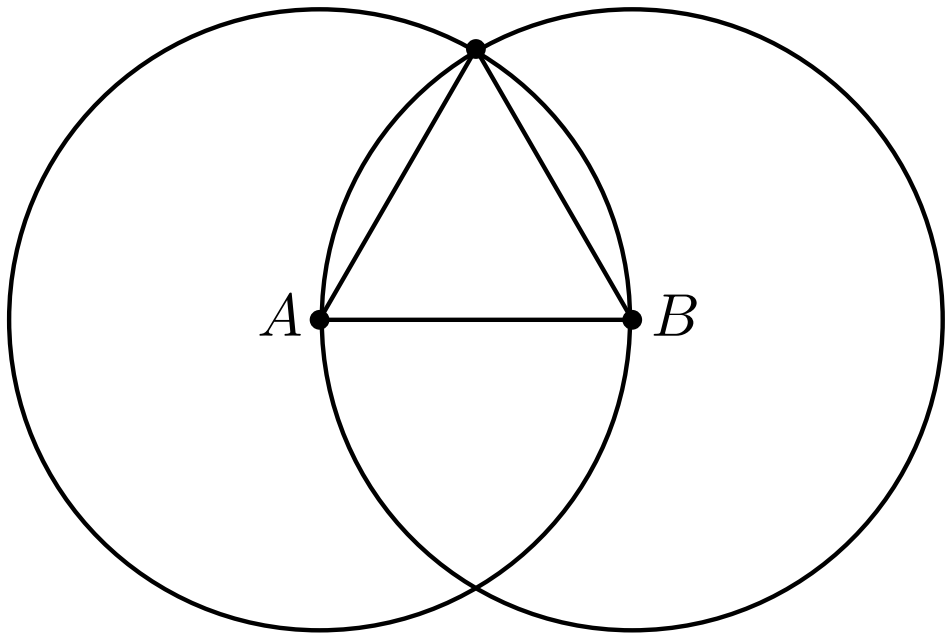
The third goes back to Hilbert:

- Construct an equilateral triangle without using circles

We haven't proved these yet with our methods but are confident we can do it.

Euclid

Book I, Prop. 1. constructs an equilateral triangle.



Why do the two circles meet?

Euclid from Tarski?

- Quaife did not get as far as proving any theorem about circles.
- Neither did Szmielew or Gupta.
- As of summer 2012, neither by hand nor by machine had development from Tarski's axioms reached the first proposition of Euclid, more than half a century after Tarski formulated his axioms.

Euclid I.1 from Tarski

- To prove I.1 we will need the circle-circle continuity axiom.
- *A priori* it seems we might need the upper dimension axiom, too, but we don't. Circle-circle continuity is sphere-sphere continuity in $\mathbb{R}^3$.
- Otter proves Euclid I.1 from circle-circle continuity in less than two seconds, with a good choice of inference rules.
- When we first did it, it took eleven minutes.
- That's about how long it will take you by hand.

Euclid and Tarski

- I.2 is immediate from Tarski's extension axiom; Euclid only postulated you can extend a segment *somehow*.
- I.3 defines $\leq$; it is not a theorem.
- I.4 is the SAS congruence criterion. That requires defining angle congruence; it is Satz 11.4 in Szmielew!
- Angle congruence and indeed comparison of angles ($\leq$ for angles) are primitive in Euclid, but defined in Tarski's system.

The resulting complications have little to do with automated deduction. They are the consequence of choosing a very parsimonious formal language.

Therefore, we should complete Szmielew Chapter 11 first, or take some axioms about comparison and congruence of angles, in order to formalize Euclid directly.

The road map again

Geometric Theorem → Algebraic Translation

Chou, Wu, Descartes

Here be dragons

Gröbner bases, etc.

CAD

Geometric Proof ← *Descartes, Hilbert* ← Algebraic "Proof"

Proof by computation, in theory

- Start with a geometry theorem.
- Express it as algebraic equations (or inequalities) using analytic geometry, introducing new variables for the coordinates of the points to be constructed.
- Calculate to see if these equations can be satisfied.
- If so, then you have a proof in some sense.
- But you still don't have a first-order proof.

Proof by computation, in practice

- CAD decomposition breaks down on five or six variables.
- No new theorem proved by CAD
- Wu's method
- Chou's area method
- These methods proved hundreds of beautiful theorems!
- In that sense, they far outperformed resolution theorem proving.
- I am about to complain about what they *can't* do–but I stand in awe of what they *can* do.

Some defects of Wu's and Chou's methods

- Both these methods work only on theorems that translate to algebra using equations, with no inequalities. Thus the "simple" betweenness theorems of Szmielew Chapter 3 are out-of-scope.
- You can't ask for a proof from ruler-and-compass axioms. You can only ask if the theorem is true in $\mathbb{R}^2$.
- Thus there is no problem trisecting an angle; this is not about ruler-and-compass geometry.
- A proposition like Euclid I.1 is just trivial: all the subtleties and beauties of the first-order proof are not captured by these methods. It just computes algebraically that there is a point on both circles.
- In short, we're not doing geometry. We're doing algebra.

How can we bridge the gap?

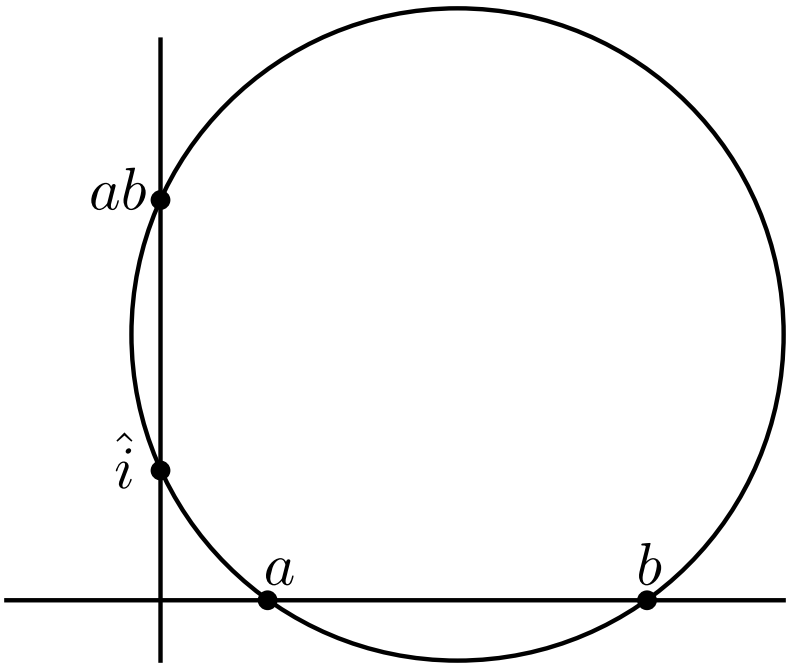
Down the right and left across the bottom of the road map.

- Formalize the translation from geometry to algebra.
- Take the quotes off "proof" in the lower right: algebraic "proof" must become algebraic proof. That is: Figure out how to convert the algebra performed by Chou's method into first-order proofs of algebraic theorems, from some algebraic axioms.
- Back-translate to geometry, using the geometric definitions of addition and multiplication.
- In theory this can certainly be done.
- How about in practice?

Defining arithmetic in geometry

Descartes showed how to define multiplication and addition of *positive* numbers in geometry. Hilbert gave a different definition of multiplication, but it needs the same hard work to justify it.

- Addition translates into segment "insertion" (extension for positive elements).
- Multiplication, as defined by Hilbert, works like this:



Model-theoretic conclusions

- By Descartes and Hilbert, models of Euclidean geometries (A1-A10) are $\mathbb{F}^2$ where $\mathbb{F}$ is an ordered field.
- Line-circle and circle-circle continuity axioms correspond to euclidean fields.
- That characterization does not help us find proofs.

Models and interpretations

- In general model-theoretic arguments are looked at by proof theorists as "interpretations."
- An interpretation maps formulas of the source theory into formulas of the target theory, preserving provability.

$$\vdash \phi \;\Rightarrow\; \vdash \hat{\phi}$$

- Usually the proof also shows how to transform the proofs efficiently. We have interpretations from geometry to field theory that express the model theory.

Advantage of Interpretations over Models

- An interpretation enables you to translate proofs from one theory to the other.
- I wrote out the details of the interpretations between geometry and field theory, because I was working on constructive geometry, where model theory is not available.
- There are dozens of pages of details.
- Model theory is easier, but proof theory is more informative.

Proofs by computation?

- In theory, then, we could get a proof from geometric axioms out of a computation.
- In practice, Chou was aware of this, but he says, "I know of no single theorem proved in this way."

Geometry to algebra–two approaches

The top arrow of the road map.

Cartesian analytic geometry:

- Coordinatize every point.
- Convert segment congruence to equations.
- Convert betweenness to inequalities.

Chou's area method:

- position ratios, signed areas, Pythagorean differences.
- Co-side theorem, co-angle theorem, etc.
- Works well for theorems asserting coincidence or collinearity.
- Equations, not inequalities.

Vector Geometry

A formal framework encompassing both computation and proof.

- A first-order theory VG that contains both geometry and algebra.
- In VG we can formalize the translation in both directions.
- The whole diagram of geometry and algebra, proof and (algebraic) computation, can be formalized in VG.

Language of Vector Geometry

Three sorts:

- points p, q, a, b
- scalars α, β, λ, s, t
- vectors $\mathbf{u}$, $\mathbf{v}$

Intuitively you may think of vectors as equivalence classes of directed line segments under the equivalence relation of parallel transport. Constructors and accessors:

- $p \circ q$ is a vector.
- scalar multiplication: $\lambda\mathbf{u}$ is a vector
- dot product: $\mathbf{u} \cdot \mathbf{v}$ is a scalar
- cross product: $\mathbf{u} \times \mathbf{v}$ is a scalar (not a vector, we are in two dimensions)

Language of Vector Geometry

Relations:

- betweenness and equidistance from Tarski's language
- Equality for points, equality for vectors, equality for scalars. Technically these are different symbols.
- $x < y$ for scalars.

Function symbols (other than constructors and accessors) and constants:

- Skolem symbols for Tarski's language, e.g. ext, ip, ic.
- $0, 1, *, +, /$, unary and binary $-$, and $\sqrt{}$ for scalars.
- $\mathbf{0}$ is a vector; $\mathbf{u} + \mathbf{v}$, $\mathbf{u} - v$, and $-\mathbf{u}$ are vectors.
- $\hat{0}$, $\hat{1}$, and $\hat{i}$ are unequal points.
- $\hat{i}$, a point equidistant from 1 and from $-1 = ext(1, 0, 0, 1)$.

Division by zero

$1/0$ is "some scalar" rather than "undefined", because we want to use theorem provers with this language and they don't use the logic of partial terms. You can't prove anything about $1/0$ so it doesn't matter that it has some undetermined value. Other "undefined" terms are treated the same way.

You have the axiom $x \neq 0 \rightarrow x * (1/x) = 1$, not the axiom $x * (1/x) = 1$.

Axioms of Vector Geometry

- Tarski's axioms for ruler-and-compass geometry.
- The scalars form a euclidean field.
- The obvious axioms for $-$ and $/$ and $\sqrt{}$
- The vectors form a vector space over the scalars.
- The usual laws for dot product and 2d cross product.
- $a \circ b = -b \circ a$
- $p \circ p = \mathbf{0}$
- $E(\hat{0}, \hat{i}, \hat{0}, \hat{1})$
- $E(\hat{i}, \hat{1}, \hat{i}, -\hat{1})$ where $-\hat{1} = ext(\hat{1}, \hat{0}, \hat{1}, \hat{0})$
- If ab and cd are parallel and congruent then $a \circ b = \pm c \circ d$, with the sign depending on whether ad intersects bc or not.
- If a, b, c, and d are collinear and ab and cd are congruent, then $a \circ b = \pm c \circ d$, with the appropriate sign (given by betweenness conditions).

From computation to proof

Around the dragons, all inside the theory VG.

The plan:

- Start with a geometric theorem ϕ to be proved.
- Do the analytic geometry to compute $\hat{\phi}$. (By Chou or Descartes)
- Prove $\phi \leftrightarrow \hat{\phi}$.
- Find (e.g. by Chou's program or by hand) an informal proof that $\hat{\phi}$ is true, by calculation.
- Get a formal proof in VG of $\hat{\phi}$, i.e., verify the calculation.
- Combine it with the proof of $\hat{\phi} \rightarrow \phi$ to get a proof of ϕ.
- Eliminate the non-geometrical axioms to get a proof of ϕ.

Analytic geometry in VG

Across the top of the road map

- Let ϕ be a formula of EG. Let $\hat{\phi}$ be its translation into field theory (expressed using scalar variables in VG).
- Then VG proves $\phi \leftrightarrow \hat{\phi}$. If ϕ is AE, so is $\hat{\phi}$.
- There may be more than one way to compute a translation $\hat{\phi}$.
- We want a way that makes it as easy as possible to find proofs that $\phi \rightarrow \hat{\phi}$ and $\hat{\phi} \rightarrow \phi$.

Chou's method formalizable in VG

Across the top by Chou instead of Descartes

- The position ratio:

$$\frac{ab}{cd} := pr(a,b,c,d) = \frac{(a \circ b) \cdot (c \circ d)}{(c \circ d) \cdot (c \circ d)}$$

  Our pr is defined whenever $c \neq d$. Chou's is defined only when a, b, c, and d are collinear, but in that case they agree.

- The signed area of an oriented triangle is defined by

$$\mathcal{A}(p,q,r) := \frac{1}{2}(q \circ p) \times (q \circ r).$$

- Chou's other important concepts and theorems can also be defined and proved in VG.
- This should be checked by machine.

Algebra in VG

Down the right side of the road map

If t and s are terms of euclidean field theory (with the larger language of scalars in VG), and t are s are computationally equal using the usual laws of algebra, then they are provably equal in euclidean field theory, and hence in VG.

That is, computations arising from Euclidean theorems can be verified in VG.

Formalizing the back-translation

Left across the bottom of the road map

- Find proofs from Tarski's axioms of the laws of field theory, using the geometrical definitions of addition and multiplication.
- This uses the hardest theorem that Szmielew got to, namely the theorem of Pappus (or Pascal as Hilbert called it).
- Even the commutativity of addition is not completely trivial.
- Chapter 15 of Szmielew has the details.
- Nobody has yet done it before 2012 with a theorem prover or a proof checker.
- Narboux didn't get that far in 2006, but he's speaking at this conference.
- Wos and I didn't get that far.
- This really should be done. *Accio Firebolt! (Harry Potter flew over the dragons on his Firebolt.)*

A test case: the centroid theorem (medians all meet)

- Probably possible to get a proof directly, but not easy.
- Anyway, a good test case for the computation-to-proof paradigm.
- Chou's algebraic proof comparatively simple
- Cartesian analytic geometry not very complicated either.
- Formalize the geometry-to-algebra reasoning in VG.
- Formalize the algebraic computation in VG.
- Carry out the back-translation and get a formal proof in EG.
- Shorten that long proof using Wos's proof-shortening techniques.
- Would the resulting proof be beautiful, or a mess?