Algorithms and Proofs in Geometry

Michael Beeson

Stanford, Feb. 2008

www.MichaelBeeson.com/Research
Michael.Beeson@sjsu.edu

Euclid in Proclus’s words (450 CE)

- Euclid … put together the "Elements", arranging in order many of Eudoxus's theorems, perfecting many of Theaetetus's, and also bringing to irrefutable demonstration the things which had been only loosely proved by his predecessors. This man lived in the time of the first Ptolemy; for Archimedes, who followed closely upon the first Ptolemy makes mention of Euclid, and further they say that Ptolemy once asked him if there were a shorter way to study geometry than the Elements, to which he replied that there was no royal road to geometry. He is therefore younger than Plato's circle, but older than Eratosthenes and Archimedes; for these were contemporaries, as Eratosthenes somewhere says. In his aim he was a Platonist, being in sympathy with this philosophy, whence he made the end of the whole "Elements" the construction of the so-called Platonic figures.

Pythagoras and Euclid

- The first “foundational crisis” was the discovery of the irrationality of $\sqrt{2}$.
- Euclid’s *Elements* are to Pythagoras as *Principia Mathematica* is to Russell’s paradox.
- This according to Max Dehn, *Die Grundlegung der Geometrie in Historischer Entwicklung,* in Moritz Pasch’s *Vorlesungen über Neuere Geometrie.*

Postulates *vs.* Axioms in Euclid (also according to Max Dehn)

- Postulates set forth our abilities to make certain constructions.
- Axioms merely state (static) properties
- Aristotle and Proclus offer different explanations of the difference, but I like Dehn's explanation.
- The idea is not Dehn's but is already attributed to Geminus by Proclus.
- Example: (Postulate 3) *To describe a circle with any center and distance.*

The Parallel Postulate

- As an axiom: *Given a line L and a point P not on L, there exists exactly one line through P that does not meet L.*
- As Postulate 5 [Heath translation]: *If a straight line falling on two straight lines make the interior angles on the same side less than two right angles, the two straight lines, if produced indefinitely, meet on that side on which are the angles less than the two right angles.*

Euclid’s 48 Constructions

- The last book culminates in the construction of the Pythagorean solids
- 38 of these are in Books I-IV
- We will study the foundations today so the first ten constructions are more than enough.

Four views of Euclid's constructions

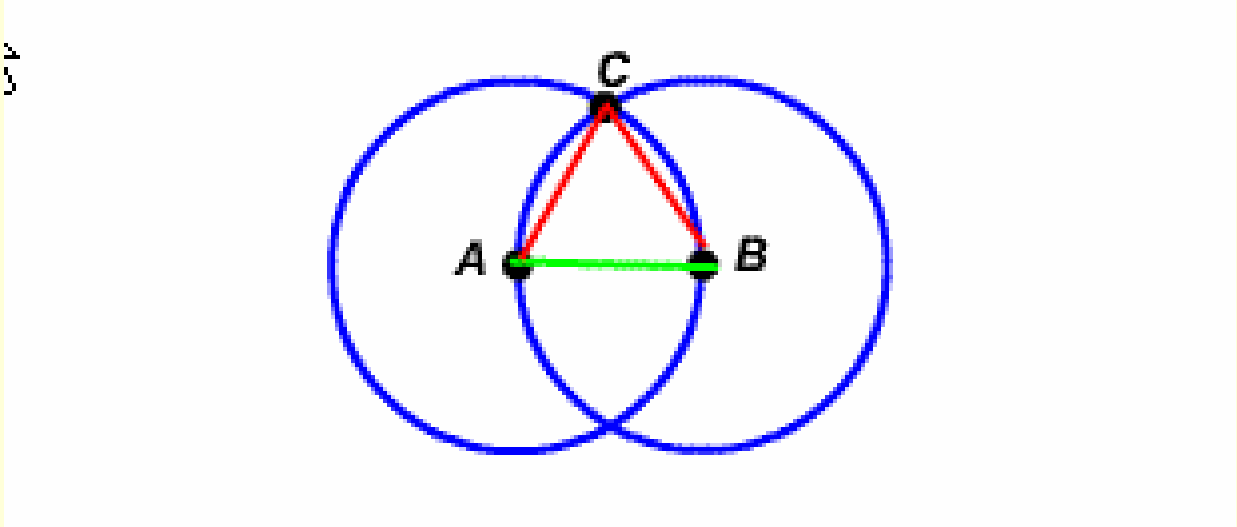
- **Algebra**: definability of some constructions in terms of others
- **Computer Science**: a programming language for Euclidean constructions
- **Logic**: A formal theory close to Euclid, close to textbooks, useful for computerization.
- **Constructive mathematics**: Axiomatization of constructive geometry.

Where we’re not going today

- Finding proofs of geometric theorems by computer, either by algebra or resolution proof-search.
- Quantifier-elimination techniques
- Decidability or undecidability of various theories (except for remarks made in passing)

Book I, Proposition 1

- *On a given finite straight line to construct an equilateral triangle.*



Euclid’s Data Types

- Point
- Line
- Segment
- Ray
- Angle
- Circle
- Arc
- Triangle, Square, Closed Polygon
- We are not considering 3D constructions

Primitive Constructions

Segment(A,B)

Circle(A,B) (center A, passes through B)

Ray(A,B) (A is the endpoint)

Line(A,B)

Arc(C,A,B) (circle C, from A to B)

IntersectLines(A,B,C,D) (AB meets CD)

IntersectLineCircle1(A,B,C,D) (C is center)

IntersectLineCircle2(A,B,C,D)

IntersectCircles1(c1,c2)

IntersectCircles2(c1,c2)

Geoscript

- A programming language for describing elementary geometrical constructions
- No iterative constructs
- Variables and assignment statements
- Function calls
- No re-use of variables in a function
- No conditional constructs
- Multiple return values

www.dynamicgeometry.org

- The 48 Euclidean constructions in Euclid's words, animated (Ralph Abraham)
- An applet *Diagrammer* allows you to make your own constructions. (Chris Mathenia and Brian Chan)
- An applet *Constructor* provides a visual interpreter for *Geoscript*. You can step through or into the 48 Euclidean scripts. (with some help from Thang Dao.)

Descartes

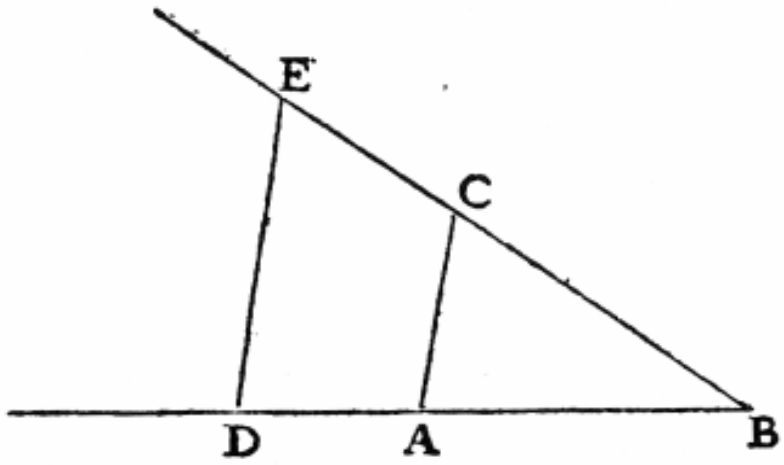
La Geometrie (1637). Introduced the idea of performing arithmetic on (the lengths of) segments by geometrical construction.

The opening of *La Geometrie*

Any problem in geometry can easily be reduced to such terms that a knowledge of the lengths of certain straight lines is sufficient for its construction…to find required lines it is merely necessary to add or subtract other lines; or else, taking one line which I shall call unity, and having given two other lines, to find a fourth line which is to one of the given lines as the other is to unity (which is the same as multiplication); or, again, to find a fourth line which is to one of the given lines as unity is to the other (which is equivalent to division); or, finally, to find one, two or several mean proportionals between unity and some other line (which is the same as extracting the square root, cube root, etc., of the given line.)

Page 2 of *La Geometrie*

La Multiplication.

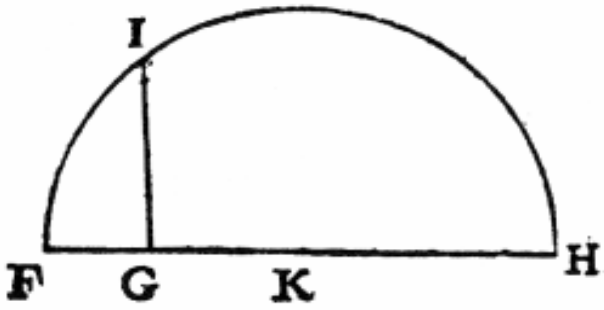


Soit par exemple A B l'vnité, & qu'il faille multiplier B D par B C, ie n'ay qu'a ioindre les poins A & C, puis tirer D E parallele a C A, & B E eſt le produit de cete Multiplication.

La Diuiſion.

Oubien s'il faut diuiſer B E par B D, ayant ioint les poins E & D, ie tire A C parallele a D E, & B C eſt le produit de cete diuiſion.

l'Extraction dela racine quarrée.



Ou s'il faut tirer la racine quarrée de G H, ie luy adiouſte en ligne droite F G, qui eſt l'vnité, & diuiſant F H en deux parties eſgales au point K, du centre K ie tire

Flaws in Euclid

Book I, Prop. 1 has the first flaw. Nothing in Euclid guarantees the intersection of the circles. In general what we now call “betweenness” is missing.

Assuming the parallel postulate instead of proving it seemed a flaw. Efforts to eliminate this “flaw” led to the 1870s work of Pasch, Verona, and others on formalized geometry, as well as to the development of non-Euclidean geometry.

These in turn influenced Peano, who invented the symbols used in modern logic.

What is geometry about?

- Points, lines, planes, and their properties?
- How to construct points, segments, angles with certain properties?
- Nothing at all!? [Hilbert, 1899, *Foundations of Geometry*]:
- “One must be able to say at all times—instead of points, straight lines, and planes—tables, chairs, and beer mugs.”

Formalizations of Geometry

- Hilbert's system was second-order. Second order continuity makes it (second-order) categorical. (Theorem 32 of Hilbert)
- Tarski's "elementary geometry" is first-order but has full first-order continuity.
- Geometry of constructions only has circle-circle continuity and line-circle continuity.

What is a minimal set of primitive constructions?

- Circle-circle continuity implies line-circle continuity. See for example Major Exercise 1, Chapter 4 of Greenberg, *Euclidean and Non-Euclidean Geometries,* fourth edition. You must assume the construction Extend(A,B,C,D) (extend AB past B by CD), i.e. the case of line-circle continuity where the line is a diameter.

Line-circle continuity implies circle-circle continuity.

- In fact, *one fixed circle* and a straightedge suffice!
- In view of Descartes, it suffices to be able to bisect a segment (then you can do his square root construction and solve the equations), but you need circles to bisect a segment.
- It was done directly in the 19th century.

Jean Victor Poncelet

An officer in Napoleon's army in 1812, he was abandoned as dead at the Battle of Krasnoy, then captured by the Russians and imprisoned at Saratov until 1814. During this period he developed "the basis for his book, *Traité des Propriétés Projectives des Figures"* (Paris, 1822), which contains the theorems mentioned.

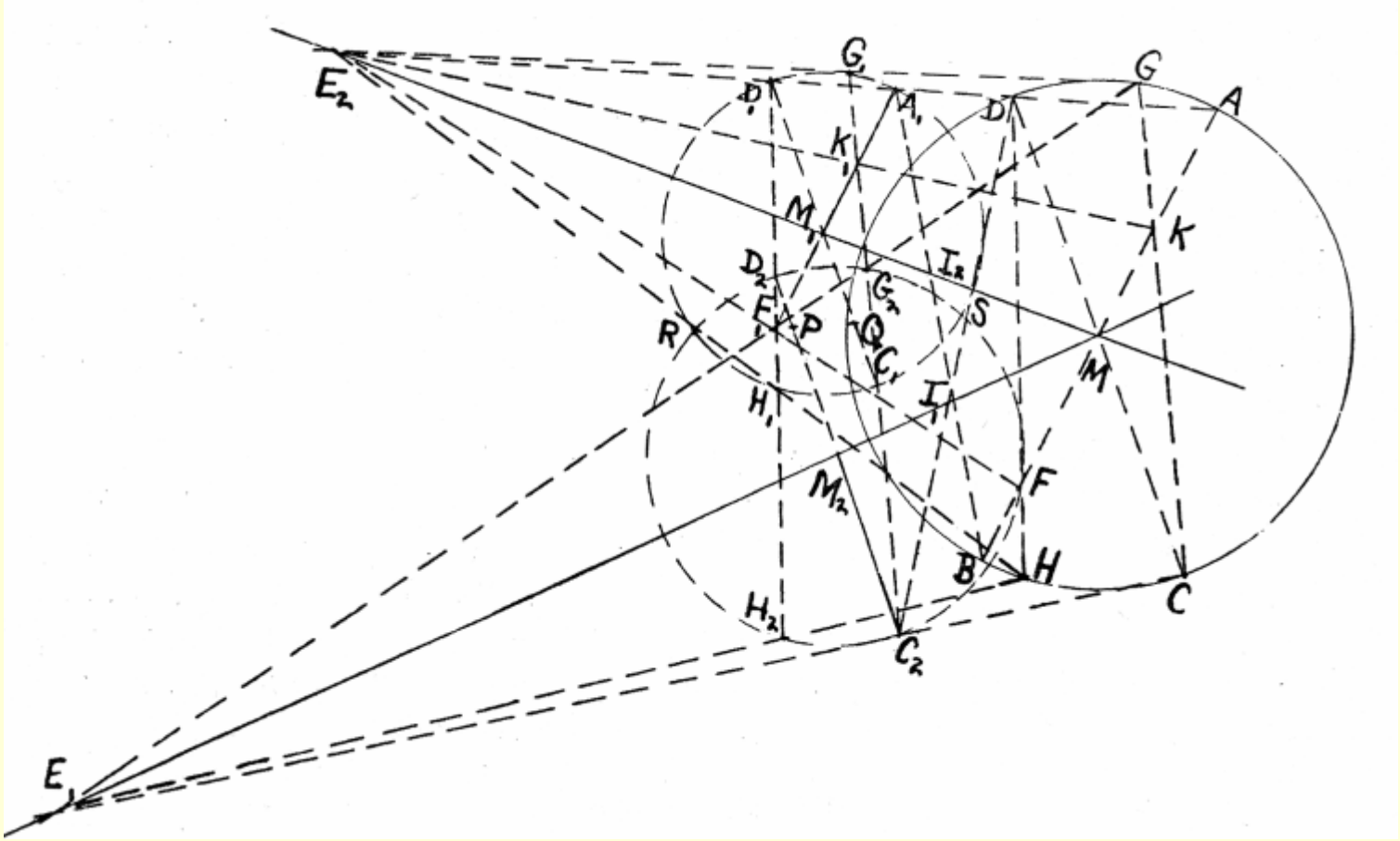
Jakob Steiner

- Independently reproved Poncelet's result in his wonderful book,

  Die geometrischen Constructionen ausgefürht mittels der geraden Linie und eines festen Kreises, Berlin (1833).

- In this era the focus in geometry was still algorithmic rather than axiomatic.

Steiner's Construction (Fig. 24)



The algebraic view

- We have a three-sorted algebra (points, lines, and circles) with some operations:
- Constructors *Line(A,B), Circle(A,B)* and accessors *center(C), pointOnCircle(C), point1On(L), point2On(L).*
- Further operations:

  IntersectLines

  IntersectLineCircle1, IntersectLineCircle2,

  IntersectCircles1, IntersectCircles2

A theorem in the algebraic setting

- Let Circle3(A,B,C) be the circle with center A and radius BC.
- Theorem (with Freek Wiedijk) Circle3 is not definable from the operations on the previous slide.
- Proof, all functions of one variable so definable become undefined when one of the variables is set equal to a constant. But not so for Circle3(P,β,γ).

An open question

- Let *project(P,L)* be the point *Q* on line *L* such that *P* lies on the perpendicular to *L* at *Q.* *Note:* this is defined whether or not *P* is on *L*.
- I conjecture *project* is not definable from the elementary constructions mentioned above, including *Circle3.*

D. Kijne

- A 1956 Ph. Thesis called *Plane Construction Field Theory* took an algebraic approach, but all the systems considered have “decision functions” such as test-for-equality, test-for-incidence.
- Including such functions creates discontinuous constructions, which we want to avoid.

Models of the elementary constructions

- The “standard plane”
- The “recursive plane”. Points are given by recursive functions giving rational approximations to within 1/n.
- The minimal model, the points constructible by ruler and compass
- The algebraic plane, points with algebraic coordinates
- The Poincaré model—these constructions work in non-Euclidean geometry too.

Connections to field theory

- Every model is a plane over some ordered field.
- Because of quantifier elimination (Tarski) every real-closed field gives a model of Tarski geometry.
- Euclidean fields (every positive element has a square root) correspond to the geometry of constructions.

A problem of Tarski

- Is the geometry of constructions decidable?
- Ziegler (1980) says not. Indeed any finitely axiomatizable field theory that has R or the p-adics as a model is undecidable. His proof is only 11 (difficult) pages. (I have translated this paper if anyone wants an English version.)

Another problem of Tarski

- Is the smallest Euclidean field Q(sqrt) decidable?
- Goes beyond J. Robinson's famous results for Q and the algebraic number fields, because Q(sqrt) is not of finite degree over Q.
- Still an open problem (as far as I know)

Still of interest to work with geometry rather than algebra

- Hilbert introduced the primitives of *betweenness* (A is between B and C) and *congruence* (of segments), and considered points, lines, and planes with an *incidence relation*.
- Tarski's theory has variables for points only. Congruence of segments AB and CD becomes the *equidistance relation* δ(A,B,C,D).
- Details are in Borsuk and Szmielew

Scott's theory

- Full set theory in which the points are Quine atoms, i.e. sets such that x = {x}.
- This is not a ZF-style set theory.
- In some ways closer to informal geometry, but as yet no experiments with automated deduction in this theory.
- I am going to take a different direction.

Multisorted Theories

- Points, segments, lines, arcs, rays.
- I do plane geometry only, so no planes
- No variables for angles
- Much easier to translate textbook proofs in a multisorted theory
- Good for automated deduction, too. Not necessary to use unary predicates for the sorts due to *Implicit Typing* metatheorem.

Geometry of Constructions

- Quantifier-free axiomatization
- Terms for the primitive geometric constructions.
- Models are planes over Euclidean fields
- Conservative over Tarski's geometry of constructions.

Theory EGC plus classical logic

- Six sorts: Point, Line, Circle, Segment, Ray, Arc.
- Angles treated as triples of points.
- Function symbols for the elementary constructions *IntersectLines,*

  IntersectLineCircle1, IntersectLineCircle2,

  IntersectCircles1, IntersectCircles2
- Also for *Circle3(A,B,C)*, which constructs the circle with center *A* and radius *BC.*

  and
- Logic of partial terms (LPT) because these functions are partial.

EGC, continued

- Quantifier-free, disjunction-free axiomatization
- All existential quantifiers removed using explicit terms built from the function symbols.
- To distinguish the two intersection points of circles, we need to specify whether center-center-point is a “right turn” or a “left turn”.
- It is possible to define “ABC has the same handedness as PQR”. Then use the three constants α,β,γ from Axiom 1 and specify $\alpha\beta\gamma$ to be “left” and $\alpha\gamma\beta$ to be “right”. With care this can be done quantifier-free.
- I have verified in detail the equivalence of EGC to the theory in Greenberg’s textbook.

Intuitionistic Geometry

- Decidable equality means A=B or A $\neq$ B.
- If points are given by real numbers there's no algorithm to decide equality.
- If points are given by rational or Euclidean numbers then there is an algorithm, but not a geometric construction, i.e. no Geoscript program, to decide equality.
- Euclid, as made right by Proclus, uses proof by cases (and often only one case is illustrated in Euclid).

Book I, Proposition 2

- Given point A and segment BC, construct segment AD congruent to BC. (*To place at a given point, as an extremity, a straight line equal to a given straight line.*)
- Euclid's construction assumes B (or C) is different from A.
- The Euclidean construction is not continuous in B as B approaches A (as I demonstrated during the talk using the applet at www.dynamicgeometry.org)
- Therefore without further assumptions the theorem above, (which does not assume A different from B or C), or at least its proof, cannot be realized by a (single, uniform) Euclidean construction.
- This was realized already by Proclus, who considered eight "cases" (different diagrams) including the case A=B, which Heath thinks is superfluous.
- We already proved Circle3 is not definable from the (other) elementary constructions. Book I. Prop.2 amounts to Circle3.

Apartness

- Apartness (introduced by Heyting) is a positive version of inequality. A # B means (intuitively) that we can find a lower bound on the distance from A to B.
- Axiomatically one could add # as a primitive relation with natural axioms. In particular

  not A # B implies A = B

  A # B implies A ≠ B

  B # C implies A # B or A # C

An apartness constructor

- apart(A,B,C)
- If B # C then P = apart(A,B,C) is defined
- P=B or P=C
- P # A
- Intuitively: just compute A, B, and C to an accuracy less than 1/3 of |B-C|.
- But apart, although computable, is not extensional and not continuous. For that reason I am interested in theories without apartness.
- Also apartness does not occur in Euclid, so if we want a theory that is close to Euclid, we shouldn’t include apartness.

Nevertheless here's a nice theory with apartness: (IGC)

- Multi-sorted, with intuitionistic logic.
- Apartness [but it does not occur in Euclid!]
- three constants α,β,γ (noncollinear points).
- f(u,v) # f(a,b) implies u # a or v # b for primitive constructions f.
- Quantifier-free and disjunction-free axiomatization if apartness is not used. (terms for elementary constructions, no continuity schema). But the apartness axioms have disjunction.
- Use LPT (logic of partial terms) because the constructions are partial (not always defined)

The uniform version of Book I, Prop. 2, is provable in IGC

- Recall that was: for every A,B,C, if B # C then there exists D with AD = BC.
- It can be proved in IGC: Let B # C. Then by the apartness axioms, either A # B or A # C. So Euclid's construction can be carried out, starting from an end of the given segment BC that is apart from A.
- In other words, *Circle3* can be defined if we allow an apartness constructor.

Connection to Field Theory revisited

- If field theory is formulated with apartness (as in Heyting's book) then IGC corresponds naturally to Euclidean fields, just as in the classical case.
- Even without apartness, we can still coordinatize in some weaker theories.
- But since we no longer have quantifier elimination, it is not clear that IGC with some version of full continuity corresponds to intuitionistic real closed fields (RCF).
- All natural versions of intuitionistic RCF are undecidable (Gabbay 1972 without apartness, Gabbay 1977 with apartness)

Euclidean Geometry of Constructions (EGC)

- Intuitionistic logic, but no constructor *apart*.
- We take "Markov's principle" $\neg\neg$ P $\supset$ P for atomic P (betweenness, equidistance, equality, and definedness)
- The axiomatization is quantifier-free and disjunction-free.
- Seems to correspond better to Euclid's *Elements* than IGC.
- "Markov's principle" is b $\neq$ c $\supset$ b # c, but EGC is not IGC + MP because EGC does not have the apartness axiom above.
- Coordinatization requires one more construction: *project(P,L)* that projects point P on line L. Without this we cannot connect to field theory.

Projection and coordinatization

- The axioms for projection are

  project(P,L) is on L

  P lies on the perpendicular to L at project(P,L).
- Using projection, we can assign coordinates on two perpendicular lines to any point P.
- Projection is continuous, like the other basic constructions.
- Projection is computable—we can compute *project(P,L)* to any desired accuracy.

Projection and Coordinatization

- We obviously need *project* to assign coordinates (x,y) to points.
- It's not so obvious that *project* is enough to define addition, multiplication, and sqrt without needing test-for-equality, but it is!
- Example lemma: *para*(*p,L*) constructs a line through *p* that is parallel to *L* if *p* is not on *L*, and equal to *L* if *p* is on *L*. Then *para* can be defined using *project*.

Extraction of Algorithms from Proofs

- We know how to extract terms for computable functions from proofs in number theory or analysis.
- Now we want to extract geometrical constructions from proofs in EGC and related theories.
- Tools from proof theory used in the number-theory case:

Cut elimination
Realizability

Extracting constructions from proofs in geometry

Suppose EGC proves

$\forall x(P(x) \supset \exists y\ A(x,y))$

with P negative. Then there exist a term t(x) of EGC such that EGC proves

$\forall x(P(x) \supset A(x,[y:=t(x)]))$

(Here x can stand for several variables.)

Proof by cut-elimination

- Standard proof method, appealing to permutability of inferences (Kleene 1951)
- Consider a cut-free proof of $\Gamma \Rightarrow \exists y\ A(x,y)$, where Γ is a list of universal closures of axioms and the hypotheses P.
- the last step can therefore be assumed to introduce the quantifier, so the previous step gives the desired conclusion.
- Doesn't work if apartness is used because the apartness axioms involve disjunction and such inferences don't permute.

Local Continuity

- The primitive geometrical constructions (interpreted in the standard model) are all continuous on their domains, and those domains are open.
- This property is preserved under composition.
- Hence every term of EGC defines a locally continuous function.

Local continuity of theorems of EGC

Theorem. Suppose EGC proves

$\forall x(\mathrm{P}(x) \supset \exists y\, \mathrm{A}(x,y))$

with P negative. Then there is a locally continuous Euclidean construction of y from x, i.e. y is given by a term t defined and continuous where P holds.

Constructions and classical logic

Suppose EGC with classical logic proves

$\forall x(P(x) \supset \exists y\, A(x,y))$

with P and A quantifier-free. Then there exist terms $t_1(x),\ldots,t_n(x)$ of EGC such that EGC proves

$\forall x(P(x) \supset A(x,[y:=t_1(x)]) \vee \ldots \vee A(x,[y:=t_n(x)])$

(Here x can stand for several variables.)

Proof: by Herbrand's theorem.

Realizability

- A tool used in the metatheory of intuitionistic systems. We define "*e* realizes *A*", written *e* r *A,* for each formula A. Here *e* can be a term or a program (e.g. index of a recursive function). The key clauses are
- *e* r (A $\supset$ B) iff $\forall q$ (*q* r A $\supset$ Ap(*e*,*q*) r B)
- *e* r $\exists x$ A iff p1(e) r A[x:=p0(e)].

Here p0 and p1 are projection functions,

x = <p0(*x*), p1(*x*)> if x is a pair.

Adding lambda terms to geometry

- To define realizability, we need lambda terms (and application, written Ap(f,x))
- Of course, combinators would also work.
- I have already studied in general what happens when we add lambda terms to a first order theory.
- We need realizability for IGC since cut-elimination doesn’t work with apartness.

Lambda Logic

- Introduced (for other purposes) in IJCAR-2004. See papers on my website www.MichaelBeeson.com/Research
- Type-free lambda logic plus first-order logic.
- IGC in lambda logic contains lambda, Ap, beta-reduction as well as IGC. (We need unary predicates *Point, Line,* etc. because lambda logic is not multisorted.)
- Let GT be IGC plus lambda logic.

q-realizability

- Similar to realizability but the main clauses are
- e r $(A \supset B)$ iff $\forall q\ (q \text{ r } A \supset Ap(e,q) \text{ r } B)$
- e r $\exists x\ A$ iff A & p1(e) r A[x:=p0(e)].

This tool is used to extract programs from proofs.

Soundness of Realizability

- If IGC proves A then GT proves *t* r A for some term normal term *t* whose free variables are among those of A.
- Similarly for *q*-realizability.

Extraction of constructions in IGC

Extraction theorem. Suppose IGC proves

$\forall x(\mathrm{P}(x) \supset \exists y\, \mathrm{A}(x,y))$

with P a conjunction of atomic formulae.

Then there is a term t of IGC such that

IGC proves

$\forall x(\mathrm{P}(x) \supset \exists y\, \mathrm{A}(x,t(x)))$

Proof

- From q-realizability we know that

  GT proves

  $\forall x(\mathrm{P}(x) \supset \exists y\ \mathrm{A}(x,t(x)))$

  for some normal term *t* of GT. Since that term takes points to points, it corresponds to a term of IGC (as has to be shown). But to complete the proof we must show that GT is conservative over IGC (modulo the identification of function symbols of IGC with constants of GT).

Conservativity of GT over IGC

- Lambda logic is conservative over FOL plus the schema “there exist at least N things” (for each N).
- But IGC already proves there exists at least N things.
- Hence IGC + lambda logic is conservative over IGC.
- Hence GT is conservative over IGC.
- That completes the proof of the extraction theorem.

Conclusion

- The algorithmic and axiomatic viewpoints have a long history in geometry
- Modern axiomatizations of classical geometry are well understood.
- I tried to bring a modern viewpoint also to the algorithmic view of geometry,
- and then to connect that view with the modern axiomatic view using the tools of lambda calculus and realizability.
- There are still some open questions!

Two conjectures

- For a formula A in the language of ordered fields, let A* be its translation into arithmetic of finite types, letting variables range over the Bishop reals, and let A_{rec} be its translation into HA, letting variables range over the recursive reals.
- Suppose arithmetic of finite type proves A*. Then intuitionistic RCF proves A.
- Suppose HA + CT + MP proves A_{rec}. Then RCF + MP proves A.