Semantic methods in proof theory

Jeremy Avigad

Department of Philosophy

Carnegie Mellon University

avigad@cmu.edu

http://macduff.andrew.cmu.edu

Proof theory

Hilbert's goal: Justify classical mathematics.

Hilbert's program:

1. Devise formal systems to represent classical mathematical reasoning.
2. Prove the consistency of these formal systems using finitary methods.

The modified Hilbert's program: Prove the consistency of these formal systems using *constructive* methods.

Kreisel's program: Extract constructive information from proofs in classical theories.

Informal goals: Obtain satisfying constructive analyses of classical methods in mathematics.

Proof theoretic reductions

These take the following form:

For any $\varphi \in \Gamma$, if T proves φ, then T' proves φ'.

Many proof theoretic results follow this pattern:

- Equiconsistency: φ is just $\perp$
- Ordinal analysis: e.g. Γ is Π_2, and T' expresses some kind of transfinite induction or recursion
- Functional interpretation: T' is a quantifier-free theory axiomatizing some interesting class of functions
- Foundational reductions: e.g. T is classical, T' is constructive
- Combinatorial independences: T' is a weak theory plus some interesting combinatorial principle

Such results can be interesting for philosophical, logical, mathematical, or computational reasons.

Two approaches

Assuming both proof systems are sound and complete, the following two statements are equivalent:

> If T proves φ, then T' proves φ'

and

> If $T' \cup \{\neg\varphi'\}$ has a model, then $T \cup \{\neg\varphi\}$ has a model.

Despite the theoretic equivalence, the syntactic and semantic approaches are very different:

- The proofs yield different information
- The proofs rely on different intuitions

A range of methods

1. **Semantic:** given a model of T', construct a model of T

   Examples: GB and ZFC, ACA_0 and PA, nonstandard analysis

2. **Internalized semantic:** in T', prove the existence of models of (portions of) T

   Examples: forcing arguments, nonstandard set theory

3. **Semantic interpretation:** interpret a model of T in T'

   Examples: ZFC with $V = L$, RCA_0 in $I\Sigma_1$, PA in T

4. **Syntactic translation:** translate proofs in T to proofs in T'

   Examples: the double-negation intepretation, the Dialectica interpretation

These are not sharp distinctions.

Applications

I will survey the use of semantic methods in analyzing

- Classical theories
- Constructive theories
- Bounded arithmetic / propositional proof systems

with an eye towards obtaining

- Conservation results
- Functional interpretations
- Combinatorial independences
- Ordinal analyses

PA and $\mathbf{ACA_0}$

PA is first-order arithmetic. ACA_0 is a second-order version, with an axiom of comprehension

$$\exists X \, \forall y \, (y \in X \leftrightarrow \varphi(y))$$

for arithmetic φ, and induction for *sets*.

Theorem. ACA_0 is conservative over *PA* for arithmetic formulas.

Proof (semantic). If $\mathcal{M}$ is a model of $PA \cup \{\neg\varphi\}$, let $S_{\mathcal{M}}$ consist of the sets definable from parameters. Then $\langle \mathcal{M}, S_{\mathcal{M}} \rangle$ is a model of $ACA_0 \cup \{\neg\varphi\}$.

Proof (syntactic). Add "names" for the definable sets, eliminate cuts, replace names by formulas.

Similar considerations show that *GB* is conservative over *ZFC*.

Some additional information

The syntactic argument shows that given a proof d in ACA_0, there is a proof d' in PA, with $|d'| < 2^0_{p(|d|)}$.

Theorem (Solovay). There is no elementary bound on the increase in the length of proofs.

Proof. "Shortening of cuts." Show that ACA_0 has short proofs of $Con(I\Sigma_{2^0_n})$.

This shows that one *cannot* hope to interpret ACA_0 in PA.

Conservation results with speedup

GB	ACA_0	$\Pi^1_1 - CA_0$	ATR_0	$I\Sigma_1$
ZFC	PA	$ID_{<\omega}$	$\widehat{ID}_{<\omega}$	PRA

Credits: Solovay, Kleene, Kreisel, Feferman, Avigad, Parsons, Mints, Takeuti, Ignatovic.

A stronger result

Σ^1_1-AC_0 augments ACA_0 with a principal of arithmetic choice:

$$\forall x \, \exists Y \; \varphi(x, Y) \rightarrow \exists Y \, \forall x \; \varphi(x, Y_x)$$

Theorem (Barwise-Schlipf). Σ^1_1-AC_0 is conservative over PA for arithmetic sentences.

Proof (semantic). Uses recursive saturation.

Proof (syntactic; Sieg). Uses cut elimination.

Proof (syntactic; Feferman). Uses the Dialectica interpretation with a nonconstructive μ operation.

The semantic argument

Start with a model $\mathcal{M}$ of PA.

- Take a saturated (or even recursively saturated) elementary extension, $\mathcal{M}'$.
- Let $\widehat{\mathcal{M}}$ be have first-order part $\mathcal{M}'$, and second-order part the definable sets of $\mathcal{M}'$.

Now suppose

$$\widehat{\mathcal{M}} \models \forall x \, \exists Y \; \varphi(x, Y).$$

Then the diagram of $\mathcal{M}'$ together with the type

$$\{\neg\varphi(c, \{y \mid \psi(y)\})\}_{\psi}$$

is inconsistent. Since some finite subset is inconsistent, we see that

$$\varphi(c, \{y \mid \psi_1(y)\}) \vee \ldots \vee \varphi(c, \{y \mid \psi_k(y)\})$$

holds in $\mathcal{M}'$, for some $\psi_1, \ldots, \psi_k$. As a result,

$$\widehat{\mathcal{M}} \models \exists Y \, \forall x \; \varphi(x, Y).$$

Another conservation result: RCA_0 and $I\Sigma_1$

RCA_0 restricts the comprehension axiom in ACA_0 to recursive (Δ_1 definable) sets. Induction is augmented to include Σ_1 formulas.

Theorem. RCA_0 is conservative over $I\Sigma_1$ (without speedup).

Proof. Interpret the sets of RCA_0 with codes $\langle \ulcorner \varphi \urcorner, \ulcorner \psi \urcorner \rangle$ for Δ_1 definable sets, and use a Σ_1 truth predicate for the membership relation.

Weak König's lemma

WKL_0 augments RCA_0 with a weak form of König's lemma: "every infinite binary tree has a path."

Theorem (Friedman). WKL_0 is conservative over PRA for Π_2 formulas.

Proof (semantic). Uses a nonstandard model of PRA and semiregular cuts.

Proof (syntactic; Sieg). Use cut-elimination, and hereditary majorizability.

Proof (syntactic; Kohlenbach). Uses the Dialectica interpretation and hereditary majorizability for higher type functionals.

A stronger result

Theorem (Harrington). *WKL*$_0$ is conservative over *RCA*$_0$ for Π^1_1 sentences.

Proof (semantic). inspired by the Jokusch-Soare low basis theorem, which states that every recursive binary tree has a *low* path $P \leq_T 0'$. Given a model of *RCA*$_0$:

1. Take a countable elementary submodel.
2. Iteratively add a generic path through a tree, then the sets recursive in it.

Proof (Hájek, syntactic). Formalize a recursion theoretic model of *WKL*$_0$, in *RCA*$_0$.

Proof (Avigad, syntactic). Internalize the (iterated, proper-class) forcing argument in *RCA*$_0$. (This also works for *WKL*$+_0$.)

Conservation results

2nd-order	RCA_0	WKL_0	ACA_0	ATR_0	$\Pi^1_1 - CA_0$
1st-order	$I\Sigma_1$	$I\Sigma_1$	PA	$\widehat{ID}_{<\omega}$	$ID_{<\omega}$
Speedup?	No	No	Yes	Yes	Yes

Other subsystems of analysis

Theorem (Friedman). Σ^1_1-AC is conservative over $(\Pi^0_1\text{-}CA)_{<\varepsilon_0}$ for arithmetic sentences.

Proof (semantic). Use a nonstandard models of $(\Pi^0_1\text{-}CA)_{\omega_k}$ with definable descending sequences of ordinals.

Proof (syntactic; Tait). Uses cut elimination.

Proof (syntactic; Feferman). Uses the Dialectica interpretation.

There are corresponding results for Σ_{n+1}-AC and Σ_{n+1}-AC_0

Theorem (Friedman). ATR_0 is conservative over $(\Pi^0_1\text{-}CA)_{<\Gamma_0}$ for arithmetic sentences.

Stronger theories

Impredicative subsystems of second-order arithmetic, in conjunction with admissible set theory, have been studied by Arai, Buchholz, Jäger, Pohlers, Rathjen.

The methods are invariably syntactic (or “interpretive semantic”).

Forcing

Forcing can also be understood in a number of different ways:

1. Given a model of set theory $\mathcal{M}$ and a poset P, construct a generic object G and $\mathcal{M}[G]$
2. Construct in $\mathcal{M}$ a boolean valued model (Scott,Solovay)
3. Topos theory: interpret forcing as a sheaf construction (Lawvere-Tierney)

One can usually extract syntactic translations from these.

Reductions for intuitionistic theories

Methods:

1. Kripke models, Beth models (e.g. Smorynski)
2. Realizability, modified realizability (Kleene, Kreisel)
3. Topos theory, sheaf semantics

As an example of the latter, Moerdijk and Palmgren have used sheaf constructions to obtain conservation results for inutuitionistic nonstandard analysis.

Reducing classical theories to constructive theories

The double-negation translation (syntactic: Gödel, Gentzen) reduces PA to HA, ZF to IZF, PA_2 to HA_2.

Other reductions:

- Buchholz: iterated inductive definitions, ID_α
- Coquand-Hofmann: $I\Sigma_1$ and S^1_2
- Avigad: admissible set theory, Σ^1_1-AC

The methods are similar, but Buchholz and Avigad focus on the syntactic translation, while Coquand and Hofmann focus on the algebraic interpretation (involving a construction due to Sambin).

Weak and bounded fragments of arithmetic

Theorem. $B\Sigma_{k+1}$ is Π_{k+2}-conservative over $I\Sigma_k$.

Original proofs by Paris and Friedman (independently) were semantic. Sieg offered the first proof-theoretic proof.

Theorem. S^1_2 is conservative over PV for Π_2 sentences.

Original proof by Buss was syntactic. Wilkie discovered a model-theoretic version.

Various results involving (WKL) over weak theories: Kohlenbach (syntactic), Ferreira (semantic).

Bounded arithmetic and proof complexity

Given a natural translation of formulas $\forall x\ \varphi(x, R)$, where φ is bounded, to a sequence of propositional formulas $\hat{\varphi}_n$:

Theorem. If $I\Delta_0(R)$ proves $\forall x\ \varphi(x, R)$, then there are polynomial-size constant depth-Frege proofs of $\hat{\varphi}_n$.

Original proof by Paris and Wilkie (semantic); easy proof by cut elimination.

Theorem. There are no polynomial-size constant-depth Frege proofs of the pigeonhole principle.

The original proof by Ajtai used forcing over a nonstandard model of arithmetic. There are now syntactic proofs by Beame, Bellantoni, Impagliazzo, Krajiĉek, Pitassi, Pudlák, Urquhart, Woods.

Combinatorial independences

Paris and Harrington define a predicate $PH(a, b)$ which says that the interval $[a, b]$ has a certain Ramsey-theoretic property. The assertion

$$\forall a \; \exists b \; PH(a, b)$$

can be proved using the infinitary version Ramsey's theorem.

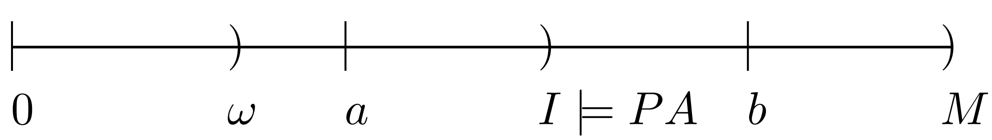
Theorem (Paris-Harrington). *PA* doesn't prove $\forall a \; \exists b \; PH(a, b)$.

Proof (semantic). Suppose a and b are nonstandard elements of a model M of true arithmetic, and

$$M \models PH(a, b).$$

Show that there is an initial segment I of M containing a but not b, such that

$$I \models PA.$$



The Paris-Harrington Statement

Definition: A set $X \subset \mathbb{N}$ is *large* if $|X| > min(X)$.

For example, $\{4, 9, 23, 46, 78\}$ is large because it has 5 elements, the smallest of which is 4.

Definition: Say

$$[a, b] \to_* (m)^l_r$$

if, no matter how you r-color the l-tuples from $[a, b]$, there is a *large* homogeneous subset of size at least m.

The Paris-Harrington Statement:

$$\forall m, l, r, a \ \exists b \ [a, b] \to_* (m)^l_r.$$

This assertion follows from the infinitary version of Ramsey's theorem by a short compactness argument.

$PH(a, b)$ is the predicate

$$[a, b] \to_* (a)^a_a.$$

Ordinal analysis

Theorem (Gentzen). The proof-theoretic ordinal of PA is ε_0.

Proof (syntactic). Show how to unwind the proof of a Σ_1 sentence in a $<\varepsilon_0$-recursive way.

Proof (syntactic; Schutte). Embed the proof in infinitary logic, and eliminate cuts there.

Proof (more semantic; Ackermann-Hilbert). Assign ordinal to epsilon terms in a $<\varepsilon_0$-recursive way.

Another semantic approach

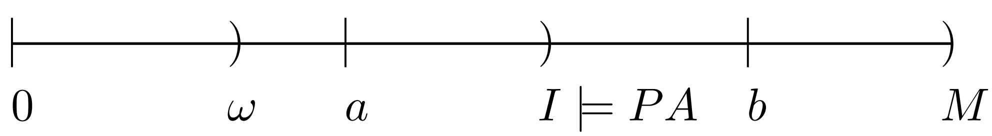
For any ordinal notatation α, Ketonen and Solovay show how to define the finitary combinatorial notion "$[a, b]$ is α-large."

Theorem (K-S, Paris, Sommer): Suppose a and b are nonstandard elements of a model M of true arithmetic, and

$$M \models [a, b] \text{ is } \varepsilon_0\text{-large.}$$

Then there is an initial segment I of M containing a but not b, such that

$$I \models PA.$$



Suprisingly, one can extract all the consequences of a traditional ordinal analysis from this construction.

Avigad and Sommer have extended the method to a number of predicative subsystems of second-order arithmetic.

Current goals

1. Develop a direct, finitary version of the semantic approach to ordinal analysis
2. Extend semantic methods to impredicative theories
3. Understand the model-construction principles used to obtain Friedman's latest combinatorial independences