Between proof theory and model theory

Jeremy Avigad

Department of Philosophy

Carnegie Mellon University

avigad@cmu.edu

http://andrew.cmu.edu/∼avigad

Overview

Three traditions in logic:

- Syntactic (formal deduction)
- Semantic (interpretations and truth)
- Algebraic

Contents of this talk:

1. Conservation results in proof theory
2. A model-theoretic approach
3. An algebraic approach

Conservation results

Many theorems in proof theory have the following form:

For $\varphi \in \Gamma$, if T_1 proves φ, then T_2 proves φ'

where

- T_1 and T_2 are theories
- Γ is a class of formulae
- φ' is some "translation" of φ (possibly φ itself)

If $T_1 \supseteq T_2$, this is a *conservation theorem.* These can be:

1. Foundationally reductive (classical to constructive, infinitary to finitary, impredicative to predicative, nonstandard to standard)
2. Otherwise informative (ordinal analysis, combinatorial independences, functional interpretations)

An example

The set of primitive recursive functions is the smallest set of functions from $\mathbb{N}$ to $\mathbb{N}$ (of various arities)

- containing 0, $S(x) = x + 1$, $p_i^n(x_1, \ldots, x_n) = x_i$
- closed under composition
- closed under primitive recursion:

$$f(0, \vec{z}) = g(\vec{z}), \quad f(x+1, \vec{z}) = h(f(x, \vec{z}), x, \vec{z})$$

Primitive recursive arithmetic is an axiomatic theory

- with defining equations for the primitive recursive functions
- quantifier-free induction:

$$\frac{\varphi(0) \qquad \varphi(x) \to \varphi(x+1)}{\varphi(t)}$$

PRA can be presented either as a first-order theory or as a quantifier-free calculus.

Theorem. (Herbrand) Suppose first-order *PRA* proves $\forall x\, \exists y\, \varphi(x, y)$, with φ quantifier-free. Then for some function symbol f, quantifier-free *PRA* proves $\varphi(x, f(x))$.

Strengthening the conservation result

Let $I\Sigma_1(PRA)$ denote the theory obtained by adding induction for Σ_1 formulae,

$$\theta(0) \wedge \forall x\ (\theta(x) \rightarrow \theta(x+1)) \rightarrow \forall x\ \theta(x),$$

where $\theta(x)$ is of the form $\exists y\ \psi(x, y, \vec{z})$ for some quantifier-free formula, ψ.

Theorem. (Mints, Parsons, Takeuti) If $I\Sigma_1$ proves $\forall x\ \exists y\ \varphi(x, y)$ with φ q.f., then so does PRA.

In other words: $I\Sigma_1$ is conservative over PRA for Π_2 sentences.

In fact (Paris, Friedman) one can conservatively add a schema of Σ_2 collection.

But wait, there's more

Let RCA_0 be an extension of $I\Sigma_1$ with set variables $X, Y, Z \ldots$ and axioms asserting that "the universe of sets is closed under recursive definability."

RCA_0 is a reasonable framework for formalizing recursive mathematics.

Theorem. RCA_0 is conservative over $I\Sigma_1$.

WKL_0 adds a compactness principle: every infinite tree on $\{0, 1\}$ has a path.

Theorem. (Harrington, strengthening Friedman) WKL_0 is Π^1_1 conservative over RCA_0.

Now how much would you pay?

You get all this:

- Primitive recursive functions
- Σ_1 induction
- Σ_2 collection
- Recursive comprehension
- Weak König's lemma
- Other second-order principles (Simpson and students)
- Higher types (Parsons, Kohlenbach, others)
- Flexible type structures (Feferman, Jäger, Strahm)
- Nonstandard arithmetic/analysis (Avigad)
- ...

without losing Π_2 conservativity over PRA.

Furthermore, one can formalize interesting portions of mathematics in these theories (Friedman, Simpson, Kohlenbach, and many others).

Simpson calls this a "partial realization of Hilbert's program."

Interlude

Recall the contents of this talk:

1. Conservation results in proof theory
2. A model-theoretic approach
3. An algebraic approach

I have described a proof-theoretic *goal*. Now let us consider a model-theoretic *method*.

Proof theory versus model theory

Differences:

- Proof vs. truth
- Derivations vs. structures
- Definability in a theory vs. definability in a model

Areas of overlap:

- Soundness and completeness
- Models of arithmetic
- Nonstandard arithmetic and analysis
- Elimination of quantifiers (e.g. for RCF)
- ...

Model theoretic methods are often used in proof theory, e.g. in proving conservation results.

Saturated models

Model theorists also like to get "something for nothing."

Let $\mathcal{M}$ be a model for a language L. $L(\mathcal{M})$ is the set of formulae with parameters from $\mathcal{M}$.

The *complete diagram* of $\mathcal{M}$ is the set of sentences of $L(\mathcal{M})$ true in $\mathcal{M}$.

A *type* is a set of sentences in $L(\mathcal{M}) + \vec{c}$, where $\vec{c}$ are some new constants.

A type Γ is *realized* in $\mathcal{M}$ if for some $\vec{a} \in \mathcal{M}$, $\langle \mathcal{M}, \vec{a} \rangle \models \Gamma$.

Definition. Let $\mathcal{M}$ be a model of cardinality λ. $\mathcal{M}$ is *saturated* if every type involving less than λ parameters from $\mathcal{M}$ that is consistent with the complete diagram of $\mathcal{M}$ is realized in $\mathcal{M}$.

Theorem (GCH). Every model has a saturated elementary extension.

Proof. Start with the complete diagram $\mathcal{M}$. Make a transfinite list of types. Iterate, and realize types...

Herbrand-saturated models

The *universal diagram* of $\mathcal{M}$ is the set of universal sentences of $L(\mathcal{M})$ true in $\mathcal{M}$.

A type is *universal* if it consists of universal sentences, and *principal* if it consists of a single sentence.

Definition. $\mathcal{M}$ is *Herbrand saturated* if every universal principle type consistent with the universal diagram of $\mathcal{M}$ is realized in $\mathcal{M}$.

Theorem. Every model has an Herbrand saturated 1-elementary extension (i.e. an extension preserving truth of Σ_1 formulae).

Proof. As before, iterate, and realize universal types. Cut down to a term model at the end.

Corollary. Every consistent universally axiomatized theory has an Herbrand-saturated model.

Application to proof theory

Recall our prototypical proof-theoretic result:

If $T_1 \vdash \varphi$, then $T_2 \vdash \varphi$.

By soundness and completeness, this is equivalent to

If $T_2 \cup \{\neg\varphi\}$ has a model, so does $T_1 \cup \{\neg\varphi\}$.

So, instead of translating proofs, we can "translate" models.

I will show:

- Herbrand-saturated models have nice properties.
- In particular, an Herbrand-saturated model of *PRA* satisfies Σ_1 induction.

From the latter, it follows that $I\Sigma_1$ is conservative over *PRA* for Π_2 formulae.

A nice property of Herbrand-saturated models

The following theorem says that any Π_2 assertion true in $\mathcal{M}$ is true for a very concrete reason.

Theorem. Suppose $\mathcal{M}$ is Herbrand-saturated, and

$$\mathcal{M} \models \forall \vec{x}\, \exists \vec{y}\, \varphi(\vec{x}, \vec{y}, \vec{a}),$$

where φ is quantifier-free and $\vec{a}$ are parameters from $\mathcal{M}$. Then there are sequences of terms $\vec{t}_1(\vec{x}, \vec{z}, \vec{w}), \ldots, \vec{t}_k(\vec{x}, \vec{z}, \vec{w})$, and parameters $\vec{b}$ from $\mathcal{M}$ such that

$$\mathcal{M} \models \forall \vec{x}\, \varphi(\vec{x}, \vec{t}_1(\vec{x}, \vec{a}, \vec{b}), \vec{a}) \vee \ldots \vee \varphi(\vec{x}, \vec{t}_k(\vec{x}, \vec{a}, \vec{b}), \vec{a}).$$

Proof. Just use the definition of Herbrand saturation, and Herbrand's theorem.

Modeling Σ_1 induction

Suppose $\mathcal{M}$ is an Herbrand-saturated model of primitive recursive arithmetic, satisfying

- $\exists y\, \varphi(0, y, \vec{a})$
- $\forall x\, (\exists y\, \varphi(x, y, \vec{a}) \rightarrow \exists y\, \varphi(x+1, y, \vec{a}))$.

with φ q.f. Rewrite the second formula as

$$\forall x, y\, \exists y'\, (\varphi(x, y, \vec{a}) \rightarrow \varphi(x+1, y', \vec{a})).$$

Then, by our "nice property", there are a primitive recurisve function symbol g and parameters $\vec{b}$ and c such that $\mathcal{M}$ satisfies

- $\varphi(0, c, \vec{a})$,
- $\varphi(x, y, \vec{a}) \rightarrow \varphi(x+1, g(x, y, \vec{a}, \vec{b}), \vec{a})$.

Let $h(x, \vec{z}, v, \vec{w})$ by the symbol denoting the function defined by

$$\begin{aligned} h(0, \vec{z}, v, \vec{w}) &= v \\ h(x+1, \vec{z}, v, \vec{w}) &= g(x, h(x, \vec{z}, v, \vec{w}), \vec{z}, \vec{w}). \end{aligned}$$

Then $\mathcal{M}$ satisfies

$$\mathcal{M} \models \forall x\, \varphi(x, h(x, \vec{a}, c, \vec{b}), \vec{a}).$$

and so $\mathcal{M} \models \forall x\, \exists y\, \varphi(x, y, \vec{a})$.

Other applications

This is, essentially, the model-theoretic version of Siegs' "Herbrand analysis" and Buss' "witnessing method."

The method applies most directly to universal theories; but any theory can be *made* universal by adding appropriate Skolem functions. So it works for

- S^1_2 over PV
- WKL_0 over PRA
- $B\Sigma_{k+1}$ over $I\Sigma_k$
- Σ^1_1-AC over PA

and so on.

Interlude

Back to the table of contents:

1. Conservation results in proof theory
2. A model-theoretic approach
3. An algebraic approach

Using model-theoretic methods, one can prove

If $T_1 \vdash \varphi$, then $T_2 \vdash \varphi$.

by showing instead that

If $T_2 \cup \{\neg\varphi\}$ has a model, so does $T_1 \cup \{\neg\varphi\}$.

Suppose someone gives you a proof of φ in T_1. Where is the corresponding proof in T_2?

An algebraic approach can be used to recover some constructive information.

Back to the model theoretic construction

Theorem. Every consistent universal theory T has an Herbrand-saturated model.

Proof. Let L_ω be L plus new constant symbols $c_0, c_1, c_2, \ldots$. Let $\theta_1(\vec{x}_1, \vec{y}_1), \theta_2(\vec{x}_2, \vec{y}_2), \ldots$ enumerate the quantifier-free formulae of L_ω. Let $S_0 = T$. At stage i, pick a fresh sequence of constants $\vec{c}$, and let

$$S_{i+1} = \begin{cases} S_i \cup \{\forall \vec{y}_{i+1}\ \theta_{i+1}(\vec{c}, \vec{y}_{i+1})\} & \text{if this is consistent} \\ S_i & \text{otherwise.} \end{cases}$$

Let $S_\omega = \bigcup_i S_i$. Let $S' \supseteq S_\omega$ be maximally consistent. "Read off" a model from S'; this model is Herbrand saturated.

Making it constructive

Main ideas:

- We don't need a "classical model." If we use a Boolean-valued model, we do not need the maximally consistent extension.
- Use a *forcing relation*. Conditions are finite sets of universal formulae that are true in a "generic" model.
- Omit the consistency check; simply allow that some conditions force $\perp$.
- We do not need to enumerate anything; genericity takes care of that.

The forcing relation

A *condition* is a finite set of universal sentences of L_ω.

Define $p \Vdash \theta$ inductively. Intuition: "θ is true in any generic model satisfying p."

$$\begin{array}{rcl} p \Vdash \theta & \equiv & PRA \cup p \vdash \theta \quad \text{for atomic } \theta \\ p \Vdash \bot & \equiv & PRA \cup p \vdash \bot \\ p \Vdash (\theta \wedge \eta) & \equiv & p \Vdash \theta \text{ and } p \Vdash \eta \\ p \Vdash (\theta \rightarrow \eta) & \equiv & \text{for every condition } q \supseteq p, \text{ if } q \Vdash \theta, \text{ then } q \Vdash \eta \\ p \Vdash \forall x\, \theta(x) & \equiv & \text{for every closed term } t \text{ of } L_\omega,\ p \Vdash \theta(t) \end{array}$$

Define $\neg\varphi$, $\varphi \vee \psi$, and $\exists x\, \varphi$ in terms of the other connectives.

A formula ψ is said to be forced, written $\Vdash \psi$, if $\emptyset \Vdash \psi$.

The algebraic version of the proof

Lemma. All the axioms of $I\Sigma_1$ are forced.

Lemma. If a Π_2 sentence is forced, it is provable in PRA.

Theorem. $I\Sigma_1$ is Π_2 conservative over PRA.

Proof. If $I\Sigma_1$ proves $\forall x\, \exists y\, \varphi(x, y)$, it is forced, and hence provable in PRA.

Notes on the proof

Q. What makes the proof "algebraic"?

A. Defining $[\![\varphi]\!] = \{p \mid p \Vdash \varphi\}$ yields a Boolean-valued model of $I\Sigma_1$.

Q. What makes the proof constructive?

A. Two answers:

1. Can formalize it in Martin-Löf type theory.
2. Can read of an explicit algorithm: from a proof d in $I\Sigma_1$, get a typed term T_d, denoting a proof in PRA. Normalizing T_d yields the proof.

Conclusions

Some other uses of algebraic methods:

- nonstandard arithmetic
- weak König's lemma
- eliminating Skolem functions
- proving cut elimination theorems

Questions:

- Are there other metamathematical or proof-theoretic applications?
- Are there concrete computational applications?
- Can algebraic methods be useful in studying particular mathematical theories, and extracting additional information?
- Are there model-theoretic applications, e.g. in constructivizing model-theoretic results?
- Are there applications to bounded arithmetic and proof complexity?