Proof Theory and Subsystems of Second-Order Arithmetic

1. Background and Motivation

   Why use proof theory to study theories of arithmetic?

2. Conservation Results

   Showing that if a theory T_1 proves φ, then a seemingly weaker theory T_2 proves it as well.

3. Functional Interpretations

   Characterizing the computable functions that a theory T can prove to be total.

4. Combinatorial Independences

   Finding finitary combinatorial assertions that are true but not provable in T.

5. Summary

Two Views of Mathematics

Classical: Mathematical objects exist in an independent "Platonic realm."

- The law of the excluded middle (*tertium non datur*) holds.
- Proof by contradiction (*reductio ad absurdum*) is valid.

Constructive: Mathematical truth cannot be divorced from practice.

- A statement is neither true nor false until we've demonstrated it to be one or the other.
- To prove existence, one needs to construct an explicit witness.

Hilbert's Program

Hilbert felt that classical reasoning played an indispensible part in mathematics. He proposed proving that such reasoning could not lead to a contradiction, using "finitistic" arguments that were acceptable to everyone.

Gödel (1931): Any reasonable theory of arithmetic cannot prove its own consistency.

This implied that finitistic methods could not even justify themselves, let alone any stronger theory.

Proof Theory's Goals

Modified Hilbert's Program: Prove the consistency of classical reasoning using constructive (rather than finitary) means.

Kreisel's Program: Extract constructive, computational information from classical reasoning.

Line of attack:

1. Describe formal theories that model classical reasoning about some portion of the mathematical universe.

2. Use mathematical techniques to study these theories as formal objects.

Languages for Arithmetic

The language of first-order arithmetic:

- Constants: 0, S, $+$, $\times$
- Logical Symbols: $\wedge$, $\vee$, $\rightarrow$, $\neg$, $\forall$, $\exists$
- Variables $x_1, x_2, x_3, \ldots$ range over natural numbers

In this language one can code other finitary objects, like sequences and strings.

The language of second-order arithmetic:

- Constants: 0, S, $+$, $\times$
- Logical Symbols: $\wedge$, $\vee$, $\rightarrow$, $\neg$, $\forall$, $\exists$
- Variables $x_1, x_2, x_3, \ldots$ range over natural numbers
- Variables $X_1, X_2, X_3, \ldots$ range over sets of numbers

Using these sets, one can code countably infinite objects, like real numbers and continuous functions.

Peano Arithmetic

PA is a theory in the language of first-order arithmetic, based on the following:

- Logical axioms and rules
- Defining equations for S, $+$, and $\times$
- An induction axiom

  $$\varphi(0) \wedge \forall x\, (\varphi(x) \to \varphi(Sx)) \to \forall x\, \varphi(x)$$

  for every formula $\varphi(x)$.

In PA one can formalize most finitary arguments in number theory and combinatorics.

Arithmetic Comprehension

$\mathbf{ACA_0}$ is a theory in the language of second-order arithmetic, based on the following:

- Logical axioms and rules
- Defining equations for S, $+$, and $\times$
- A single induction axiom

$$0 \in Y \land \forall x\,(x \in Y \rightarrow Sx \in Y) \rightarrow \forall x\,(x \in Y)$$

- A comprehension axiom

$$\exists Y\ \forall x\,(x \in Y \leftrightarrow \varphi(x))$$

  for every arithmetic formula φ.

In the last axiom Y represents the set

$$\{x \in \mathbb{N} \mid \varphi(x)\}.$$

In ACA_0 one can formalize a good deal of calculus, linear algebra, topology, and more.

A Conservation Result

Definition: Say that a theory T_1 is conservative over T_2 for formulas in Γ if, whenever T_1 proves some formula φ in Γ, T_2 proves it as well.

Theorem (folklore): ACA_0 is conservative over PA for arithmetic formulas.

Proof: If PA doesn't prove φ, there is a model M of $PA + \neg\varphi$. Expand this to a model M' of $ACA_0 + \neg\varphi$ by taking the arithmetic sets of M to be the second-order part.

In fact, if M is recursively saturated, M' also satisfies a Σ^1_1 axiom of choice.

The above proof does not provide an effective translation of proofs in ACA_0 to proofs in PA. This can be obtained using a straightforward cut-elimination argument.

Consequences

1. A constructive consistency proof for PA yields a constructive consistency proof for ACA_0.

2. ACA_0 and PA prove the same computable functions to be total.

3. Though calculus, linear algebra, and topology may be useful in proving finitary theorems, they are inessential.

A Speedup Result

On the other hand, we have

Theorem (Solovay): There is a polynomial $p(n)$ and a sequence of formula φ_n, such that for every n there is a proof of φ_n in ACA_0 using $p(n)$ symbols, but any proof of φ_n in PA requires at least 2^0_n symbols.

Proof: Let $\psi(n)$ say "there is a truth definition for Σ^0_n formulas." Then ACA_0 proves $\psi(0)$ and

$$\forall x\ (\psi(x) \to \psi(x+1)).$$

With a bit of cleverness, we can use this to get short proofs of $Con(I\Sigma_{2^0_n})$.

As a result we can say that ACA_0 has a superexponential (in fact, non-elementary) **speedup** over PA.

Another Conservation Result

$\mathbf{RCA_0}$ is a weak subsystem of ACA_0, which includes a restricted form of induction and comprehension for recursive sets. It is conservative over primitive recursive arithmetic (PRA).

$\mathbf{WKL+_0}$ adds a weak version of König's lemma (asserting that every infinite binary tree has a path) and a version of the Baire category theorem. It is strong enough to prove, for example, the Heine-Borel theorem, as well as the completeness and compactness of first-order logic.

Theorem (Harrington, Brown and Simpson): The theory $WKL+_0$ is conservative over RCA_0 for Π^1_1 formulas.

A Noneffective Proof

Lemma: Given a model M of RCA_0, and a tree $T \in M$ one can add a "generic" path through T, and get another model of RCA_0.

$$M \models RCA_0 \rightsquigarrow M[G] \models RCA_0$$

Lemma (Harrington): Every countable model M of RCA_0 can be expanded to a model M' of WKL_0 with the same first order part.

Proof: Keep adding paths through trees.

$$M = M_0 \subseteq M_1 \subseteq M_2 \subseteq \ldots \subseteq M_\omega$$

Lemma (Brown and Simpson): Ditto for $WKL{+}_0$.

Proof: Force to add generic Cohen reals.

An Effective Version

Theorem (Avigad): There is an effective translation of $WKL{+}_0$-proofs to RCA_0-proofs in which the increase in length is polynomially-bounded.

Proof: Formalize forcing in RCA_0. Then if $WKL{+}_0$ proves φ, RCA_0 proves "φ is forced," and hence, for Π^1_1 formulas, φ is true.

Difficulties:

1. Need to formalize forcing in RCA_0 (proper class forcing for (WKL))
2. Need to use strong forcing for (BCT) to keep complexity down
3. Need to name sets that are recursive in the generic
4. Need to iterate the forcing (i.e. define 2-forcing, 3-forcing, etc.)
5. Need to do the iteration uniformly and generically (and keep complexity down)
6. Need to restrict to a definable cut (RCA_0 doesn't have enough induction)

Yet Another Conservation Result

$\mathbf{ATR_0}$ is an extension of ACA_0 which allows one to iterate arithmetic constructions transfinitely, along any well-ordering. It is strong enough to prove some results from descriptive set theory, including Lusin's theorem, open determinacy, and the assertion that open sets are Ramsey.

$\widehat{\mathbf{ID}}_{<\omega}$ is a first-order theory that augments Peano Arithmetic with constants to denote fixed-points of arithmetic inductive definitions.

Theorem (Avigad): ATR_0 is conservative over $\widehat{ID}_{<\omega}$ for arithmetic formulas, but there is a non-elementary speedup.

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

$\mathbf{ATR_0}$ and $\widehat{\mathbf{ID}}_{<\omega}$

ATR_0 extends ACA_0 with a schema that allows one to define sets by *Arithmetic Transfinite Recursion*:

$$\forall \prec (WO(\prec) \rightarrow \exists X \, \forall z \, (X_z = \{y \mid \varphi(y, X^z)\}))$$

Definition: A positive arithmetic operator is given by arithmetic formula $\varphi(x, Y)$ in which the predicate Y occurs positively.

Idea: $\Gamma_\varphi(Y) = \{x | \varphi(x, Y)\}$ satisfies

$$Y \subseteq Z \rightarrow \Gamma_\varphi(Y) \subseteq \Gamma_\varphi(Z)$$

$\widehat{ID}_{<\omega}$ is a theory in the language of first-order arithmetic with extra constants P_φ, and axioms

$$P_\varphi = \{x \mid \varphi(x, P_\varphi)\}.$$

Lemma: (ATR) is equivalent to a second-order version of the $\widehat{ID}$ axioms, namely

$$(FP) \;\; \forall Z \, \exists Y (Y = \{x | \varphi(x, Y, Z)\})$$

Proof: Assuming (FP), show how to build hierarchies along $\prec$ inductively. Conversely, assuming (ATR), show how to get fixed points of positive arithmetic operators by modeling the classical proof, and using a "pseudo-hierarchy."

Functional Intepretations

Suppose we know that

$$\forall x\ \exists y\ \varphi(x, y),$$

where x and y range over natural numbers and φ is some "finitely checkable" property. Then

$$f(x) = \text{the least } y \text{ such that } \varphi(x, y)$$

defines a total recursive (computable) function.

If a theory T proves $\forall x\ \exists y\ \varphi(x, y)$, we can then say that T proves that the function f is total.

Goal: Characterize the types of recursive functions that a theory T can prove to be total.

A Class of Functionals

The finite types are defined inductively as follows:

- $\mathbb{N}$ is a finite type
- if A and B are finite types, so is $A \to B$

The Primitive Recursive Functionals of Finite Type:

- Include 0 and S
- Are closed under explicit definition
- Are closed under primitive recursion:

$$\begin{cases} F(0) & = & G_1 \\ F(Sx) & = & G_2(x, F(x)) \end{cases}$$

The Dialectica Interpretation

Theorem (Gödel): The provably total recursive functions of PA are exactly the primitive recursive functionals of type $\mathbb{N} \to \mathbb{N}$.

Proof: Write down a functional (quantifier-free) theory T whose terms denote the primitive recursive functionals of finite type. From a proof of

$$\forall x \, \exists y \, \varphi(x, y)$$

in PA, one can extract a term f and a proof of

$$\varphi(x, f(x))$$

in T.

2nd-order	**1st-order**	**functions**
WKL_0, RCA_0	$I\Sigma_1$	primitive recursive functions
ACA_0	PA	primitive recursive functionals
ATR_0	$\widehat{ID}_{<\omega}$	???

Question: What kind of computational schema can we use to characterize the provably total recursive functions of stronger theories?

Predicative Functionals

Answer: Use Martin-Löf's notion of *universes* of types, which allow for a kind of "predicative" polymorphism.

Theorem (Avigad): The provably total recursive functions of ATR_0 and $\widehat{ID}_{<\omega}$ are exactly the ones that can be defined using these universes.

More precisely, one can define theories P_n that axiomatize primitive recursive functionals with n such universes. P_0 is just (a logic-free variant of) T and each P_n is just a stripped-down version of ML_n.

Theorem: The provably total recursive functions of $\widehat{ID}_n$ are exactly the ones that are represented by terms of P_n.

The Interpretations

In the theories below, the superscript i denotes an intuitionist variant that avoids the law of the excluded middle. First,

$$ATR_0 \leadsto \widehat{ID}_{<\omega}$$

via a cut-elimination. Then,

$$\begin{aligned} PA &\leadsto PA^i \\ &\leadsto P_0 \end{aligned}$$

is essentially the Dialectica interpretation.

$$\begin{aligned} \widehat{ID}_1 &\leadsto \Sigma^1_1\text{-}AC \\ &\leadsto \Sigma^1_1\text{-}AC^i \\ &\leadsto \textit{Frege-}PA^i \\ &\leadsto P_1. \end{aligned}$$

The last step internalizes the interpretation of PA^i in P_0.

Iterating, we get

$$\begin{aligned}
\widehat{ID}_2 &\rightsquigarrow \Sigma^1_1\text{-}AC(\widehat{ID}_1) \\
&\rightsquigarrow \Sigma^1_1\text{-}AC^i(\widehat{ID}_1^{i+}) \\
&\rightsquigarrow \textit{Frege-}\widehat{ID}_1^{i+} \\
&\rightsquigarrow P_2.
\end{aligned}$$

where the last step internalizes the interpretation of $\widehat{ID}_1^{i+}$ to P_1.

$$\begin{aligned}
\widehat{ID}_3 &\rightsquigarrow \Sigma^1_1\text{-}AC(\widehat{ID}_2) \\
&\rightsquigarrow \Sigma^1_1\text{-}AC^i(\widehat{ID}_2^{i+}) \\
&\rightsquigarrow \textit{Frege-}\widehat{ID}_2^{i+} \\
&\rightsquigarrow P_3.
\end{aligned}$$

And so on . . .

Combinatorial Independences

For any consistent theory T that includes basic arithmetic, Gödel showed how to construct a statement about natural numbers that is true but not provable in T. This statement encodes logical notions, like provability in T itself.

Question: Can we find more natural combinatorial statements that can't be proven in T?

The Paris-Harrington Theorem

If a and b are natural numbers and $a < b$, use $[a, b]$ to denote the set

$$\{a, a+1, a+2, \ldots, b\}.$$

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

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

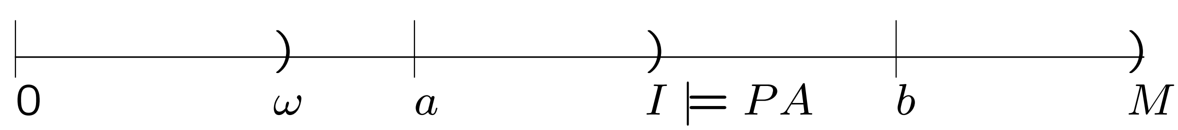
can be proven using the infinitary version Ramsey's theorem.

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

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

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

$$I \models PA.$$



Corollary: PA doesn't prove

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

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

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

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:

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

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

$PH(a, b)$ is the predicate

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

Another Combinatorial Independence

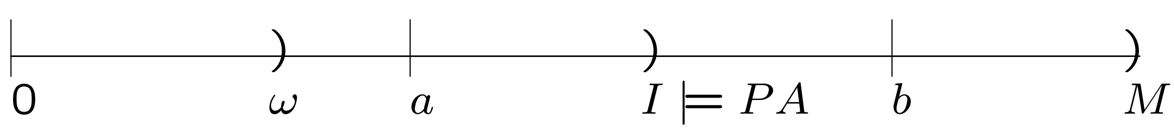
For any ordinal notatation α, Ketonen and Solovay show how to define the finitary combinatorial notion "$[a, b]$ is α-large."

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.

Current Work

Sommer and I have extended these constructions to a number of important predicative theories. Using appropriately large intervals we can obtain sharp upper bounds for the proof theoretic ordinals of RCA_0, WKL_0, ACA_0, Σ^1_1-AC_0, $(\Pi^0_1\text{-}CA)^{<\alpha}$, ACA, Σ^1_1-AC, $\widehat{ID}_n$, ATR_0, ATR.

The World According to a Proof Theorist

Very strong theories are designed to explore powerful assumptions about the mathematical universe.

Strong theories like Zermelo-Fraenkel set theory can formalize most mathematical arguments, and are acceptable to most mathematicians.

Theories of "ordinary strength" correspond roughly to the types of arguments that most mathematicians actually use in day-to-day practice.

Weak theories are concerned with "feasibly computable" objects and are relevant to complexity theory.

Some Subsystems of Analysis

1. RCA_0: Recursive Comprehension

$$\forall x\ (\varphi(x) \leftrightarrow \psi(x)) \rightarrow \exists X\ \forall y\ (y \in X \leftrightarrow \varphi(y))$$

2. WKL_0: Weak König's Lemma

$$\forall T\ (T \text{ an infinite binary tree} \rightarrow \\ \exists P\ (P \text{ a path through } T))$$

3. ACA_0: Arithmetic Comprehension

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

4. ATR_0: Arithmetic Transfinite Recursion

$$\forall \prec\ (WO(\prec) \rightarrow \exists X\ \forall z\ (X_z = \{y \mid \varphi(y, X^z)\}))$$

5. Π^1_1-CA_0: Π^1_1 Comprehension

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

Representative Theorems

1. RCA_0: Recursive Comprehension

   recursive mathematics, intermediate value theorem

2. WKL_0: Weak König's Lemma

   Heine-Borel theorem, compactness and completeness of first-order logic

3. ACA_0: Arithmetic Comprehension

   Bolzano-Weierstrass theorem, least upper bound theorem, Ramsey's theorem for $\mathbb{N}^3$

4. ATR_0: Arithmetic Transfinite Recursion

   comparability of well-orderings, Lusin's theorem, open determinacy, open sets are Ramsey

5. Π^1_1-CA_0: Π^1_1 Comprehension

   Cantor-Bendixson theorem, Silver's theorem, $F_\sigma \cap G_\delta$ sets are Ramsey, Kruskal's theorem

The Theories (ω-Models)

1. RCA_0: Recursive Comprehension

   Turing ideals; the recursive sets

2. WKL_0: Weak König's Lemma

   Scott sets; no minimal

3. ACA_0: Arithmetic Comprehension

   Closure under Turing jump; the arithmetic sets

4. ATR_0: Arithmetic Transfinite Recursion

   no minimal; all contain HYP

5. Π^1_1-CA_0: Π^1_1 Comprehension

   no minimal; all contain HYP

Proof Theory's Methods

1. Study alternate axiomatizations, theorems, interpretations, conservative extensions, natural models
2. Reverse mathematics
3. Ordinal analysis
4. Functional interpretations
5. Combinatorial independences

What next?

1. Extend model-theoretic ordinal analysis to impredicative theories.

2. Find combinatorial independences for impredicative theories, e.g. using the Galvin-Prikry theorem.

3. Give functional interpretations to impredicative theories.

4. Explore model-theoretic and proof-theoretic applications to proof complexity and weak fragments of arithmetic.

5. Explore recursive analogs of large-cardinal axioms and reflection properties.