On circular reasoning and proof theory

Anupam Das[1]

University of Copenhagen

Logic Seminar
Melbourne, 19th December 2018

[1]Supported by a Marie Skłodowska-Curie fellowship, ERC project 753431.

A bad example: 7 is odd (or even?!)

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\vdots}{11 \text{ is odd}}}{10 \text{ is even}}}{9 \text{ is odd}}}{8 \text{ is even}}}{7 \text{ is odd}}$$

A bad example: 7 is odd (or even?!)

$\vdots$	$\vdots$
11 is odd	11 is even
10 is even	10 is odd
9 is odd	9 is even
8 is even	8 is odd
7 is odd	7 is even

This sort of reasoning can be fallacious!

A better example: natural numbers have parity

$$E(x) := \exists y. x = 2y$$
$$O(x) := \exists y. x = 2y + 1$$

$$\dfrac{\dfrac{\dfrac{\overline{\overline{\;\;\;\;\;\;}}}{\Rightarrow E(0)}}{\Rightarrow E(0) \lor O(0)}}{x = 0 \Rightarrow E(x) \lor O(x)} \qquad \dfrac{\dfrac{\dfrac{\vdots}{\Rightarrow E(y) \lor O(y)}\bullet \quad \dfrac{\overline{\overline{\;\;\;\;\;\;}}}{E(y) \Rightarrow O(y+1)} \quad \dfrac{\overline{\overline{\;\;\;\;\;\;}}}{O(y) \Rightarrow E(y+1)}}{\Rightarrow E(y+1) \lor O(y+1)}}{x = y + 1 \Rightarrow E(x) \lor O(y)}$$

$$\dfrac{\dfrac{\cdots}{\Rightarrow E(x) \lor O(x)}\bullet}{\Rightarrow \forall x.(E(x) \lor O(x))}$$

Irrationality of $\sqrt{2}$ via infinite descent

$$\dfrac{\dfrac{\dfrac{}{\Rightarrow 2 \text{ is prime}} \qquad \dfrac{\dfrac{\dfrac{\vdots}{b^2 = 2c^2 \Rightarrow}\,\bullet}{c < a, 4c^2 = 2b^2 \Rightarrow}}{\exists x < a. a = 2x, a^2 = 2b^2 \Rightarrow}}{a^2 = 2b^2 \Rightarrow}\,\bullet}{\Rightarrow \forall x, y.\, x^2 \neq 2y^2}$$

Irrationality of $\sqrt{2}$ via infinite descent

$$\dfrac{\dfrac{\dfrac{}{\Rightarrow 2 \text{ is prime}} \qquad \dfrac{\dfrac{\dfrac{\vdots}{b^2 = 2c^2 \Rightarrow}\,\bullet}{c < a, 4c^2 = 2b^2 \Rightarrow}}{\exists x < a.a = 2x, a^2 = 2b^2 \Rightarrow}}{a^2 = 2b^2 \Rightarrow}\,\bullet}{\Rightarrow \forall x, y.\, x^2 \neq 2y^2}$$

- Apparently non-wellfounded reasoning.
- Why is it sound?

Cyclic proofs

- Proof theory for FOL with inductive defintions.
- (Automated) proofs of program termination in separation logic.
- Proof systems for the modal μ-calculus.
- Metalogical results, like interpolation.
- Proof search procedures.
- ...

Cyclic proofs

- Proof theory for FOL with inductive defintions.
- (Automated) proofs of program termination in separation logic.
- Proof systems for the modal μ-calculus.
- Metalogical results, like interpolation.
- Proof search procedures.
- $\dots$

A motivating abstract question:

Question (Brotherston-Simpson conjecture)

Are inductive proofs and cyclic proofs equally powerful?

Cyclic proofs

- Proof theory for FOL with inductive defintions.
- (Automated) proofs of program termination in separation logic.
- Proof systems for the modal μ-calculus.
- Metalogical results, like interpolation.
- Proof search procedures.
- ...

A motivating abstract question:

Question (Brotherston-Simpson conjecture)

Are inductive proofs and cyclic proofs equally powerful?

This talk is about the special case of **first-order arithmetic**.

Outline

A sequent calculus presentation of PA

A sequent calculus presentation of PA

Peano Arithmetic, written PA, can be specified by a deduction system as follows:

- Δ_0-initial sequents for the instances of Q: defining properties of $\mathsf{0}, \mathsf{s}, +, \times, <$.
- An induction rule:

$$\frac{\Gamma \Rightarrow \Delta, A(\mathsf{0}) \quad \Gamma, A(a) \Rightarrow \Delta, A(\mathsf{s}a)}{\Gamma \Rightarrow \Delta, A(t)}$$

A sequent calculus presentation of PA

Peano Arithmetic, written PA, can be specified by a deduction system as follows:

- Δ_0-initial sequents for the instances of Q: defining properties of $0, \mathsf{s}, +, \times, <$.
- An induction rule:

$$\frac{\Gamma \Rightarrow \Delta, A(0) \quad \Gamma, A(a) \Rightarrow \Delta, A(\mathsf{s}a)}{\Gamma \Rightarrow \Delta, A(t)}$$

- We include an explicit substitution rule for unifying sequents in cycles:

$$\theta\text{-}sub \; \frac{\Gamma \Rightarrow \Delta}{\theta(\Gamma) \Rightarrow \theta(\Delta)}$$

Peano Arithmetic, written PA, can be specified by a deduction system as follows:

- Δ_0-initial sequents for the instances of Q: defining properties of $0, \mathsf{s}, +, \times, <$.
- An induction rule:

$$\frac{\Gamma \Rightarrow \Delta, A(0) \quad \Gamma, A(a) \Rightarrow \Delta, A(\mathsf{s}a)}{\Gamma \Rightarrow \Delta, A(t)}$$

- We include an explicit substitution rule for unifying sequents in cycles:

$$\theta\text{-}sub \frac{\Gamma \Rightarrow \Delta}{\theta(\Gamma) \Rightarrow \theta(\Delta)}$$

Definition

$I\Phi$ is the fragment of PA where induction is restricted to formulae $A \in \Phi$. In particular $I\Sigma_n$ has induction only on formulae $\exists x_1.\forall x_2. \dots .Qx_n.A$, with A recursive.

Proposition (Folklore)

For $n \geq 0$ we have that $I\Sigma_n = I\Pi_n$.

Proposition (Folklore)

For $n \geq 0$ we have that $I\Sigma_n = I\Pi_n$.

Theorem ((Free-)cut elimination)

If $\mathsf{PA} \vdash S(\vec{a})$, then there is a sequent proof π of $S(\vec{a})$ containing only subformulae of $S(\vec{a})$, an induction formula of π or an initial sequent of π.

Proposition (Folklore)

For $n \geq 0$ we have that $I\Sigma_n = I\Pi_n$.

Theorem ((Free-)cut elimination)

If $\mathsf{PA} \vdash S(\vec{a})$, then there is a sequent proof π of $S(\vec{a})$ containing only subformulae of $S(\vec{a})$, an induction formula of π or an initial sequent of π.

Corollary

For $n \geq 0$, if $I\Sigma_{n+1} \vdash \forall \vec{x}.\varphi(\vec{x})$, for $\varphi \in \Sigma_n$, then $\Rightarrow \varphi(\vec{a})$ has a sequent proof containing only Σ_n formulae.

Non-wellfounded arithmetic (Simpson '12)

Definition (Precursors and traces)

A **preproof** is a locally correct infinite derivation tree.

Definition (Precursors and traces)

A **preproof** is a locally correct infinite derivation tree. Let $(S_i)_i$ be an infinite branch of a preproof. We say t' is a precursor of t at i if:

- S_i concludes a θ-*sub* step and $t = \theta(t')$; or
- S_i concludes any other step and t' is t; or
- S_i concludes any other step and $t = t'$ occurs in the antecedent of S_i.

Definition (Precursors and traces)

A **preproof** is a locally correct infinite derivation tree. Let $(S_i)_i$ be an infinite branch of a preproof. We say t' is a precursor of t at i if:

- S_i concludes a θ-*sub* step and $t = \theta(t')$; or
- S_i concludes any other step and t' is t; or
- S_i concludes any other step and $t = t'$ occurs in the antecedent of S_i.

A **trace** along an infinite branch $(S_i)_i$ is a sequence $(t_i)_{i \geq n}$ such that:

1. t_i is a a precursor of t_{i+1}; or
2. $t_{i+1} < t_i$ occurs in the antecedent of S_i. (a ‘progress point’)

Definition (Precursors and traces)

A **preproof** is a locally correct infinite derivation tree. Let $(S_i)_i$ be an infinite branch of a preproof. We say t' is a precursor of t at i if:

- S_i concludes a *θ-sub* step and $t = \theta(t')$; or
- S_i concludes any other step and t' is t; or
- S_i concludes any other step and $t = t'$ occurs in the antecedent of S_i.

A **trace** along an infinite branch $(S_i)_i$ is a sequence $(t_i)_{i \geq n}$ such that:

1. t_i is a a precursor of t_{i+1}; or
2. $t_{i+1} < t_i$ occurs in the antecedent of S_i. (a 'progress point')

Definition (∞-proofs)

A ∞**-proof** (or just 'proof') is a preproof where each infinite branch has an infinitely progressing trace.

Irrationality of $\sqrt{2}$ again

$$\dfrac{\dfrac{\dfrac{}{\Rightarrow 2 \text{ is prime}} \qquad \dfrac{\dfrac{\dfrac{\vdots}{b^2 = 2c^2 \Rightarrow}\,\bullet}{\underline{c < a}, 4c^2 = 2b^2 \Rightarrow}}{\exists x < a. a = 2x, a^2 = 2b^2 \Rightarrow}}{a^2 = 2b^2 \Rightarrow}\,\bullet}{\Rightarrow \forall x, y.\, x^2 \neq 2y^2}$$

Irrationality of $\sqrt{2}$ again

$$\dfrac{\dfrac{\dfrac{}{\Rightarrow 2 \text{ is prime}} \qquad \dfrac{\dfrac{\dfrac{\vdots}{b^2 = 2c^2 \Rightarrow}\,\bullet}{\underline{c < a}, 4c^2 = 2b^2 \Rightarrow}}{\exists x < a. a = 2x, a^2 = 2b^2 \Rightarrow}}{a^2 = 2b^2 \Rightarrow}\,\bullet}{\Rightarrow \forall x, y.\, x^2 \neq 2y^2}$$

There is an infinitely progressing trace $(a, c, b)^\omega$.

Soundness of ∞-proofs

Theorem (folklore)

If A has a ∞-proof, then $\mathbb{N} \models A$.

Theorem (folklore)
If A has a ∞-proof, then $\mathbb{N} \models A$.

Proof idea.

- Suppose otherwise, and build a branch of invalid sequents $(S_i)_i$.
- Simultaneously build assignments ρ_i witnessing the invalidity.

Theorem (folklore)
If A has a ∞-proof, then $\mathbb{N} \models A$.

Proof idea.

- Suppose otherwise, and build a branch of invalid sequents $(S_i)_i$.
- Simultaneously build assignments ρ_i witnessing the invalidity.
- By definition, there is an infinitely progressing trace $(t_i)_{i \geq n}$ along $(S_i)_i$.
- Can induce an infinite descending sequence $\rho_{i_1}(t_{i_1}) > \rho_{i_2}(t_{i_2}) > \cdots$ □

A finitary fragment: the cyclic proofs

A finitary fragment: the cyclic proofs

Definition
A cyclic proof is a ∞-proof with only finitely many distinct subtrees.

A finitary fragment: the cyclic proofs

Definition

A cyclic proof is a ∞-proof with only finitely many distinct subtrees. CA is the theory of sentences that have cyclic proofs.

Proposition (folklore)

We can effectively check if a finite graph is a correct cyclic proof.

Definition

A cyclic proof is a ∞-proof with only finitely many distinct subtrees. CA is the theory of sentences that have cyclic proofs.

Proposition (folklore)

We can effectively check if a finite graph is a correct cyclic proof.

Proof.

Let π be a regular preproof. Define:

- $\mathcal{A}_b^\pi$ a (deterministic) Büchi automaton recognising infinite branches of π.
- $\mathcal{A}_t^\pi$ a NBA recognising branches of π with an infinitely progressing trace.

Now simply check if $\mathcal{L}(\mathcal{A}_b^\pi) \subseteq \mathcal{L}(\mathcal{A}_t^\pi)$. $\square$

Definition
A cyclic proof is a ∞-proof with only finitely many distinct subtrees. CA is the theory of sentences that have cyclic proofs.

Proposition (folklore)
We can effectively check if a finite graph is a correct cyclic proof.

Proof.
Let π be a regular preproof. Define:

- $\mathcal{A}_b^\pi$ a (deterministic) Büchi automaton recognising infinite branches of π.
- $\mathcal{A}_t^\pi$ a NBA recognising branches of π with an infinitely progressing trace.

Now simply check if $\mathcal{L}(\mathcal{A}_b^\pi) \subseteq \mathcal{L}(\mathcal{A}_t^\pi)$. □

NB: inclusion of Büchi automata is **PSPACE**-complete.

Outline

Previous work

Previous work

Theorem (Simpson '11)

CA = PA.

Previous work

Theorem (Simpson '11)

$\mathsf{CA} = \mathsf{PA}$.

- Formalises soundness argument for ∞-proofs in an appropriate fragment of SO arithmetic (ACA_0).
- (Basic automaton theory for ω-languages, can be carried out in ACA_0.)

Theorem (Simpson '11)
$\mathsf{CA} = \mathsf{PA}$.

- Formalises soundness argument for ∞-proofs in an appropriate fragment of SO arithmetic (ACA_0).
- (Basic automaton theory for ω-languages, can be carried out in ACA_0.)
- The result for PA is obtained by conservativity of ACA_0 over PA.

Previous work

Theorem (Simpson '11)

CA = PA.

- Formalises soundness argument for ∞-proofs in an appropriate fragment of SO arithmetic (ACA_0).
- (Basic automaton theory for ω-languages, can be carried out in ACA_0.)
- The result for PA is obtained by conservativity of ACA_0 over PA.
- Possibly non-elementary blowup in proof size, due to non-uniformity.

Previous work

Theorem (Simpson '11)
CA = PA.

- Formalises soundness argument for ∞-proofs in an appropriate fragment of SO arithmetic (ACA_0).
- (Basic automaton theory for ω-languages, can be carried out in ACA_0.)
- The result for PA is obtained by conservativity of ACA_0 over PA.
- Possibly non-elementary blowup in proof size, due to non-uniformity.

Theorem (Implicit in Berardi & Tatsuta '17)
$\mathsf{CA} + \mathcal{I} = \mathsf{PA} + \mathcal{I}$ *for any set of Martin-Löf ordinary inductive definitions* $\mathcal{I}$ *and their associated rules.*

- 'Structural' argument, relying on proof-level manipulations.

Previous work

Theorem (Simpson '11)
CA = PA.

- Formalises soundness argument for ∞-proofs in an appropriate fragment of SO arithmetic (ACA_0).
- (Basic automaton theory for ω-languages, can be carried out in ACA_0.)
- The result for PA is obtained by conservativity of ACA_0 over PA.
- Possibly non-elementary blowup in proof size, due to non-uniformity.

Theorem (Implicit in Berardi & Tatsuta '17)
$\mathsf{CA} + \mathcal{I} = \mathsf{PA} + \mathcal{I}$ *for any set of Martin-Löf ordinary inductive definitions* $\mathcal{I}$ *and their associated rules.*

- 'Structural' argument, relying on proof-level manipulations.
- Relies on some nontrivial infinitary combinatorics specialised to arithmetic.

Previous work

Theorem (Simpson '11)
$\mathsf{CA} = \mathsf{PA}$.

- Formalises soundness argument for ∞-proofs in an appropriate fragment of SO arithmetic (ACA_0).
- (Basic automaton theory for ω-languages, can be carried out in ACA_0.)
- The result for PA is obtained by conservativity of ACA_0 over PA.
- Possibly non-elementary blowup in proof size, due to non-uniformity.

Theorem (Implicit in Berardi & Tatsuta '17)
$\mathsf{CA} + \mathcal{I} = \mathsf{PA} + \mathcal{I}$ *for any set of Martin-Löf ordinary inductive definitions* $\mathcal{I}$ *and their associated rules.*

- 'Structural' argument, relying on proof-level manipulations.
- Relies on some nontrivial infinitary combinatorics specialised to arithmetic.
- High logical complexity.

Definition

Write $C\Sigma_n$ for the theory axiomatised by the universal closures of CA proofs containing only Σ_n-formulae.

NB: A $C\Sigma_n$ proof of a Σ_n sequent will contain only Σ_n formulae anyway, by free-cut elimination.

Definition

Write $C\Sigma_n$ for the theory axiomatised by the universal closures of CA proofs containing only Σ_n-formulae.

NB: A $C\Sigma_n$ proof of a Σ_n sequent will contain only Σ_n formulae anyway, by free-cut elimination.

Question (Simpson '17)

1. *How does the logical complexity of* CA *and* PA *compare?*
   Does $C\Sigma_m = I\Sigma_n$ for appropriately chosen m, n?

Some questions

Definition

Write $C\Sigma_n$ for the theory axiomatised by the universal closures of CA proofs containing only Σ_n-formulae.

NB: A $C\Sigma_n$ proof of a Σ_n sequent will contain only Σ_n formulae anyway, by free-cut elimination.

Question (Simpson '17)

1. *How does the logical complexity of* CA *and* PA *compare?*
   Does $C\Sigma_m = I\Sigma_n$ *for appropriately chosen* m, n*?*
2. *How does the proof complexity of* PA *and* CA *compare?*

Definition

Write $C\Sigma_n$ for the theory axiomatised by the universal closures of CA proofs containing only Σ_n-formulae.

NB: A $C\Sigma_n$ proof of a Σ_n sequent will contain only Σ_n formulae anyway, by free-cut elimination.

Question (Simpson '17)

1. *How does the logical complexity of* CA *and* PA *compare?*
   Does $C\Sigma_m = I\Sigma_n$ *for appropriately chosen* m, n*?*
2. *How does the proof complexity of* PA *and* CA *compare?*
3. *Does cut-admissibility hold for any non-trivial fragment of* CA*?*

Digression: calibrating intuitions

Digression: calibrating intuitions

It is tempting to think that $I\Sigma_n = C\Sigma_n$.

Digression: calibrating intuitions

It is tempting to think that $I\Sigma_n = C\Sigma_n$. However this is not the case:

Example (Simpson '17)

Recall the Ackermann-Péter function:

$$A(x, y) = \begin{cases} y+1 & x = 0 \\ A(x-1, 1, z) & x > 0, y = 0 \\ A(x-1, A(x, y-1)) & x, y > 0 \end{cases}$$

Let $A(x, y, z)$ be an appropriate Σ_1 formula computing its graph.

It is tempting to think that $I\Sigma_n = C\Sigma_n$. However this is not the case:

Example (Simpson '17)

Recall the Ackermann-Péter function:

$$A(x,y) \;=\; \begin{cases} y+1 & x=0 \\ A(x-1,1,z) & x>0, y=0 \\ A(x-1, A(x,y-1)) & x,y>0 \end{cases}$$

Let $A(x,y,z)$ be an appropriate Σ_1 formula computing its graph. We have:

$$\dfrac{\dfrac{}{x=0 \Rightarrow A(x,y,y+1)} \qquad \dfrac{\dfrac{\begin{matrix}\vdots \\ \overset{(A)}{\Rightarrow} \exists z.A(x-1,1,z)\end{matrix}}{x>0, y=0 \Rightarrow \exists z.A(x,y,z)} \qquad \dfrac{\dfrac{\begin{matrix}\vdots \\ \overset{(B)}{\Rightarrow} \exists z.A(x,y-1,z)\end{matrix} \qquad \begin{matrix}\vdots \\ \overset{(C)}{\Rightarrow} \exists z.A(x-1,y',z)\end{matrix}}{\Rightarrow \exists z, y'.\, A(x,y-1,y') \wedge A(x-1,y',z)}}{x, y>0 \Rightarrow \exists z.\, A(x,y,z)}}{x>0 \Rightarrow \exists z.A(x,y,z)}}{\Rightarrow \exists z.A(x,y,z)}$$

On the other hand, some intuitions have simple proofs:

Proposition

For $n \geq 0$, $C\Sigma_n = C\Pi_n$.

On the other hand, some intuitions have simple proofs:

Proposition

For $n \geq 0$, $C\Sigma_n = C\Pi_n$.

Proof.

Simply replace every sequent $\vec{p}, \Gamma \Rightarrow \Delta$ with $\vec{p}, \bar{\Gamma} \Rightarrow \bar{\Delta}$, where $\vec{p}$ exhausts all atomic formulae in the antecedent. □

Summary of contribution

Summary of contribution

Theorem
$C\Sigma_n = I\Sigma_{n+1}$, over Π_{n+1} theorems.

Summary of contribution

Theorem
$C\Sigma_n = I\Sigma_{n+1}$, over Π_{n+1} theorems.

$\supseteq$: by structural methods manipulating normal forms of inductive proofs.

Summary of contribution

Theorem
$C\Sigma_n = I\Sigma_{n+1}$, over Π_{n+1} theorems.

- $\supseteq$: by structural methods manipulating normal forms of inductive proofs.
- $\subseteq$: soundness argument can be formalised in conservative SO extensions.

Summary of contribution

Theorem
$C\Sigma_n = I\Sigma_{n+1}$, *over* Π_{n+1} *theorems.*

- $\supseteq$: by structural methods manipulating normal forms of inductive proofs.
- $\subseteq$: soundness argument can be formalised in conservative SO extensions.

Theorem
PA *and* CA *proof size differs only elementarily.*

Summary of contribution

Theorem
$C\Sigma_n = I\Sigma_{n+1}$, over Π_{n+1} theorems.

- $\supseteq$: by structural methods manipulating normal forms of inductive proofs.
- $\subseteq$: soundness argument can be formalised in conservative SO extensions.

Theorem
PA *and* CA *proof size differs only elementarily.*

Proof idea.
Soundness argument can be made uniform in PA. Relies on:

- Deterministic acceptance of branch automaton is arithmetical.
- Well-foundedness of only finite ordinals is needed for the argument.
- $\rightsquigarrow$ arithmetical approximation of non-deterministic acceptance. □

Outline

Main lemma

Lemma

Let π be a $I\Pi_{n+1}$ proof, containing only Π_{n+1} formulae, of

$$\Gamma, \forall x_1.A_1, \dots, \forall x_l.A_l \Rightarrow \Delta, \forall y_1.B_1, \dots, \forall y_m.B_m \qquad (\star)$$

where Γ, Δ, A_i, B_j are Σ_n and $\vec{x}, \vec{y}$ occur only in $\vec{A}, \vec{B}$ respectively.

Main lemma

Lemma

Let π be a $I\Pi_{n+1}$ proof, containing only Π_{n+1} formulae, of

$$\Gamma, \forall x_1.A_1, \ldots, \forall x_l.A_l \Rightarrow \Delta, \forall y_1.B_1, \ldots, \forall y_m.B_m \qquad (\star)$$

where Γ, Δ, A_i, B_j are Σ_n and $\vec{x}, \vec{y}$ occur only in $\vec{A}, \vec{B}$ respectively.

Then there is a $C\Sigma_n$ derivation $\lceil \pi \rceil$ of the form:

$$\{\Gamma \Rightarrow \Delta, A_i\}_{i \leq l}$$

$$\lceil \pi \rceil$$

$$\Gamma \Rightarrow \Delta, B_1, \ldots, B_m$$

Moreover, no free variables of $(\star)$ occur as eigenvariables in $\lceil \pi \rceil$.

Translation of an induction step to a cyclic proof, idea

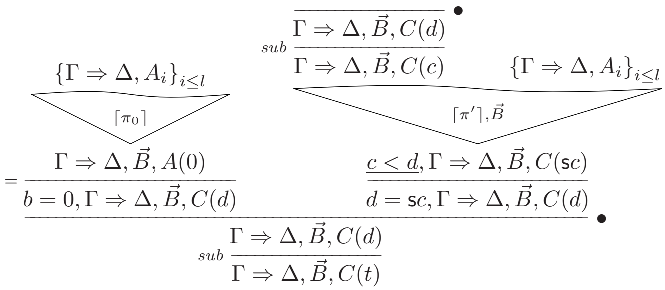
If π extends proofs π_0, π' by an induction step,

$$\text{\textit{ind}}\ \frac{\Gamma, \forall\vec{x}.\vec{A} \Rightarrow \Delta, \forall\vec{y}.\vec{B}, \forall z.C(0) \quad \Gamma, \forall\vec{x}.\vec{A}, \forall z.C(c) \Rightarrow \Delta, \forall\vec{y}.\vec{B}, \forall z.C(\mathsf{s}c)}{\Gamma, \forall\vec{x}.\vec{A} \Rightarrow \Delta, \forall\vec{y}.\vec{B}, \forall x.C(t)}$$

If π extends proofs π_0, π' by an induction step,

$$\frac{\Gamma, \forall\vec{x}.\vec{A} \Rightarrow \Delta, \forall\vec{y}.\vec{B}, \forall z.C(0) \qquad \Gamma, \forall\vec{x}.\vec{A}, \forall z.C(c) \Rightarrow \Delta, \forall\vec{y}.\vec{B}, \forall z.C(\mathsf{s}c)}{\Gamma, \forall\vec{x}.\vec{A} \Rightarrow \Delta, \forall\vec{y}.\vec{B}, \forall x.C(t)}\ \mathit{ind}$$

we define $\lceil \pi \rceil$ to be the following cyclic proof:



Outline

Reverse mathematics of ω-word automata

Reason about infinite words/sets in conservative SO extensions of FO arithmetic.

$$\mathsf{RCA}_0 \approx I\Sigma_1 \approx \text{ primitive recursive arithmetic}$$

Reason about infinite words/sets in conservative SO extensions of FO arithmetic.

$$\mathsf{RCA}_0 \approx I\Sigma_1 \approx \text{ primitive recursive arithmetic}$$

For an appropriate formalisation of NBA complementation, we have:

Theorem (Kolodziejczyk, Michalewski, Pradic & Skrzypczak '16)

$$\mathsf{RCA}_0 + \Sigma^0_2\text{-}\mathsf{IND} \vdash \forall\, NBA\, \mathcal{A}.\, \forall X.\, (X \in \mathcal{L}(\mathcal{A}^c) \equiv X \notin \mathcal{L}(\mathcal{A})) \qquad (1)$$

Reason about infinite words/sets in conservative SO extensions of FO arithmetic.

$$\mathsf{RCA}_0 \approx I\Sigma_1 \approx \text{ primitive recursive arithmetic}$$

For an appropriate formalisation of NBA complementation, we have:

Theorem (Kolodziejczyk, Michalewski, Pradic & Skrzypczak '16)

$$\mathsf{RCA}_0 + \Sigma^0_2\text{-}\mathsf{IND} \vdash \forall\, NBA\, \mathcal{A}.\ \forall X.\ (X \in \mathcal{L}(\mathcal{A}^c) \equiv X \notin \mathcal{L}(\mathcal{A})) \tag{1}$$

Moreover, for each NBA $\mathcal{A}$, we have:

$$\mathsf{RCA}_0 \vdash \forall X.\ (X \in \mathcal{L}(\mathcal{A}^c) \equiv X \notin \mathcal{L}(\mathcal{A})) \tag{2}$$

Reason about infinite words/sets in conservative SO extensions of FO arithmetic.

$$\mathsf{RCA}_0 \approx I\Sigma_1 \approx \text{ primitive recursive arithmetic}$$

For an appropriate formalisation of NBA complementation, we have:

Theorem (Kolodziejczyk, Michalewski, Pradic & Skrzypczak '16)

$$\mathsf{RCA}_0 + \Sigma^0_2\text{-}\mathsf{IND} \vdash \forall\, NBA\, \mathcal{A}.\, \forall X.\, (X \in \mathcal{L}(\mathcal{A}^c) \equiv X \notin \mathcal{L}(\mathcal{A})) \qquad (1)$$

Moreover, for each NBA $\mathcal{A}$, we have:

$$\mathsf{RCA}_0 \vdash \forall X.\, (X \in \mathcal{L}(\mathcal{A}^c) \equiv X \notin \mathcal{L}(\mathcal{A})) \qquad (2)$$

NB: (2) is implicit in that work. It is not trivial!

From cycles to induction

From cycles to induction

Write $\mathrm{ArAcc}(X, \mathcal{A}_2)$ for:

"eventually, there are runs of X on $\mathcal{A}_2$ hitting final states arbitrarily often"

From cycles to induction

Write $\mathrm{ArAcc}(X, \mathcal{A}_2)$ for:

"eventually, there are runs of X on $\mathcal{A}_2$ hitting final states arbitrarily often"

Theorem

$I\Sigma_1(X)$ + "$\mathcal{A}_2$ has a complement" proves:

$$\forall \, DBA \, \mathcal{A}_1.(\text{“}\mathcal{A}_1 \subseteq \mathcal{A}_2\text{”} \wedge X \in \mathcal{L}(\mathcal{A}_1)) \supset \mathrm{ArAcc}(X, \mathcal{A}_2)$$

Write $\mathrm{ArAcc}(X, \mathcal{A}_2)$ for:

"eventually, there are runs of X on $\mathcal{A}_2$ hitting final states arbitrarily often"

Theorem

$I\Sigma_1(X)$ + "$\mathcal{A}_2$ has a complement" proves:

$$\forall \mathit{DBA}\ \mathcal{A}_1.(\text{"}\mathcal{A}_1 \subseteq \mathcal{A}_2\text{"} \wedge X \in \mathcal{L}(\mathcal{A}_1)) \supset \mathrm{ArAcc}(X, \mathcal{A}_2)$$

- $X \in \mathcal{L}(\mathcal{A}_1)$ is arithmetical due to determinism.
- (Emptiness, unions and intersections of NBA formalisable in RCA_0.)

From cycles to induction

Write $\mathrm{ArAcc}(X, \mathcal{A}_2)$ for:

"eventually, there are runs of X on $\mathcal{A}_2$ hitting final states arbitrarily often"

Theorem
$I\Sigma_1(X)$ + "$\mathcal{A}_2$ has a complement" proves:

$$\forall \, DBA \, \mathcal{A}_1.(\text{"}\mathcal{A}_1 \subseteq \mathcal{A}_2\text{"} \wedge X \in \mathcal{L}(\mathcal{A}_1)) \supset \mathrm{ArAcc}(X, \mathcal{A}_2)$$

- $X \in \mathcal{L}(\mathcal{A}_1)$ is arithmetical due to determinism.
- (Emptiness, unions and intersections of NBA formalisable in RCA_0.)

The soundness argument of $C\Sigma_n$ constructs a Δ_{n+1}-definable invalid branch,

From cycles to induction

Write $\mathrm{ArAcc}(X, \mathcal{A}_2)$ for:

"eventually, there are runs of X on $\mathcal{A}_2$ hitting final states arbitrarily often"

Theorem

$I\Sigma_1(X)$ + "$\mathcal{A}_2$ has a complement" proves:

$$\forall\, DBA\ \mathcal{A}_1.(\text{“}\mathcal{A}_1 \subseteq \mathcal{A}_2\text{”} \wedge X \in \mathcal{L}(\mathcal{A}_1)) \supset \mathrm{ArAcc}(X, \mathcal{A}_2)$$

- $X \in \mathcal{L}(\mathcal{A}_1)$ is arithmetical due to determinism.
- (Emptiness, unions and intersections of NBA formalisable in RCA_0.)

The soundness argument of $C\Sigma_n$ constructs a Δ_{n+1}-definable invalid branch, so:

Corollary

1. PA *elementarily simulates* CA.
2. $I\Sigma_{n+1} \supseteq C\Sigma_n$.

Outline

Provably recursive functions of $C\Delta_0$

- For $n \geq 1$, the provably recursive functions of $C\Sigma_n$ are just those of $I\Sigma_{n+1}$.

Provably recursive functions of $C\Delta_0$

- For $n \geq 1$, the provably recursive functions of $C\Sigma_n$ are just those of $I\Sigma_{n+1}$.
- However $C\Delta_0$ is Π_1-axiomatised, so by Parikh's theorem we have:

Corollary

The provably recursive functions of $C\Delta_0$ are just those of $I\Delta_0$, i.e. the linear-time hierarchy.

Provably recursive functions of $C\Delta_0$

- For $n \geq 1$, the provably recursive functions of $C\Sigma_n$ are just those of $I\Sigma_{n+1}$.
- However $C\Delta_0$ is Π_1-axiomatised, so by Parikh's theorem we have:

Corollary

The provably recursive functions of $C\Delta_0$ are just those of $I\Delta_0$, i.e. the linear-time hierarchy.

Failure of cut-admissibility

Provably recursive functions of $C\Delta_0$

- For $n \geq 1$, the provably recursive functions of $C\Sigma_n$ are just those of $I\Sigma_{n+1}$.
- However $C\Delta_0$ is Π_1-axiomatised, so by Parikh's theorem we have:

Corollary

The provably recursive functions of $C\Delta_0$ are just those of $I\Delta_0$, i.e. the linear-time hierarchy.

Failure of cut-admissibility

Corollary

For $n \geq 1$, the class of CA *proofs with only Σ_{n-1} cuts is not complete for $C\Sigma_n$.*

Provably recursive functions of $C\Delta_0$

- For $n \geq 1$, the provably recursive functions of $C\Sigma_n$ are just those of $I\Sigma_{n+1}$.
- However $C\Delta_0$ is Π_1-axiomatised, so by Parikh's theorem we have:

Corollary

The provably recursive functions of $C\Delta_0$ are just those of $I\Delta_0$, i.e. the linear-time hierarchy.

Failure of cut-admissibility

Corollary

For $n \geq 1$, the class of CA *proofs with only Σ_{n-1} cuts is not complete for $C\Sigma_n$.*

Proof.

- $I\Sigma_{n+1} \vdash \mathsf{Con}_{I\Sigma_n}$ so $C\Sigma_n \vdash \mathsf{Con}_{I\Sigma_n}$ by Π_{n+1}-conservativity.

Provably recursive functions of $C\Delta_0$

- For $n \geq 1$, the provably recursive functions of $C\Sigma_n$ are just those of $I\Sigma_{n+1}$.
- However $C\Delta_0$ is Π_1-axiomatised, so by Parikh's theorem we have:

Corollary

The provably recursive functions of $C\Delta_0$ are just those of $I\Delta_0$, i.e. the linear-time hierarchy.

Failure of cut-admissibility

Corollary

For $n \geq 1$, the class of CA proofs with only Σ_{n-1} cuts is not complete for $C\Sigma_n$.

Proof.

- $I\Sigma_{n+1} \vdash \mathsf{Con}_{I\Sigma_n}$ so $C\Sigma_n \vdash \mathsf{Con}_{I\Sigma_n}$ by Π_{n+1}-conservativity.
- On the other hand, $C\Sigma_{n-1} \nvdash \mathsf{Con}_{I\Sigma_n}$ since otherwise $I\Sigma_n \vdash \mathsf{Con}_{I\Sigma_n}$. □

Reflection and consistency

Reflection and consistency

Rephrasing our results in terms of logical strength, we have:

Corollary

For $n \geq 0$, $I\Sigma_{n+2} \vdash \Pi_{n+1}\text{-}\mathsf{Rfn}_{C\Sigma_n}$.

Reflection and consistency

Rephrasing our results in terms of logical strength, we have:

Corollary

For $n \geq 0$, $I\Sigma_{n+2} \vdash \Pi_{n+1}\text{-}\mathsf{Rfn}_{C\Sigma_n}$. *In particular we have* $I\Sigma_{n+2} \vdash \mathsf{Con}_{C\Sigma_n}$.

Incompleteness

Reflection and consistency

Rephrasing our results in terms of logical strength, we have:

Corollary

For $n \geq 0$, $I\Sigma_{n+2} \vdash \Pi_{n+1}\text{-}\mathsf{Rfn}_{C\Sigma_n}$. *In particular we have* $I\Sigma_{n+2} \vdash \mathsf{Con}_{C\Sigma_n}$.

Incompleteness

Unsurprisingly, we have Gödel incompleteness for all fragments $C\Sigma_n$.

Reflection and consistency

Rephrasing our results in terms of logical strength, we have:

Corollary

For $n \geq 0$, $I\Sigma_{n+2} \vdash \Pi_{n+1}\text{-}\mathsf{Rfn}_{C\Sigma_n}$. *In particular we have* $I\Sigma_{n+2} \vdash \mathsf{Con}_{C\Sigma_n}$.

Incompleteness

Unsurprisingly, we have Gödel incompleteness for all fragments $C\Sigma_n$.

In particular, we have:

Corollary

For $n \geq 0$, $I\Sigma_{n+1} \nvdash \mathsf{Con}_{C\Sigma_n}$.

Reflection and consistency

Rephrasing our results in terms of logical strength, we have:

Corollary

For $n \geq 0$, $I\Sigma_{n+2} \vdash \Pi_{n+1}\text{-}\mathsf{Rfn}_{C\Sigma_n}$. *In particular we have* $I\Sigma_{n+2} \vdash \mathsf{Con}_{C\Sigma_n}$.

Incompleteness

Unsurprisingly, we have Gödel incompleteness for all fragments $C\Sigma_n$.

In particular, we have:

Corollary

For $n \geq 0$, $I\Sigma_{n+1} \nvdash \mathsf{Con}_{C\Sigma_n}$.

Proof.

Otherwise $C\Sigma_n \vdash \mathsf{Con}_{C\Sigma_n}$ by Π_{n+1}-conservativity. □

Reverse mathematics of McNaughton's theorem

In fact, there is a curious consequence for ω-automaton theory.

In fact, there is a curious consequence for ω-automaton theory.

Theorem

A natural formulation of McNaughton's theorem, that every NBA has an equivalent deterministic parity automaton, is not provable in RCA_0.

In fact, there is a curious consequence for ω-automaton theory.

Theorem

A natural formulation of McNaughton's theorem, that every NBA has an equivalent deterministic parity automaton, is not provable in RCA_0.

Proof idea.

- If $\mathcal{A}_1$ is a DBA, we can check $\mathcal{L}(\mathcal{A}_1) \subseteq \mathcal{L}(\mathcal{A}_2)$ by complementing $\mathcal{A}_1$ in RCA_0 and checking for universality of $\mathcal{A}_1^c \cup \mathcal{A}_2$.

In fact, there is a curious consequence for ω-automaton theory.

Theorem

A natural formulation of McNaughton's theorem, that every NBA has an equivalent deterministic parity automaton, is not provable in RCA_0.

Proof idea.

- If $\mathcal{A}_1$ is a DBA, we can check $\mathcal{L}(\mathcal{A}_1) \subseteq \mathcal{L}(\mathcal{A}_2)$ by complementing $\mathcal{A}_1$ in RCA_0 and checking for universality of $\mathcal{A}_1^c \cup \mathcal{A}_2$.
- (Given McNaughton, we may check universality already in RCA_0).

Reverse mathematics of McNaughton's theorem

In fact, there is a curious consequence for ω-automaton theory.

Theorem

A natural formulation of McNaughton's theorem, that every NBA has an equivalent deterministic parity automaton, is not provable in RCA_0.

Proof idea.

- If $\mathcal{A}_1$ is a DBA, we can check $\mathcal{L}(\mathcal{A}_1) \subseteq \mathcal{L}(\mathcal{A}_2)$ by complementing $\mathcal{A}_1$ in RCA_0 and checking for universality of $\mathcal{A}_1^c \cup \mathcal{A}_2$.
- (Given McNaughton, we may check universality already in RCA_0).
- This allows us to formalise, say, the soundness of $C\Delta_0$ already in $I\Sigma_1$, contradicting Gödel's second incompletess result for $C\Delta_0$. □

In fact, there is a curious consequence for ω-automaton theory.

Theorem

A natural formulation of McNaughton's theorem, that every NBA has an equivalent deterministic parity automaton, is not provable in RCA_0.

Proof idea.

- If $\mathcal{A}_1$ is a DBA, we can check $\mathcal{L}(\mathcal{A}_1) \subseteq \mathcal{L}(\mathcal{A}_2)$ by complementing $\mathcal{A}_1$ in RCA_0 and checking for universality of $\mathcal{A}_1^c \cup \mathcal{A}_2$.
- (Given McNaughton, we may check universality already in RCA_0).
- This allows us to formalise, say, the soundness of $C\Delta_0$ already in $I\Sigma_1$, contradicting Gödel's second incompletess result for $C\Delta_0$. □

This was not known before!

Outline

Summary and open questions

Optimal logical complexity result. In fact:

Corollary

$C\Sigma_n$ is precisley the Π_{n+1} consequences of $I\Sigma_{n+1}$.

Optimal logical complexity result. In fact:

Corollary

$C\Sigma_n$ is precisley the Π_{n+1} consequences of $I\Sigma_{n+1}$.

Proof complexity differs only elementarily. In fact:

Corollary

PA *exponentially simulates* CA. *This is optimal, unless there is a more efficient way to check cyclic proof soundness.*

Summary and open questions

Optimal logical complexity result. In fact:

Corollary

$C\Sigma_n$ is precisley the Π_{n+1} consequences of $I\Sigma_{n+1}$.

Proof complexity differs only elementarily. In fact:

Corollary

PA *exponentially simulates* CA. *This is optimal, unless there is a more efficient way to check cyclic proof soundness.*

Question

What is the logical strength of McNaughton's theorem, in general?

Optimal logical complexity result. In fact:

Corollary

$C\Sigma_n$ is precisley the Π_{n+1} consequences of $I\Sigma_{n+1}$.

Proof complexity differs only elementarily. In fact:

Corollary

PA *exponentially simulates* CA. *This is optimal, unless there is a more efficient way to check cyclic proof soundness.*

Question

What is the logical strength of McNaughton's theorem, in general?

Question

What about computational interpretations and constructivity?

Optimal logical complexity result. In fact:

Corollary

$C\Sigma_n$ is precisley the Π_{n+1} consequences of $I\Sigma_{n+1}$.

Proof complexity differs only elementarily. In fact:

Corollary

PA *exponentially simulates* CA. *This is optimal, unless there is a more efficient way to check cyclic proof soundness.*

Question

What is the logical strength of McNaughton's theorem, in general?

Question

What about computational interpretations and constructivity?

Thank you.