Reflection principles
in weak and strong arithmetics

Emil Jeřábek

jerabek@math.cas.cz

http://math.cas.cz/~jerabek/

Institute of Mathematics of the Czech Academy of Sciences, Prague

Logic Colloquium
Prague, August 2019

Strong fragments of arithmetic

$EA =$ basic theory of Kalmár elementary functions
$\sim I\Delta_0 + EXP$

$I\Sigma_i = EA +$ induction schema

$$\varphi(0) \wedge \forall x \left(\varphi(x) \to \varphi(x+1)\right) \to \forall x\, \varphi(x) \qquad (\varphi\text{-}IND)$$

for $\varphi \in \Sigma_i$: $\qquad \exists x_1 \, \forall x_2 \, \ldots \, Qx_i \, \underbrace{\theta(x_1, \ldots, x_i, \ldots)}_{\text{bounded quantifiers}}$

Strict hierarchy: $EA \subsetneq I\Sigma_1 \subsetneq I\Sigma_2 \subsetneq \cdots \subsetneq PA$

non-conservative even for universal sentences

General reference: [Bek05]

Weak fragments of arithmetic

$PV_1 =$ basic theory of polynomial-time functions

$T_2^i = PV_1 + \Sigma_i^b\text{-}IND$

$S_2^i = PV_1 +$ polynomial induction schema

$$\varphi(0) \wedge \forall x \left(\varphi(\lfloor x/2 \rfloor) \to \varphi(x) \right) \to \forall x \, \varphi(x) \qquad (\varphi\text{-}PIND)$$

for $\varphi \in \Sigma_i^b$: $\exists x_1 \le t_1 \, \forall x_2 \le t_2 \, \ldots \, Qx_i \le t_i \, \underbrace{\theta(x_1, \ldots, x_i, \ldots)}$

$\qquad\qquad\qquad\qquad\qquad\qquad\qquad$ sharply bounded quantifiers
$\qquad\qquad\qquad\qquad\qquad\qquad\qquad\quad \exists u \le |t|, \, \forall u \le |t|$

Hierarchy? $PV_1 \subseteq S_2^1 \subseteq T_2^1 \subseteq S_2^2 \subseteq \cdots \subseteq T_2 = I\Delta_0 + \Omega_1$

$S_2^i \subseteq T_2^i$: conjectured non-conservative for universal sentences

$T_2^i \subseteq S_2^{i+1}$: $\forall \Sigma_{i+1}^b$-conservative, still conjectured strict

General reference: [Kra95], [CN10], [J18]

Gödel for the win

What makes the difference?

> **Strong fragments**
>
> $I\Sigma_{i+1} \vdash \mathrm{Con}(I\Sigma_i)$

> **Weak fragments**
>
> ► $T_2^{i+1} \nvdash \mathrm{Con}(T_2^i)$, in fact:
> ► [PW87] $EA \nvdash \mathrm{Con}(Q)$!
> ► [Pud90] $T_2 \nvdash \mathrm{BdCon}(PV_1)$

Can bounded arithmetic prove the consistency of anything?

Propositional proof systems

pps = sound and complete proof system for **CPC** with
poly-time recognizable proofs [CR74]

- ▶ Frege: textbook system with finitely many
  axiom schemata and rules
  p-equivalent: sequent calculus, natural deduction
- ▶ Extended Frege (*EF*): may introduce shorthand variables
  p-equivalent: substitution Frege, circuit Frege
- ▶ Quantified propositional sequent calculus G:
  introduction rules for propositional quantifiers
    - ▶ G_i: only Σ_i^q cut formulas

    $$\exists \vec{x_1} \, \forall \vec{x_2} \, \ldots \, Q\vec{x_i} \, \underbrace{\theta(\vec{x_1}, \ldots, \vec{x_i}, \ldots)}_{\text{quantifier-free}}$$

    - ▶ G^*, G_i^*: proofs tree-like

Propositional consistency statements

- ▶ [Cook75] PV_1 proves $\mathrm{Con}(EF)$
- ▶ [KP90] T_2^i (and S_2^{i+1}) proves $\mathrm{Con}(G_i)$ and $\mathrm{Con}(G_{i+1}^*)$

NB: $G_i \geq_p G_{i+1}^*$, $G_i \equiv_p^{\Pi_{i+1}^q} G_{i+1}^*$

Consistency statements = universal sentences (not just Π_1)

Tight correspondence [KP90]

- ▶ $PV_1 + \mathrm{Con}(G_i) \equiv \mathsf{Th}_\forall(T_2^i)$
- ▶ $T_2^i \vdash \mathrm{Con}(P) \implies G_i$ p-simulates P (more or less)
- ▶ translation of T_2^i to G_i: see next slide

$\mathrm{Con}(G_i)$ = strongest consistency statement provable in T_2^i

Similarly for S_2^i and G_i^* (NB: $\mathsf{Th}_\forall(S_2^i) = \mathsf{Th}_\forall(T_2^{i-1})$)

Propositional translation

[Cook75], [KP90]

- ▶ true universal sentence $\forall x\, \theta(x)$
  $\mapsto$ sequence of propositional tautologies $[\![\theta]\!]_n$, $n \in \mathbb{N}$
- ▶ true $\forall \Sigma_i^b$ sentence $\forall x\, \theta(x)$
  $\mapsto$ sequence of Σ_i^q tautologies $[\![\theta]\!]_n$
  - ▶ if $a_{n-1} \ldots a_1 a_0$ binary representation of $a \in \mathbb{N}$:

    $$\mathbb{N} \vDash \theta(a) \iff [\![\theta]\!]_n(a_0, \ldots, a_{n-1}) \text{ is true}$$

- ▶ $T_2^i \vdash \forall x\, \theta(x) \implies [\![\theta]\!]_n$ have poly-size G_i-proofs
- ▶ $S_2^i \vdash \forall x\, \theta(x) \implies [\![\theta]\!]_n$ have poly-size G_i^*-proofs

$\mathrm{Con}(T)$ **vs.** $\mathrm{Con}(P)$

$\mathrm{Con}(T)$ same outside as inside:

- $T \stackrel{?}{\vdash} \mathrm{Con}(T)$ can be diagonalized ($\implies$ Gödel's theorem)

  - no obvious way to diagonalize $T \stackrel{?}{\vdash} \mathrm{Con}(P)$

- $\mathrm{Con}(T)$ can be iterated $\implies$ transfinite hierarchy
  - $\mathrm{Con}(P)$ cannot be directly iterated
  - $\mathrm{Th}_\forall(T_2^i)$ finitely axiomatizable while $\mathrm{Th}_\forall(I\Sigma_i)$ reflexive

Possible twist: use $[\![\mathrm{Con}(P)]\!]_n$ inside P?

- usually P has poly-size proofs of $[\![\mathrm{Con}(P)]\!]_n$!
  $\implies$ no point in iterating it

- diagonalization prevented by a fixed length-bound

Reflection principles

Relativize consistency statements:

▶ "X + all true Π_i formulas" consistent
   $\iff$ all Σ_i consequences of X are true

First-order reflection principles

▶ Local: $\mathrm{Rfn}_\Gamma(T) = \left\{ \Box_T \varphi \to \varphi : \varphi \in \Gamma \right\}$, $\Gamma = \Sigma_i, \Pi_i$
▶ Uniform: $\mathrm{RFN}_{\Sigma_i}(T) = \forall \phi \in \Sigma_i \left(\Box_T \phi \to \mathrm{Tr}_{\Sigma_i}(\phi) \right)$
   $= \left\{ \forall x \left(\Box_T \varphi(\dot{x}) \to \varphi(x) \right) : \varphi \in \Sigma_i \right\}$

Propositional reflection principles

▶ $\mathrm{RFN}_i(P) = \forall \phi \in \Sigma_i^q \left(\Box_P(\phi) \to \forall e \left(e \vDash_{\Sigma_i^q} \phi \right) \right)$
▶ analogue of local reflection?

Characterizing theories by RFN

Strong fragments [Lei83]

- $I\Sigma_i \equiv EA + \mathrm{RFN}_{\Sigma_{i+1}}(EA)$

Weak fragments [KP90]

- $S_2^i \equiv PV_1 + \mathrm{RFN}_{i+1}(cfG^*) \equiv PV_1 + \mathrm{RFN}_{i+1}(G_i^*)$
- $j \leq i$: $\mathrm{Th}_{\forall\Sigma_j^b}(S_2^i) \equiv PV_1 + \mathrm{RFN}_j(G_i^*)$
- $j < i$: $\equiv PV_1 + \mathrm{RFN}_j(G_{i-1})$
- $T_2^{i-1} \equiv \mathrm{Th}_{\forall\Sigma_i^b}(S_2^i) \equiv PV_1 + \mathrm{RFN}_i(G_i^*)$

NB: propositional translation $\implies$ G_i^* and G_{i-1} have poly-size proofs of $[\![\mathrm{RFN}_{i+1}(G_i^*)]\!]_n$ and $[\![\mathrm{RFN}_{i-1}(G_{i-1})]\!]_n$

Finite axiomatizability

Consequences of characterization by RFN:

Strong fragments

- ▶ $I\Sigma_i$ itself is finitely axiomatizable
- ▶ $j \le i \implies \mathsf{Th}_{\Pi_{j+1}}(I\Sigma_i)$ is reflexive

Weak fragments

- ▶ S_2^i, T_2^i are finitely axiomatizable
- ▶ $\mathsf{Th}_{\forall\Sigma_j^b}(S_2^i)$, $\mathsf{Th}_{\forall\Sigma_j^b}(T_2^i)$ finitely axiomatizable for all j

Induction rules

Induction in the form of deduction rules

▶ $\Gamma\text{-}IND^R$: $\dfrac{\varphi(0) \quad \forall x \left(\varphi(x) \to \varphi(x+1)\right)}{\forall x\, \varphi(x)}$

▶ $\Gamma\text{-}PIND^R$: $\dfrac{\varphi(0) \quad \forall x \left(\varphi(\lfloor x/2 \rfloor) \to \varphi(x)\right)}{\forall x\, \varphi(x)}$

$T + R =$ closure of theory T under rule R

$[T, R] =$ closure of T under unnested applications of R

$[T, R]_0 = T$, $[T, R]_{n+1} = [[T, R]_n, R]$: $T + R = \bigcup_n [T, R]_n$

$R \equiv R'$ if $[T, R] = [T, R']$ for every T

Reflection rules

Strong fragments [Bek97]

▶ $\Sigma_i\text{-}IND^R \equiv \dfrac{\varphi}{\mathrm{RFN}_{\Sigma_i}(EA + \varphi)}$, $\varphi \in \Pi_{i+1}$ over $I\Sigma_{i-1}$

▶ $\Pi_i\text{-}IND^R \equiv \dfrac{\varphi}{\mathrm{RFN}_{\Sigma_{i-1}}(EA + \varphi)}$, $\varphi \in \Pi_{i+1}$

Weak fragments [J18]

▶ $\Sigma_i^b\text{-}(P)IND^R \equiv \dfrac{\varphi}{\mathrm{RFN}_i(G_i^{(*)} + \varphi)}$, $\varphi \in \forall \Sigma_i^b$

▶ $\Pi_i^b\text{-}(P)IND^R \equiv \dfrac{\varphi}{\mathrm{RFN}_{i-1}(G_i^{(*)} + \varphi)}$, $\varphi \in \forall \Sigma_i^b$

$G_i + \forall x\, \theta(x) = G_i$ with axioms $[\![\theta]\!]_n(\vec{A})$, $\vec{A}$ quantifier-free

Parameter-free induction

Consider the induction axiom

$$\varphi(0) \wedge \forall x \left(\varphi(x) \rightarrow \varphi(x+1) \right) \rightarrow \forall x \, \varphi(x)$$

▶ standard induction schemata:
  φ may have arbitrary free variables (parameters)

▶ parameter-free induction: only x is free in φ

Notation: $I\Gamma^-$, Γ-IND^-, Γ-$PIND^-$

For $\Gamma = \Sigma_i, \Pi_i, \Sigma_i^b, \Pi_i^b$:

▶ Γ-induction rules equivalent to parameter-free versions

▶ Γ-$(P)IND^-$ = least theory whose all extensions are closed under Γ-$(P)IND^R$

Parameter-free reflection

Strong fragments [Bek99]

- $I\Sigma_i^- \equiv EA + \left\{ \varphi \to \mathrm{RFN}_{\Sigma_i}(EA + \varphi) : \varphi \in \Pi_{i+1} \right\}$
- $I\Pi_i^- \equiv EA + \left\{ \varphi \to \mathrm{RFN}_{\Sigma_{i-1}}(EA + \varphi) : \varphi \in \Pi_{i+1} \right\}$

Weak fragments [J18]

- $\Sigma_i^b\text{-}IND^- \equiv PV_1 + \left\{ \varphi \to \mathrm{RFN}_i(G_i + \varphi) : \varphi \in \forall\Sigma_i^b \right\}$
- $\Pi_i^b\text{-}IND^- \equiv PV_1 + \left\{ \varphi \to \mathrm{RFN}_{i-1}(G_i + \varphi) : \varphi \in \forall\Sigma_i^b \right\}$
- the same for $PIND^-$ and G_i^*

Relativized local reflection

Interpret RFN_{Σ_n} as a consistency operator:

- $\diamondsuit_T \varphi = \mathrm{RFN}_{\Sigma_n}(T + \varphi)$, $\boxdot_T \varphi = \neg \diamondsuit_T \neg \varphi$
- $\boxdot \approx$ provability operator for $T + \mathrm{Th}_{\Pi_n}(\mathbb{N})$
  Hilbert–Bernays–Löb provability conditions
- $\mathrm{Rfn}_\Gamma^n(T) = \left\{ \boxdot_T \varphi \to \varphi : \varphi \in \Gamma \right\}$

Restate the previous slide:

Strong fragments [Bek99]

- $I\Sigma_i^- \equiv EA + \mathrm{Rfn}_{\Sigma_{i+1}}^i(EA)$
- $I\Pi_i^- \equiv EA + \mathrm{Rfn}_{\Sigma_{i+1}}^{i-1}(EA)$

Is there a meaningful way to do this for bounded arithmetic?

Finite axiomatizability

Strong fragments [Bek97,99]

For $T \subseteq \Pi_{i+1}$ finite, $\Gamma = \Sigma_i$ or Π_i:
- $[T, \Gamma\text{-}IND^R]_k \subsetneq [T, \Gamma\text{-}IND^R]_{k+1}$
- $T + \Gamma\text{-}IND^R$ reflexive; $I\Sigma_i^-$, $I\Pi_i^-$ reflexive

Weak fragments [J18]

For $T \subseteq \forall\Sigma_i^b$ finite, $\Gamma = \Sigma_i^b$ or Π_i^b:
- $T + \Gamma\text{-}(P)IND^R = [T, \Gamma\text{-}(P)IND^R]$ finitely axiom'ble

Problem

Are $\Sigma_i^b\text{-}(P)IND^-$, $\Pi_i^b\text{-}(P)IND^-$ finitely axiomatizable?

Thank you for attention!

References

- ▶ L. D. Beklemishev: Induction rules, reflection principles, and provably recursive functions, Ann. Pure Appl. Logic 85 (1997), 193–242
- ▶ _____ : Parameter-free induction and provably total computable functions, Theoret. Comput. Sci. 224 (1999), 13–33
- ▶ _____ : Reflection principles and provability algebras in formal arithmetic, Russian Math. Surveys 60 (2005), 197–268
- ▶ S. A. Cook: Feasibly constructive proofs and the propositional calculus, Proc. 7th STOC, 1975, 83–97
- ▶ _____ , P. Nguyen: Logical foundations of proof complexity, Cambridge University Press, 2010
- ▶ _____ , R. Reckhow: The relative efficiency of propositional proof systems, J. Symb. Log. 44 (1979), 36–50
- ▶ E. Jeřábek: Induction rules in bounded arithmetic, arXiv:1809.10718 [math.LO]
- ▶ J. Krajíček: Bounded arithmetic, propositional logic, and complexity theory, Cambridge University Press, 1995
- ▶ _____ , P. Pudlák: Quantified propositional calculi and fragments of bounded arithmetic, Z. math. Logik Grund. Math. 36 (1990), 29–46
- ▶ D. Leivant: The optimality of induction as an axiomatization of arithmetic, J. Symb. Log. 48 (1983), 182–184
- ▶ J. B. Paris, A. J. Wilkie: On the scheme of induction for bounded arithmetic formulas, Ann. Pure Appl. Logic 35 (1987), 261–302
- ▶ P. Pudlák: A note on bounded arithmetic, Fund. Math. 136 (1990), 86–89