A hierarchy of propositional proof systems

Pavel Pudlák

Mathematical Institute, Czech Academy of Sciences, Prague [1]

Mathematical Approaches to Lower Bounds: Complexity of Proofs and Computation, Edinburgh, 4 -8 July 2022

[1]supported by EPAC, grant 19-27871X of the Czech Grant Agency

Overview

1. The lattice of propositional proof systems
2. Proof systems of theories
3. Jump operators
4. Transfinite progressions
5. How to define the supremum of a countable sequence

The lattice of propositional proof systems

- $P_1 \leq_p P_2$ if P_2 polynomially simulates P_1
- $P_1 <_p P_2$ if $P_1 \leq_p P_2$ but not otherwise

The lattice of propositional proof systems

- $P_1 \leq_p P_2$ if P_2 polynomially simulates P_1
- $P_1 <_p P_2$ if $P_1 \leq_p P_2$ but not otherwise

Fact. $\leq_p$ is a lattice ordering.

The lattice of propositional proof systems

- $P_1 \leq_p P_2$ if P_2 polynomially simulates P_1
- $P_1 <_p P_2$ if $P_1 \leq_p P_2$ but not otherwise

Fact. $\leq_p$ is a lattice ordering.

Conjecture (1980's)

This lattice $\mathcal{L}$ does not have the top element.

Proof systems of theories

Definition

Let T be a f.o. theory, polynomially axiomatized. The strong proof system of T, Q_T is defined by

1. translate propositions by replacing propositional variables p_i with $x_i = 0$;
2. interpret f.o. proofs of such formulas as proofs of the propositions.

Proof systems of theories

Definition

Let T be a f.o. theory, polynomially axiomatized. The strong proof system of T, Q_T is defined by

1. translate propositions by replacing propositional variables p_i with $x_i = 0$;
2. interpret f.o. proofs of such formulas as proofs of the propositions.

Fact. Strong proof systems of theories are cofinal in $\mathcal{L}$.

Proof systems of theories

Definition

Let T be a f.o. theory, polynomially axiomatized. The strong proof system of T, Q_T is defined by

1. translate propositions by replacing propositional variables p_i with $x_i = 0$;
2. interpret f.o. proofs of such formulas as proofs of the propositions.

Fact. Strong proof systems of theories are cofinal in $\mathcal{L}$.

Definition

The weak proof system P_T of a theory T is the strongest proof system whose soundness is provable in T. It exists only for some theories.

Jump operators

1. **Adding consistency:**

$$Q_T \quad \mapsto \quad Q_{T+Con(T)}$$

Conjecture (J. Mycielski and P.P., 1984)

Adding consistency is a jump operator, i.e.,

$$Q_T <_p Q_{T+Con(T)}$$

Jump operators

1. **Adding consistency:**

$$Q_T \quad \mapsto \quad Q_{T+Con(T)}$$

Conjecture (J. Mycielski and P.P., 1984)

Adding consistency is a jump operator, i.e.,

$$Q_T <_p Q_{T+Con(T)}$$

Proposition (Krajíček)

Let T be a theory for which P_T is defined. Then $P_{T+Con(T)}$ is defined too and

$$P_{T+Con(T)} \equiv_p Q_T.$$

2. Implicit proof system

Definition (J. Krajíček, 2004)

The implicit proof system of P, denoted by iP, proof is a pair (C, D) where C is a circuit defining a (possibly exponential size) proof in P and D is a P-proof of the correctness of C.

2. Implicit proof system

Definition (J. Krajíček, 2004)

The implicit proof system of P, denoted by iP, proof is a pair (C, D) where C is a circuit defining a (possibly exponential size) proof in P and D is a P-proof of the correctness of C.

Conjecture

Implicitation is a jump operator, i.e.,

$$P <_P iP$$

Transfinite progressions

1. Transfinite iterations of consistency.

For a theory T and an ordinal α, define T_{α}^{Con} by

- $T_0^{Con} := T$,
- $T_{\alpha+1}^{Con} := T_{\alpha}^{Con} + Con(T_{\alpha}^{Con})$;
- for limit λ, $T_{\lambda}^{Con} := \bigcup_{\alpha<\lambda} T_{\alpha}^{Con}$.

Transfinite progressions

1. Transfinite iterations of consistency.

For a theory T and an ordinal α, define T_α^{Con} by

- $T_0^{Con} := T$,
- $T_{\alpha+1}^{Con} := T_\alpha^{Con} + Con(T_\alpha^{Con})$;
- for limit λ, $T_\lambda^{Con} := \bigcup_{\alpha<\lambda} T_\alpha^{Con}$.

2. Transfinite iterations of implicitation.

For a proof system P and an ordinal α, define $i_\alpha P$ by

- $i_0 P := P$,
- $i_{\alpha+1} P := i(i_\alpha P)$;
- for limit λ, $i_\lambda P := \sup_{\alpha<\lambda} i_\alpha P$.

How to define the supremum of a countable sequence of proof systems

How to define the supremum of a countable sequence of proof systems

Definition

$P = \sup_i \{P_i\}$ iff

1. there exists a polynomial time algorithm A such that

$$P_i = P(A(\bar{i}, d));$$

2. there exist a polynomial time algorithms B^{ind}, B^{pr} such that

$$P(d) = P_{B^{ind}(d)}(B^{pr}(d)).$$

How to define the supremum of a countable sequence of proof systems

Definition

$P = \sup_i \{P_i\}$ iff

1. there exists a polynomial time algorithm A such that
$$P_i = P(A(\bar{i}, d));$$
2. there exist a polynomial time algorithms B^{ind}, B^{pr} such that
$$P(d) = P_{B^{ind}(d)}(B^{pr}(d)).$$

Definition (simple version)

$\{P_i\}$ p-simulates $\{Q_i\}$ iff

- there exists a polynomial time algorithm A such that
$$Q_i(d) = P_i(A(C(\bar{i}, d))).$$

Proposition

If

- $\{P_i\}$ *p-simulates* $\{Q_i\}$ *and*
- $\sup_i\{P_i\}$ *and* $\sup_i\{Q_i\}$ *exist,*

then

- $\sup_i\{P_i\}$ *p-simulates* $\sup_i\{Q_i\}$.

Proposition

If

- $\{P_i\}$ *p-simulates* $\{Q_i\}$ *and*
- $\sup_i\{P_i\}$ *and* $\sup_i\{Q_i\}$ *exist,*

then

- $\sup_i\{P_i\}$ *p-simulates* $\sup_i\{Q_i\}$.

Proof.

Let $P := \sup_i\{P_i\}$ and $Q := \sup_i\{Q_i\}$.

$$Q(d) = Q_{B_Q^{ind}(d)}(B_Q^{pr}(d)) =$$

$$P_{B_Q^{ind}}(C(B_Q^{ind}(d), B_Q^{pr}(d))) =$$

$$P(A_P(B_Q^{ind}(d), C(B_Q^{ind}(d), B_Q^{pr}(d)))).$$

□

My goal

1. define a transfinite progression of proof system based on the implicitation jump up to ϵ_0
2. show that ω implicitation jumps equal one consistency jump
3. characterize strong (and weak) proof systems of fragments of PA

My goal

1. define a transfinite progression of proof system based on the implicitation jump up to ϵ_0
2. show that ω implicitation jumps equal one consistency jump
3. characterize strong (and weak) proof systems of fragments of PA

thank you