On implicit proof systems

Pavel Pudlák

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

Proof Complexity and Metamathematics, Berkeley, 20-24 March 2023

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

Definition (J. Krajíček, 2004)

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

Definition (J. Krajíček, 2004)

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

How robust is this definition?

Question 1. If P p-simulated Q, does iP simulate iQ?

For a Boolean circuit C with n inputs and 1 output, define $S(C)$ the bit-string

$$S(C) := (C(00\ldots00), C(00\ldots01), \ldots, C(11\ldots11)).$$

Question 2. Let $f \in FP$. Does there exist an $F \in FP$ such that for every circuit C,

$$S(F(C)) = f(S(C)) \ ?$$

[2] *Added after lecture: Olivier Korten pointed out that the completeness of SuccintCircuitValue in EXP implies a negative answer unconditionally.*

For a Boolean circuit C with n inputs and 1 output, define $S(C)$ the bit-string

$$S(C) := (C(00\dots00), C(00\dots01), \dots, C(11\dots11)).$$

Question 2. Let $f \in FP$. Does there exist an $F \in FP$ such that for every circuit C,

$$S(F(C)) = f(S(C)) \text{ ?}$$

Example. Let f be defined by

- $f(0\dots00) := 0\dots00$,
- $f(w_1 \dots w_{n-1}w_n) := w_1 \dots w_{n-1}1$, if $w \neq 0\dots00$.

[2] *Added after lecture: Olivier Korten pointed out that the completeness of SuccintCircuitValue in EXP implies a negative answer unconditionally.*

For a Boolean circuit C with n inputs and 1 output, define $S(C)$ the bit-string

$$S(C) := (C(00\ldots00), C(00\ldots01), \ldots, C(11\ldots11)).$$

Question 2. Let $f \in FP$. Does there exist an $F \in FP$ such that for every circuit C,

$$S(F(C)) = f(S(C)) \text{ ?}$$

Example. Let f be defined by

- $f(0\ldots00) := 0\ldots00,$
- $f(w_1\ldots w_{n-1}w_n) := w_1\ldots w_{n-1}1$, if $w \neq 0\ldots00$.

f is definable by a *finite automaton*. Yet for this f, there exists $F \in FP$ iff $P = NP$.[2]

[2] *Added after lecture: Olivier Korten pointed out that the completeness of SuccintCircuitValue in EXP implies a negative answer unconditionally.*

Example. In the sequent calculus we may use the rule for $\vee$-introduction either in this form

$$\frac{\Gamma \longrightarrow \Delta, A, B}{\Gamma \longrightarrow \Delta, A \vee B}$$

or

$$\frac{\Gamma \longrightarrow \Delta, A}{\Gamma \longrightarrow \Delta, A \vee B}$$

Do we get equivalent Implicit Extended Frege proof systems?

Example. In the sequent calculus we may use the rule for $\vee$-introduction either in this form

$$\frac{\Gamma \longrightarrow \Delta, A, B}{\Gamma \longrightarrow \Delta, A \vee B}$$

or

$$\frac{\Gamma \longrightarrow \Delta, A}{\Gamma \longrightarrow \Delta, A \vee B}$$

Do we get equivalent Implicit Extended Frege proof systems?

Claim

For every two "natural" formalizations of Extended Frege System P and P', the implicit proof systems iP and iP' are polynomially equivalent.

Theorem (Krajíček, 2004)

- *V^1_2 proves the soundness of iEF.*
- *If V^1_2 proves the soundness of P, then iEF polynomially simulates P.*

Theorem (Krajíček, 2004)

- *V_2^1 proves the soundness of iEF.*
- *If V_2^1 proves the soundness of P, then iEF polynomially simulates P.*

Since Krajíček's theorem can be proved for all "natural" formalizations of EF, all the implicit versions of them polynomially simulate each other.

Theorem (Krajíček, 2004)

- *V_2^1 proves the soundness of iEF.*
- *If V_2^1 proves the soundness of P, then iEF polynomially simulates P.*

Since Krajíček's theorem can be proved for all "natural" formalizations of *EF*, all the implicit versions of them polynomially simulate each other.

Question 3. What are *natural formalizations*?

Theorem (Krajíček, 2004)

- *V_2^1 proves the soundness of iEF.*
- *If V_2^1 proves the soundness of P, then iEF polynomially simulates P.*

Since Krajíček's theorem can be proved for all "natural" formalizations of EF, all the implicit versions of them polynomially simulate each other.

Question 3. What are *natural formalizations*?

Fact

Let P, Q be proof systems. Assume that P is closed under substitutions and Q-proofs of the Q-reflection principles can be constructed in polynomial time. Then

- *P p-simulates Q iff P-proofs of the Q-reflection principles can be constructed in polynomial time.*

Question 4. Starting with a natural formalization of *EF*, do we get all *iiEF* equivalent?

Definition

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

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

We assume that the f.o. proofs are formalized in some Frege system.

Definition

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

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

We assume that the f.o. proofs are formalized in some Frege system.

Theorem

The strong proof system of Robinsons's arithmetic Q *polynomially simulates iEF.*

Lemma

The strong proof system of Robinsons's arithmetic Q is polynomially equivalent to the strong proof system of S_2^1.

Proof.

There is an interpretation of S_2^1 in Q using a formula that defines an initial segment of natural numbers. □

Lemma

The strong proof system of Robinsons's arithmetic Q *is polynomially equivalent to the strong proof system of* S_2^1.

Proof.

There is an interpretation of S_2^1 in Q using a formula that defines an initial segment of natural numbers. □

Lemma

If T *contains Robinson's arithmetic, then the strong proof system of* T *can be defined by defining a proof of a tautology* ϕ *to be a f.o. proof in* T *of* $Taut(\lceil\phi\rceil)$.

Proof.

There are P-time constructible Q proofs of

$$\phi(x_1 = 0, \ldots, x_n = 0) \equiv Taut(\lceil\phi\rceil)$$

Here $\lceil\phi\rceil$ denotes the binary numeral representing the Gödel number of ϕ. □

Lemma

S_2^1 proves the soundness of iEF for proofs of logarithmic size. Formally

$$S_2^1 \vdash \forall x, y, z(x \leq |y| \wedge Prf_{EF}(x, z) \rightarrow Taut(z)).$$

Proof.

If $x \leq |y| \wedge Prf_{EF}(y, z)$, one can expand the implicitly defined proof y to an explicit EF-proof of z. □

Lemma

S^1_2 proves the soundness of iEF for proofs of logarithmic size. Formally

$$S^1_2 \vdash \ \forall x, y, z(x \leq |y| \wedge Prf_{EF}(x, z) \rightarrow Taut(z)).$$

Proof.

If $x \leq |y| \wedge Prf_{EF}(y, z)$, one can expand the implicitly defined proof y to an explicit EF-proof of z. $\square$

Lemma

For every $n \in \mathbb{N}$, an S^1_2 proof of $\exists x(\bar{n} \leq |x|)$ can be constructed in polynomial time.

Here the numeral $\bar{n}$ is a term of the form

$$a_0 + 2(a_1 + 2(a_3 + 2(\dots a_k) \dots)),$$

where $a_i \in \{0, 1, \}$.

Lemma

There exists a formula $\alpha(x)$ such that S_2^1 proves

- $\alpha(0)$,
- $\forall x(\alpha(x) \to \alpha(x+1) \wedge \alpha(2x))$,
- $\forall x(\alpha(x) \to \exists y(x \leq |y|))$.

Lemma

There exists a formula $\alpha(x)$ such that S^1_2 proves

- $\alpha(0)$,
- $\forall x(\alpha(x) \to \alpha(x+1) \wedge \alpha(2x))$,
- $\forall x(\alpha(x) \to \exists y(x \leq |y|))$.

Hence given an *iEF* proof with the Gödel number n, we can construct in polynomial time a proof in S^1_2 that $\bar{n}$ is of logarithmic size. Then we can use the soundness of logarithmic size proofs *iEF* proofs in S^1_2.

Thank You