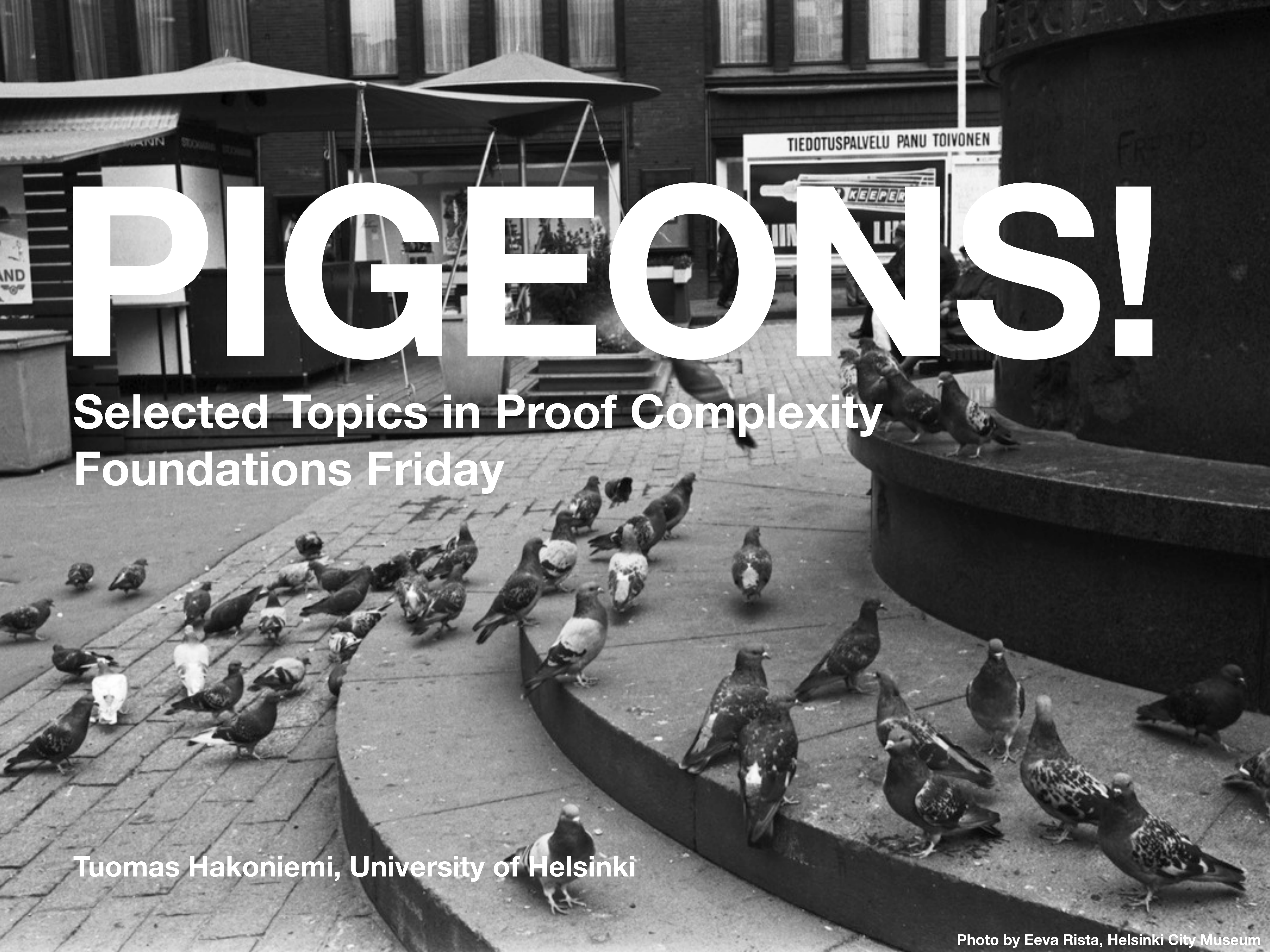


PIGEONS!

Selected Topics in Proof Complexity
Foundations Friday

Tuomas Hakoniemi, University of Helsinki

Photo by Eeva Rista, Helsinki City Museum

Beginnings

The Complexity of Theorem-Proving Procedures

Stephen A. Cook

University of Toronto

In view of the apparent complexity of {DNF tautologies}, it is interesting to examine the Davis-Putnam procedure [5]. This procedure was designed to determine whether a given formula in conjunctive normal form is satisfiable, but of course the "dual" procedure determines whether a given formula in disjunctive normal form is a tautology. I have not yet been able to find a series of examples showing the procedure (treated sympathetically to avoid certain pitfalls) must require more than polynomial time. Nor have I found an interesting upper bound for the time required.

The field of mechanical theorem proving badly needs a basis for comparing and evaluating the dozens of procedures which appear in the literature. Performance of a procedure on examples by computer is a good criterion, but not sufficient (unless the procedure proves useful in some practical way). A theoretical complexity criterion is needed which will bring out fundamental limitations and suggest new goals to pursue.

Propositional Proof Systems

Definition [Cook, Reckhow '79]

A propositional proof system is a poly-time predicate $R(x, y)$, whose domain equals TAUT (or UNSAT).

Soundness: if $R(\varphi, \pi)$, then $\varphi \in \mathsf{TAUT}$;

Completeness: if $\varphi \in \mathsf{TAUT}$, then there is some **proof** π so that $R(\varphi, \pi)$;

Feasibility: whether π is a proof of φ can be checked in polynomial time in the **length of the proof** (and the formula).

Propositional Proof Systems

Comparing systems

Definition [Cook, Reckhow '79]

A propositional proof system P p-simulates another propositional proof system Q, if there is a polynomial-time function that

- given as an input a Q-proof π of a formula φ
- outputs a P-proof of the same formula φ.

Propositional Proof Systems

The Foundational Observation

Proposition [Cook, Reckhow '79]

There is a polynomially bounded propositional proof system

if and only if

NP = coNP

A pps is polynomially bounded if there is some polynomial p so that for any φ there is some proof π so that

$$|\pi| \leq p(|\varphi|)$$

Resolution proof system

[Davis, Putnam '60]

Resolution refutation of $\{C_1, \ldots, C_m\}$ is a sequence of **clauses**

$$D_1, \ldots, D_\ell$$

where D_ℓ is the empty clause and each D_i is either an initial clause or obtained from previous ones by the **resolution rule**

$$A \vee x, B \vee \bar{x} \quad \Big/ \quad A \vee B$$

Frege systems

Common name for any sound and complete calculus consisting of a finite number of schematic inference rules, e.g. the axioms

$$\varphi \to (\psi \to \varphi)$$
$$(\varphi \to (\psi \to \xi)) \to ((\varphi \to \psi) \to (\varphi \to \xi))$$
$$(\neg\varphi \to \neg\psi) \to (\psi \to \varphi)$$

together with Modus Ponens as the only rule of inference

$$\varphi, \varphi \to \psi \quad / \quad \psi$$

Lemma [Cook, Reckhow '79]

All Frege systems are polynomially equivalent.

Frege systems

Sub- and supersystems

Extended Frege system allows introduction of short-hands by

$$z_\varphi \leftrightarrow \varphi$$

for a fresh propositional variable z_φ.

Size of Extended Frege proof $\sim$ number of lines in a Frege proof.

Bounded-depth Frege system restrict the formulas used in the proof to be of bounded **logical depth.**

Long proofs of simple principles.

Pigeonhole Principle

PHP_n^m encodes the fact that m pigeons cannot fly into n holes without a collision when $m > n$.

In clausal form:

$$\bigvee_{j \in [n]} x_{ij} \text{ for all } i \in [m]$$

$$\neg x_{ij} \vee \neg x_{ik} \text{ for all } i \in [m] \text{ and for all distinct } j, k \in [n]$$

Resolution Lower Bounds

Theorem [Haken '85]

PHP_n^{n+1} requires resolution refutations of size

$$2^{\Omega(n)}$$

Preceded by Tseitin's lower bound for **regular resolution** for the so called Tseitin formulas [Tseitin '68].

Exponential separation between regular and general resolution [Alekhnovich, Johannsen, Pitassi, Urquhart '02].

Resolution Lower Bounds

Proof idea [Beame, Pitassi '96]

In a refutation $D_1, \ldots, D_\ell$ of PHP_n^{n+1} replace each negated literal $\bar{x}_{ij}$ by the conjunction $x_{1j} \vee x_{2j} \vee \ldots x_{(i-1)j} \vee x_{(i+1)j} \vee \ldots \vee x_{(n+1)j}$ to obtain a **positive pseudo-refutation** of PHP_n^{n+1}.

Find a variable x_{ij} that occurs in many **wide** clauses (by pigeonhole principle!) and reduce to a pseudo-refutation of PHP_{n-1}^{n}.

Continue until there are no wide clauses left with a narrow pseudo-refutation of PHP_k^{k+1} for some k.

Show that any pseudo-refutation of PHP_k^{k+1} must still contain relatively wide clause.

Size-Width Trade-Off

Short proofs are narrow

Theorem [Ben-Sasson, Wigderson '01]

If a k-CNF F has a resolution refutation of size s, then it has a refutation of width

$$O(\sqrt{n \log s} + k)$$

Corollary

Any resolution refutation of a k-CNF F requires size

$$\exp\left(\Omega\left(\frac{(w(F \vdash \perp) - k)^2}{n}\right)\right)$$

Proof lower bounds from computational hardness

Feasible Interpolation

Basic set-up

Given two disjoint NP-sets A and B, an **interpolant** is a function s.t.

$$f(x) = \begin{cases} 0, \text{ when } x \in A \\ 1, \text{ when } x \in B \end{cases}$$

As A and B are in NP there are CNFs $A_n(x, y)$ and $B_n(x, z)$ so that

$$A = \bigcup_{n \in \omega} \{x \in \{0,1\}^n : \exists y, A_n(x, y) = 1\}$$

$$B = \bigcup_{n \in \omega} \{x \in \{0,1\}^n : \exists z, B_n(x, z) = 1\}$$

Disjointness of A and B $\Leftrightarrow$ unsatisfiability of $A_n(x, y) \wedge B_n(x, z)$.

Feasible Interpolation

Definition [Krajíček '97]

A pps P admits **feasible interpolation** if there is a function f that given a P-refutation π of $A_n(x, y) \wedge B_n(x, z)$ outputs a Boolean circuit $f(\pi)$ so that

$$f(\pi)(x) = \begin{cases} 1, \text{ when } A_n(x, y) \in \text{UNSAT} \\ 0, \text{ when } B_n(x, z) \in \text{UNSAT} \end{cases}$$

and

size of $f(\pi)$ is polynomial in the size of π.

Feasible Interpolation

Simple conditional lower bounds

Proposition

Suppose NP $\not\subseteq$ P/poly. Then no propositional proof system admitting feasible interpolation is polynomially bounded.

Proof.

Let P be a polynomially bounded proof system admitting feasible interpolation, and let $U \in$ NP.

Now NP $=$ coNP, and thus $U^c \in$ NP. Furthermore, as P is polynomially bounded and admits feasible interpolation, there is an interpolant of U and U^c in P/poly. But this interpolant decides U exactly, and thus $U \in$ P/poly.

Monotone Feasible Interpolation

Leveraging lower bounds for restricted models

In case A is downwards closed or B is upwards closed (or both), there is always a **monotone** interpolant.

A pps P admits **monotone feasible interpolation** if in this setting a proof of disjointness of A and B can be turned into only polynomially larger monotone interpolating circuit.

Proposition [Krajíček '97]

Resolution admits monotone feasible interpolation.

Monotone Feasible Interpolation

Lower bounds for Resolution

Consider the CNFs

$\mathrm{Clique}_{n,k}(x, y)$: “y is a clique of size k on a graph x of size n”

$\mathrm{Color}_{n,\ell}(x, z)$: “z is an ℓ-coloring of graph x”.

Theorem [Krajíček ’97] (using [Razborov ’85; Alon, Boppana ’87])

For $k \sim \sqrt{n}$ any resolution refutation of $\mathrm{Clique}_{n,k} \wedge \mathrm{Color}_{n,k-1}$ requires size

$$\exp(n^{\Omega(1)})$$

Negative results

Feasible interpolation is a sign of weakness

Theorem [Krajíček, Pudlák '98]

Extended Frege does not admit feasible interpolation unless RSA is not secure against $\mathsf{P/poly}$ adversaries.

Theorem [Bonet, Pitassi, Raz '00]

Frege does not admit feasible interpolation unless Diffie-Hellman scheme is not secure against $\mathsf{P/poly}$ adversaries.

The Proof Search Problem

Automatability

Barriers for efficient proof search

Definition [Bonet, Pitassi, Raz '00]

A propositional proof system P is **automatable** if there is an algorithm that given as input a CNF F returns a P-refutation of F in time $\mathrm{poly}(|F| + s)$, where s is the size of the smallest P-refutation of F

Lemma [Bonet, Pitassi, Raz '00]

If a propositional proof system P is automatable, then it admits feasible interpolation.

Automatability of Resolution

Some positive results

Proposition [Beame, Pitassi '96]

Tree-like resolution is automatable in time $n^{O(\log s)}$.

Proof idea:

If s is the minimal size of a refutation, and if x is the final variable to be resolved, then either

$$s(F|_{x=0} \vdash \bot\ ) \leq s/2 \text{ or } s(F|_{x=1} \vdash \bot\ ) \leq s/2$$

By size-degree trade-off, general resolution is automatable in time

$$n^{O(\sqrt{n \log s}+k)}$$

Non-automatability of Resolution

Theorem [Atserias, Müller '19]

Resolution is not automatable unless P = NP.

Proof idea (with amendments by [Garlik '20]):

$\mathrm{Ref}_s(F)$: "there is a resolution refutation of F of size s"

If $F \in \mathsf{SAT}$, then $\mathrm{Ref}_{n^c}(F)$ has poly-sized resolution refutations.

If $F \in \mathsf{UNSAT}$, then $\mathrm{Ref}_{n^c}(F)$ requires size $\exp(|F|^{\Omega(1)})$

The Crown Jewel of Proof Complexity

Bounded Arithmetic

Uniform models for Proof Complexity

Weak theories of arithmetic with close connections to computational complexity theory.

Intuitively, theories of bounded arithmetic only allow somehow computationally feasible reasoning.

Relates to propositional proof complexity via **propositional translations.** Proofs in arithmetic are the uniform counterparts of the non-uniform proofs in propositional proof systems.

The Theory $I\Delta_0$
The uniform bounded-depth Frege

Introduced by Parikh in ’71.

Basic language of arithmetic $\{\ \leq\ , +\ , \cdot\ , \ 0\ , \ 1\}$

Bounded quantifiers: $\exists x \leq t, \varphi(x, \bar{y})$ and $\forall x \leq t, \psi(x, \bar{z})$

$I\Delta_0$ is Peano arithmetic with induction restricted to formulas with only bounded quantifiers:

$$\varphi(0) \to (\forall x, (\varphi(x) \to \varphi(x+1)) \to \forall x, \varphi(x))$$

Provably total functions are the functions in the linear time function hierarchy FLTH.

Paris-Wilkie translation

From $I\Delta_0$ to bounded-depth Frege

Consider $I\Delta_0(R)$, where you allow additional binary relation symbol R in the formulas.

Define a translation from $\Delta_0(R)$-formulas into propositional ones:

$$\langle s(\bar{x}) \leq t(\bar{x}) \rangle_{\bar{k}} = \begin{cases} \top\text{ , when } s(\bar{k}) \leq t(\bar{k}) \\ \bot \text{ otherwise} \end{cases}$$

$\langle R(s(\bar{x}), t(\bar{x})) \rangle_{\bar{k}} = r_{ij}$, where $i = s(\bar{k})$ and $j = t(\bar{k})$.

$$\langle \exists y \leq t(\bar{x}), \varphi(\bar{x}, y) \rangle_{\bar{k}} = \bigvee_{\ell \leq t(\bar{k})} \langle \varphi(\bar{x}, y) \rangle_{\bar{k},\ell}$$

Paris-Wilkie Translation

From provability to upper bounds

For any $\Delta_0(R)$-formula $\varphi(\bar{x})$ the translation $\langle \varphi(\bar{x}) \rangle_{\bar{k}}$ is a constant depth Boolean formula of length polynomial in the sum of $\bar{k}$.

Theorem [Paris, Wilkie '85]

Let $\varphi(\bar{x})$ be a $\Delta_0(R)$-formula, and suppose that

$$I\Delta_0(R) \vdash \forall \bar{x}, \varphi(\bar{x})$$

Then for any tuple $\bar{k}$ there is constant-depth Frege proof of $\langle \varphi(\bar{x}) \rangle_{\bar{k}}$ of size polynomial in the sum of $\bar{k}$.

Bounded-depth Frege and PHP_n^{n+1}

From unprovability to lower bounds

$$\begin{aligned}\mathrm{PHP}(R) := \neg(&\forall x \leq z+1\, \exists y \leq z, R(x,y)\\ &\wedge \forall x \leq z+1\, \forall y, y' \leq z, \neg R(x,y) \vee \neg R(x,y'))\end{aligned}$$

Theorem [Ajtai '88]

The theory $I\Delta_0(R)$ does not prove $\mathrm{PHP}(R)$,

and **therefore**

bounded-depth Frege refutations of PHP_n^{n+1} require super-polynomial size.

Ajtai's argument

Let M be a **non-standard model of true arithmetic** and let $n \in M$ be a non-standard natural number.

Consider the **cut** $I_n = \{m \in M : m \leq n^c \text{ for some standard } c\}$

By a **forcing** argument construct an expansion $\langle I_n, R \rangle$ with $R \subseteq [n+1] \times [n]$ so that:

$$\langle I_n, R \rangle \vDash I\Delta_0(R) \quad \text{and} \quad \langle I_n, R \rangle \nvDash \mathrm{PHP}(R)$$

Therefore: If PHP_k^{k+1} has poly-sized refutation, then by **overflow,** for some non-standard n exists poly-sized refutations of PHP_n^{n+1}.

This refutation can be encoded in I_n, but I_n encodes also a satisfying assignment to PHP_n^{n+1} encoded by R. Contradiction follows from the fact that $I\Delta_0(R)$ **proves the soundness** of bounded depth Frege.

Stronger lower bounds

In ’93 Pitassi, Beame and Impagliazzo; and concurrently Krajíček, Pudlák and Woods improved the lower for PHP_n^{n+1} to

$$2^{n^{exp(-O(d))}}$$

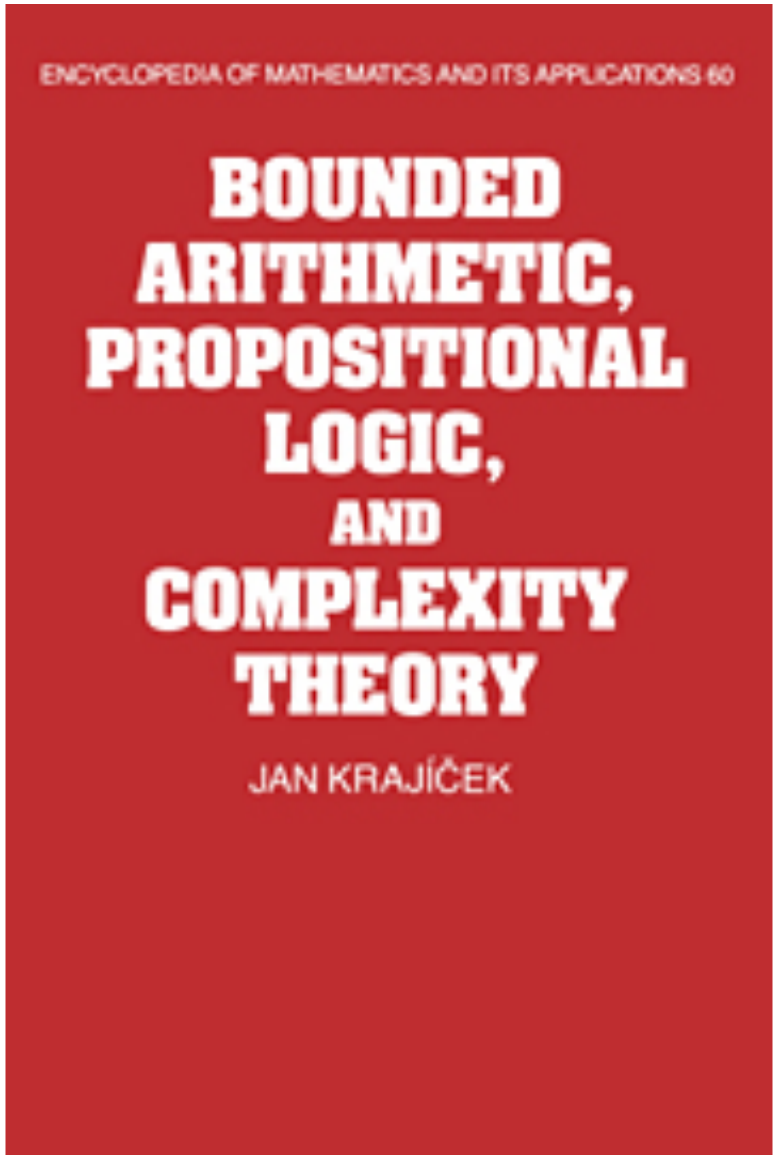
This year Håstad announced a lower bound of the form

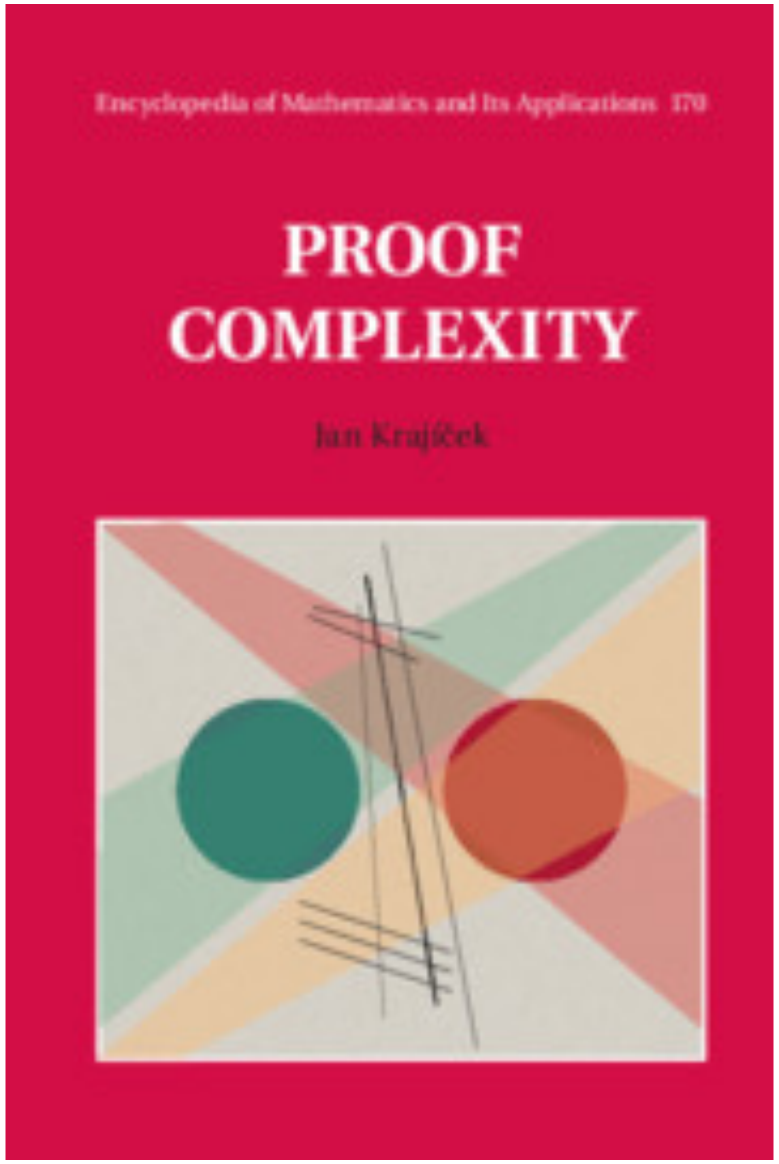
$$2^{n^{1/O(d)}}$$

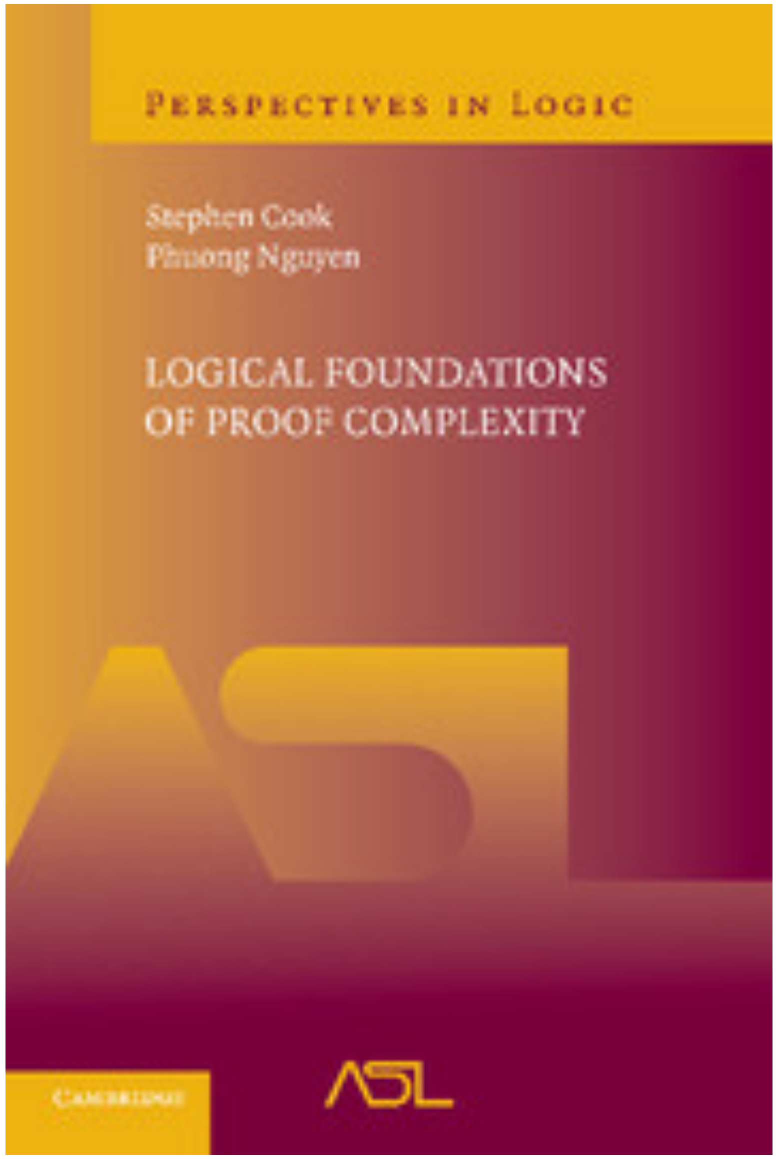
Hence, polynomial-sized Frege refutations of PHP_n^{n+1} require depth $\Omega(\log n/\log\log n)$.

In fact, there are polynomial-size Frege refutations of PHP_n^{n+1} of depth $O(\log n/\log\log n)$. [Buss ’86]

Some further reading







Thank you!