

Hard tautologies

Jan Krajíček

Charles University in Prague

A **propositional proof system** (pps) is a p-time function $f : \{0, 1\}^* \rightarrow \{0, 1\}^*$ such that

$$\text{Rng}(f) = \text{TAUT} .$$

Any x such that $f(x) = A$ is called an **f -proof of A** .

A pps f is **p-bounded** iff every tautology has a polynomially bounded f -proof, i.e.

$$\forall y \exists x (|x| \leq |y|^{O(1)}) f(x) = y .$$

Fact (Cook-Reckhow): There exists a p-bounded pps iff $\mathcal{NP} = \text{co}\mathcal{NP}$.

Problem (1):

Prove that $\mathcal{NP} \neq \text{co}\mathcal{NP}$ from a plausible computational hardness hypothesis.

A preferable form of the hypothesis:

- *Every circuit solving a specific task has to be large.*

Examples: $\mathcal{P} \neq \mathcal{NP}$, $\mathcal{P} = \mathcal{BPP}$, a strong PRNG exists

Problem (2):

*Prove that **Extended Frege system EF** is not p -bounded.*

EF can be formulated as a text-book style propositional calculus operating with circuits (Jeřábek).

EF is a canonical example of a
"strong proof system".

At present we do not know even a quadratic lower bound for EF.

Problem (3):

Does there exist an optimal pps?

optimal = has at most a polynomial slow-down over any other pps

A many-faceted question with links to quantitative aspects of Gödel's Theorem, to \mathcal{NP} -search problems, ...

It is possible that EF is optimal.

Our target problem:

Prove from a plausible computational hardness hypothesis that EF is not p -bounded.

A common weakening of problems (1) - (3).

Even to start we need:

- A framework in which to think about lower bounds for EF, and
- specific candidate hard tautologies.

A possible framework:

bounded arithmetic and its model theory.

Various bounded arithmetic theories formalize "feasible reasoning" analogously to how various classes of algorithms formalize "feasible computations".

The links between proof systems and bounded arithmetic theories form the main (maybe even "the only") knowledge about strong proof systems we have.

The upshot is:

The task of proving lower bounds for a pps P can be reduced to the task of constructing specific models of a bounded arithmetic theory T_P attached to P .

To prove a lower bound for P -proofs of

$$\varphi_n, \text{ as } n \rightarrow \infty$$

one needs to construct a model of T_P in which

φ_{n^*} can be falsified,

where n^* is "very very large".

Ex. (Ajtai):

A model where **PHP fails** for non-standard n^* ,
i.e. there is an injective map

$$F : [n^* + 1] \rightarrow [n^*] ,$$

but induction for AC^0 -properties of strings still holds.

This implied lower bounds for the **constant-depth Frege systems** F_d .

EF case requires:

Induction for \mathcal{NP} -properties of strings.

(PHP is provable there.)

A method under investigation: forcing with random variables

Candidate hard tautologies:

- **combinatorial principles** (e.g. PHP)
[works for weak proof systems only]
- **reflection formulas** $\|Ref_Q\|^n$: formalize soundness of "strong" Q w.r.t. proofs of lengths $\leq n$.
[difficult to use for lower bounds (but excellent for upper bounds)]
- complexity/logic motivated candidates
[feasible interpolation, **proof complexity generators**]

τ -formulas
alias
proof complexity generators

Motivations: feasible interpolation, pseudorandom number generators, proof complexity of forms of the PHP, model theory of bounded arithmetic.

Origins: 1999 in two papers

- Alekhnovich, Ben-Sasson, Razborov, Wigderson

- K.

Current state: about 10 papers and a theory is emerging

Definition:

A p-time map g :

$$g_n : \{0, 1\}^n \longrightarrow \{0, 1\}^m$$

with $n < m := m(n)$.

(W.l.o.g. assume that $n \rightarrow m(n)$ is injective.)

For any $b \in \{0, 1\}^m \setminus \text{Rng}(g)$ the τ -formula

$$\tau(g)_b$$

expresses:

$$"g_n(x_1, \dots, x_n) \neq b"$$

in the sense that

$$\tau(g)_b \in \text{TAUT} \quad \text{iff} \quad b \notin \text{Rng}(g) .$$

Technicalities:

- n variables x_i and $n^{O(1)} = m^{O(1)}$ auxiliary variables.
- $|\tau(g)_b| \leq m^{O(1)}$ which is for p-time map $\leq n^{O(1)}$.
- The τ -formulas can be defined and will have size $m^{O(1)}$ even if g is in **non-uniform**

$$NTime(m^{O(1)}) \cap coNTime(m^{O(1)}).$$

In particular, $\mathcal{NP} \cap co\mathcal{NP}$ is OK.

Hardness definition:

g is hard for P iff

- for every $c \geq 1$, no $\tau_b(g)$ has a P -proof of size $\leq m^c$, for $n \gg 0$.

Exponentially hard =

eventually all b need a size $2^{m^{\Omega(1)}}$ P -proof

Observation: The range $Rng(g)$ of a map g hard for all P would have to intersect all infinite \mathcal{NP} sets.

If g had this property for all \mathcal{NP} -sets of density $\geq 1/2$ we would still get $\mathcal{NP} \neq co\mathcal{NP}$ as a consequence.

Facts:

"Ordinary" PRNGs

- may be easy for EF:
e.g. a one-way permutation extended by the hard bit. [K. - Pudlák]
- but a bit-wise XOR of two independent copies (if $2n < m$) is hard for pps' with feasible interpolation. [ABRW]

Nisan-Wigderson generators: constructed under plausible assumption of the existence of hard boolean functions

A **problem** with using the original NW argument in proof complexity too:

- *The time complexity of g grows depending on the bound $m^{O(1)}$ to the size of P -proofs.*

Facts:

- Particular NW generators were shown to be exponentially hard for various algebraic pps' ([ABRW]), and
- a sparse NW-generator based on parity is exponentially hard for resolution ([K., Razborov]).

Notation:

- A : an $m \times n$ 0-1 matrix with ℓ ones per row
- $J_i(A) := \{j \leq n \mid A_{ij} = 1\}$, for $i \leq m$
- $f : \{0, 1\}^\ell \rightarrow \{0, 1\}$: a Boolean function.

The define $NW_{A,f} : \{0, 1\}^n \rightarrow \{0, 1\}^m$ by:

- the i -th bit of output is computed by f from the bits of the input that belong to $J_i(A)$.

Razborov's conjecture:

Any $NW_{A,f}$ based on A that is an (ℓ, d) combinatorial design with the original parameters of NW , and on any function f in $\mathcal{NP} \cap \text{co}\mathcal{NP}$ that is hard on average for \mathcal{P}/poly , is hard for EF .

Original parameters:

- $d = \log(m)$: intersection parameter,
- $\log(m) \leq \ell \leq m$, and
- $n = O(\ell^2)$.

Writing the inequalities dually:

$$(1) \quad m = 2^{\epsilon \cdot n^{1/2}} \quad \text{and} \quad \ell = \epsilon \cdot n^{1/2}$$

(taking the maximal value allowed for m).

$$(2) \quad H_f(\ell) \geq 2^{\Omega(\ell)} .$$

The conjecture requires that $f \in \mathcal{NP} \cap \text{co}\mathcal{NP}$.
We shall **relax** this condition to:

$$(3) \quad f \in \text{NTIME}(2^{O(\ell)}) \cap \text{coNTIME}(2^{O(\ell)}) .$$

This is maximal complexity of f for which the size of the τ -formula is still $m^{O(1)}$.

Statement (R):

Let A be an $m \times n$ matrix that is an $(\ell, \log(m))$ combinatorial design, and let f be any function such that the constraints in (1), (2) and (3) are satisfied. Then $NW_{A,f}$ is hard for EF .

Theorem([K.]):

Assume that Statement R is true. Then EF is not p -bounded.

Gadget generators:

Input string x of length $n = \ell + k \cdot t$ interpreted as

$$x = (v, u^1, \dots, u^t)$$

where

$$|v| = \ell, \quad |u^s| = k$$

for $s = 1, \dots, t$. Need $t > \ell$.

We call v the **gadget variables** and "interpret" them as defining a circuit C_v with k inputs and $k + 1$ outputs.

The **output string** y of length $m = (k + 1) \cdot t$ is defined as $y := (y^1, \dots, y^t)$ where

$$y^s := C_v(u^s)$$

for $s = 1, \dots, t$.

Example gadgets v :

- v is a graph of a map from $[k]$ in $[k + 1]$.

If v violates the onto-PHP then any u^s can be rearranged to length $k + 1$.

- v is a configuration of a clique in a graph and a coloring of the graph.

If the configuration violates the Clique/Coloring principle one can recover a violation of the WPHP.

Fact: One of the two is hard for any pps for which any lower bound is known.

Candidate gadget:

v is the data A and f defining a $NW_{A,f}$

The truth-table function:

$$tt_{s,k}$$

input: circuit C in k variables of size $s \leq 2^{k/2}$
encoded by $O(s \cdot \log(s)) < 2^k$ bits

output: the truth table $tt(C) \in \{0, 1\}^{2^k}$

Basic observation: $\tau(tt_{s,k})_b$ expresses that b is
a Boolean function with circuit complexity $> s$

Facts:

(1) For $s \geq k^{\omega(1)}$ map $tt_{s,k}$ is hard for any pps that admits feasible interpolation, assuming strong PRNG exists.

Via Razborov - Rudich's natural proofs.

(2) Assume there is a proof system P and $s(k) \geq 2^{\Omega(k)}$ such that $tt_{s,k}$ is **not hard** for P . Then $\text{BPP} \subseteq \mathcal{NP}$.

Via Impagliazzo - Wigderson derandomization.

(3) Assume there is a proof system P and $s(k) \geq k^{\omega(1)}$ such that $tt_{s,k}$ is **not hard** for P . Then $\text{EXP} \not\subseteq \mathcal{P}/\text{poly}$.

Via Impagliazzo - Kabanets - Wigderson derandomization of MA.

$$g(x) \neq b$$

may be hard but

$$g(x) \neq b \vee g(x') \neq b' \vee \dots$$

or

$$g(x) \neq b \vee g(x') \neq b'(x) \vee \dots$$

may be **easy**.

We say that g is **very hard** for P iff:

- "each such disjunction requires exponential size P -proof".

[iterability]

Theorem[K.]:

Assume that a pps P simulates resolution. Then there exists a very hard map for P iff there is $c \geq 1$ such that for $s = k^c$ the truth table function $tt_{s,k}$ is very hard for P .

Theorem[Razborov; K.]:

A very hard map exists for resolution.

A problem:

Let $MCSP$ be the set of pairs

$$(b, 1^{(s)}), \text{ with } b \in \{0, 1\}^{2^k}$$

such that $b \in \text{Rng}(tt_{s,k})$.

Is $MCSP$ \mathcal{NP} -complete?

Yablonski'59

Kabanets - Cai '99:

If $MCSP$ is \mathcal{NP} -complete under "natural" reduction from SAT then

$$E \not\subseteq \mathcal{P}/poly \text{ and } BPP \not\subseteq E .$$

Proof complexity consequences:

Assume that MCSP is \mathcal{NP} -complete provably in V_1^1 . Then:

(1) The τ -formulas from the truth-table function are the hardest tautologies over EF.

(2) Any pps can be simulated by EF augmented by circuit lower bounds for a function in E.

A natural question:

Does the hardness of $tt_{s,k}$ in
propositional logic

say anything relevant about the
mathematical hardness

of proving circuit lower bounds?

Perhaps a bit surprisingly: **YES!**

Logic has a classical way of calibrating how strong a method or axioms a proof of a theorem requires via a **hierarchy of theories**:

PRA primitive recursive arithmetic

⋮

PA Peano arithmetic = theory of finite sets

⋮ - several important subsystems of PA_2

PA_2 second order arithmetic

ZFC Zermelo-Fraenkel set theory

ZFC + large cardinals

The idea is that if your conjecture A cannot be proved in theory T while all theorems forming a method can, then the method will not prove A .

Examples:

- a lot of elementary number theory or combinatorics is in PA (even in PRA)
- a lot of "advanced" number theory is in PA
- most of mathematics is comfortably in PA_2 (even in its weak subsystems - cf. reverse mathematics)

Observation: Mathematical depth has nothing to do with how strong axioms are needed.

Theories for complexity theory: bounded arithmetic!

$S_2^2(\alpha)$: [Razborov]

corresponds to (a subsystem of) resolution R

V^0 : [Paris, Wilkie, Woods]

corresponds to constant depth Frege systems
 F_d

V_1^1 : a lot of complexity theory around \mathcal{P} , \mathcal{NP} ,
etc.

[Paris, Wilkie, Buss, K., Pudlák, Takeuti, Clote,
Cook, ...]

corresponds to EF

extensions of V_1^1 up to V^1 : probabilistic constructions, randomized models, ... [Jeřábek]

corresponds to **quantified propositional calculus G** (or "implicit EF")

Summary:

Hardness of $tt_{s,k}$ for EF or low fragments of G would mean that contemporary complexity does not imply circuit lower bounds

Connections to "natural proofs" of Razborov
- Rudich:

The provability of a superpoly circuit lower bounds for a class of circuits Γ in $S_2^2(\alpha)$ implies - via interpolation theory - the existence of a $\mathcal{P}/poly$ -natural property against Γ .

What about "natural proofs" for proof complexity?

Use the same approach.

Fact 1: Let $f : 1^{(n)} \rightarrow \varphi_n$ be a p -time construction of tautologies. If theory T_P proves that φ_n are tautologies then

P admits p -size proofs of φ_n .

Fact 2: If T_P proves a quadratic lower bound for a pps Q then

P must p -simulate Q .

- Hence you need at least EF to prove lower bounds for EF.

[1 and 2 are essent. due to Cook]

But in

Fact 3: *Theory T corresponding to P cannot prove super-poly lower bounds for P .*

[K. - Pudlák]

- Hence you need really more than EF to prove lower bounds for EF.

So if you contemplate to prove lower bounds for EF you may want to understand first **what of your approach cannot be formalized in V_1^1 .**

All known proof complexity arguments based on some form of finitary combinatorics (including random restrictions or algebraic methods) do comfortably formalize in V_1^1 .