Proof complexity, Dagstuhl
1st February 2018

Provability of weak circuit lower bounds

Ján Pich
Kurt Gödel Research Center
University of Vienna

based on a joint work with Moritz Müller

Constructive proofs of circuit lower bounds

Known circuit lower bounds for f given explicitly: AC^0, $\mathsf{AC}^0[p]$, etc.

very constructive: p-time algorithm often recognizing when f is hard

a.k.a natural proofs

Constructive proofs of circuit lower bounds

Known circuit lower bounds for f given explicitly: AC^0, $\mathrm{AC}^0[p]$, etc.
very constructive: p-time algorithm often recognizing when f is hard
a.k.a natural proofs

Razborov-Rudich: Cryptography works $\rightarrow$ no natural proof of P$\neq$NP.

Constructive proofs of circuit lower bounds

Known circuit lower bounds for f given explicitly: AC^0, $AC^0[p]$, etc.
very constructive: p-time algorithm often recognizing when f is hard
a.k.a natural proofs

Razborov-Rudich: Cryptography works $\rightarrow$ no natural proof of P$\neq$NP.

Mathematical logic:

∘ **upper bounds:** Prove all known circuit lower bounds in a constructive mathematical theory, e.g. PV_1 (p-time reasoning).
- exhibit a structure of algorithms recognizing hard functions?

Constructive proofs of circuit lower bounds

Known circuit lower bounds for f given explicitly: AC^0, $AC^0[p]$, etc.
very constructive: p-time algorithm often recognizing when f is hard
a.k.a natural proofs

Razborov-Rudich: Cryptography works $\rightarrow$ no natural proof of P$\neq$NP.

Mathematical logic:

◦ **upper bounds:** Prove all known circuit lower bounds in a constructive mathematical theory, e.g. PV_1 (p-time reasoning).
- exhibit a structure of algorithms recognizing hard functions?

◦ **lower bounds:** $PV_1 \nvdash$ strong circuit lower bounds?
- stronger 'natural proofs' barrier: P=NP consistent with PV_1?
- circuit lower bounds as hard tautologies witnessing NP$\neq$coNP?

Bounded arithmetic and propositional logic

$\mathbf{PV_1}$: first-order theory formalizing p-time reasoning (Cook '75)

$\mathbf{APC_1}$: formalizes probabilistic p-time reasoning (Jeřábek '07)

$\mathsf{APC}_1 := \mathsf{PV}_1 + $ "$\exists f \notin \mathsf{SIZE}(2^{\epsilon n})$"

Bounded arithmetic and propositional logic

$\mathbf{PV_1}$: first-order theory formalizing p-time reasoning (Cook '75)

$\mathbf{APC_1}$: formalizes probabilistic p-time reasoning (Jeřábek '07)

$\mathrm{APC}_1 := \mathrm{PV}_1 +$ "$\exists f \notin \mathrm{SIZE}(2^{\epsilon n})$"

If $\mathbf{PV_1} \vdash \forall x A(x)$ for a p-time predicate A, then tautologies expressing $\forall x A(x)$ have p-size Extended Frege **EF** proofs

If $\mathbf{APC_1} \vdash \forall x A(x)$ for a p-time predicate A, then tautologies expressing $\forall x A(x)$ have p-size **WF** proofs

WF: EF + "$\exists f \notin SIZE(2^{\epsilon n})$" (Jeřábek '04)

How to express circuit lower bounds formally

First-order formulation:

$LB(f, n^k)$: 'every circuit of size n^k fails to compute function f'

How to express circuit lower bounds formally

First-order formulation:

$LB(f, n^k)$: 'every circuit of size n^k fails to compute function f'

$$\forall n > n_0 \ \forall \text{ circuit } C \text{ of size } \leq n^k \ \exists \text{ input } y, \ |y| = n; \ C(y) \neq f(y)$$

where n_0, k are fixed constants

◦ If $f \in NP$, then $LB(f, n^k)$ is Π_3^p (i.e. $\forall\exists\forall$ statement)

How to express circuit lower bounds formally

First-order formulation:

$LB(f, n^k)$: 'every circuit of size n^k fails to compute function f'

$$\forall n > n_0 \; \forall \text{ circuit } C \text{ of size } \leq n^k \; \exists \text{ input } y, \; |y| = n; \; C(y) \neq f(y)$$

where n_0, k are fixed constants

◦ If $f \in NP$, then $LB(f, n^k)$ is Π_3^p (i.e. $\forall\exists\forall$ statement)

different scaling:

$LB_{tt}(f, n^k)$:

$\forall m, n > n_0, |m| = 2^n \; \forall$ circuit C of size $\leq n^k \; \exists \; y, \; |y| = n; \; C(y) \neq f(y)$

◦ If $f =$ SAT, then $LB_{tt}(f, n^k)$ is coNP

How to express circuit lower bounds formally

First-order formulation:

$LB(f, n^k)$: 'every circuit of size n^k fails to compute function f'

$$\forall n > n_0 \ \forall \text{ circuit } C \text{ of size } \leq n^k \ \exists \text{ input } y,\ |y| = n;\ C(y) \neq f(y)$$

where n_0, k are fixed constants

◦ If $f \in NP$, then $LB(f, n^k)$ is Π_3^p (i.e. $\forall\exists\forall$ statement)

different scaling:

$LB_{tt}(f, n^k)$:

$$\forall m, n > n_0, |m| = 2^n \ \forall \text{ circuit } C \text{ of size } \leq n^k \ \exists\, y,\ |y| = n;\ C(y) \neq f(y)$$

◦ If $f =$ SAT, then $LB_{tt}(f, n^k)$ is coNP

Easier to reason about $LB_{tt}(f, n^k)$ than about $LB(f, n^k)$.

Propositional formulation:

$tt(f, n^k)$: $$\bigvee_{y\in\{0,1\}^n} f(y) \neq C(y) \qquad \text{(expresses } LB_{tt}(f, n^k)\text{)}$$

2^n bits $f(y)$, $poly(n)$ variables for circuit C of size n^k, total size: $2^{O(n)}$

Propositional formulation:

$tt(f, n^k)$: $$\bigvee_{y \in \{0,1\}^n} f(y) \neq C(y)$$ (expresses $LB_{tt}(f, n^k)$)

2^n bits $f(y)$, $poly(n)$ variables for circuit C of size n^k, total size: $2^{O(n)}$

Lipton-Young: $f \notin SIZE(n^{O(1)}) \Rightarrow \exists A \subseteq \{0,1\}^n$ of size $poly(n)$ s.t.
$$\bigvee_{y \in A} f(y) \neq C(y)$$

Propositional formulation:

$tt(f, n^k)$: $$\bigvee_{y \in \{0,1\}^n} f(y) \neq C(y)$$ (expresses $LB_{tt}(f, n^k)$)

2^n bits $f(y)$, $poly(n)$ variables for circuit C of size n^k, total size: $2^{O(n)}$

Lipton-Young: $f \notin SIZE(n^{O(1)}) \Rightarrow \exists A \subseteq \{0,1\}^n$ of size $poly(n)$ s.t. $\bigvee_{y \in A} f(y) \neq C(y)$

$lb_A(f, n^k)$: $\bigvee_{y \in A} f(y) \neq C(y)$
- same meaning as $tt(f, n^k)$ but $poly(n)$ size

Propositional formulation:

$tt(f, n^k)$: $$\bigvee_{y \in \{0,1\}^n} f(y) \neq C(y)$$ (expresses $LB_{tt}(f, n^k)$)

2^n bits $f(y)$, $poly(n)$ variables for circuit C of size n^k, total size: $2^{O(n)}$

Lipton-Young: $f \notin SIZE(n^{O(1)}) \Rightarrow \exists A \subseteq \{0,1\}^n$ of size $poly(n)$ s.t.
$\bigvee_{y \in A} f(y) \neq C(y)$

$lb_A(f, n^k)$: $\bigvee_{y \in A} f(y) \neq C(y)$
- same meaning as $tt(f, n^k)$ but $poly(n)$ size

$lb_w(f, n^k)$: $poly(n)$ size formula expressing $LB(f, n^k)$
with existential quantifiers witnessed feasibly by w

Propositional formulation:

$tt(f, n^k)$: $\bigvee_{y \in \{0,1\}^n} f(y) \neq C(y)$ (expresses $LB_{tt}(f, n^k)$)

2^n bits $f(y)$, $poly(n)$ variables for circuit C of size n^k, total size: $2^{O(n)}$

Lipton-Young: $f \notin SIZE(n^{O(1)}) \Rightarrow \exists A \subseteq \{0,1\}^n$ of size $poly(n)$ s.t. $\bigvee_{y \in A} f(y) \neq C(y)$

$lb_A(f, n^k)$: $\bigvee_{y \in A} f(y) \neq C(y)$
- same meaning as $tt(f, n^k)$ but $poly(n)$ size

$lb_w(f, n^k)$: $poly(n)$ size formula expressing $LB(f, n^k)$
with existential quantifiers witnessed feasibly by w

Possible witnessing w of $LB(f, n^k)$: a p-time algorithm with **input**: circuit C of size n^k **output**: y s.t. $C(y) \neq f(y)$

Propositional formulation:

$tt(f, n^k)$: $$\bigvee_{y \in \{0,1\}^n} f(y) \neq C(y)$$ (expresses $LB_{tt}(f, n^k)$)

2^n bits $f(y)$, $poly(n)$ variables for circuit C of size n^k, total size: $2^{O(n)}$

Lipton-Young: $f \notin SIZE(n^{O(1)}) \Rightarrow \exists A \subseteq \{0,1\}^n$ of size $poly(n)$ s.t.
$$\bigvee_{y \in A} f(y) \neq C(y)$$

$lb_A(f, n^k)$: $\bigvee_{y \in A} f(y) \neq C(y)$
- same meaning as $tt(f, n^k)$ but $poly(n)$ size

$lb_w(f, n^k)$: $poly(n)$ size formula expressing $LB(f, n^k)$
with existential quantifiers witnessed feasibly by w
- $\exists w$ follows e.g. from $\mathrm{PV}_1 \vdash LB(f, n^k)$

Propositional formulation:

$tt(f, n^k)$: $$\bigvee_{y \in \{0,1\}^n} f(y) \neq C(y)$$ (expresses $LB_{tt}(f, n^k)$)

2^n bits $f(y)$, $poly(n)$ variables for circuit C of size n^k, total size: $2^{O(n)}$

> Lipton-Young: $f \notin SIZE(n^{O(1)}) \Rightarrow \exists A \subseteq \{0,1\}^n$ of size $poly(n)$ s.t.
> $$\bigvee_{y \in A} f(y) \neq C(y)$$

$lb_A(f, n^k)$: $\bigvee_{y \in A} f(y) \neq C(y)$
- same meaning as $tt(f, n^k)$ but $poly(n)$ size

$lb_w(f, n^k)$: $poly(n)$ size formula expressing $LB(f, n^k)$
with existential quantifiers witnessed feasibly by w
- $\exists w$ follows e.g. from $\mathrm{PV}_1 \vdash LB(f, n^k)$

> Fact: If $tt(f, n^k)$ has no poly-size constant-depth Frege proofs, then
> $lb_A(f, n^k)$ has no poly-size (full) Frege proofs.

Previous results

Lower bounds:

Razborov: $S^2_2(\alpha) \nvdash$ "$LB_{tt}(SAT, n^k)$" unless cryptography breaks

P.: $\mathrm{VNC}^1 \nvdash LB(SAT, n^k)$ unless $SIZE(n^k) \subseteq_{approx}$ "subexp NC^1"

Krajíček-Oliveira: $\forall k\ \exists f \in \mathrm{P}$ s.t. $\mathrm{PV}_1 \nvdash f \in SIZE(cn^k)$

Buss: $\mathrm{PV}_1 \nvdash \mathrm{NP} = co\mathrm{NP}$ unless P=NP

"folklore": $V^0 \nvdash SAT \in \mathrm{P/poly}$

Previous results

Lower bounds:

Razborov: $S^2_2(\alpha) \nvdash$ "$LB_{tt}(SAT, n^k)$" unless cryptography breaks

P.: $\mathrm{VNC}^1 \nvdash LB(SAT, n^k)$ unless $SIZE(n^k) \subseteq_{approx}$ "subexp NC^1"

Krajíček-Oliveira: $\forall k\ \exists f \in \mathrm{P}$ s.t. $\mathrm{PV}_1 \nvdash f \in SIZE(cn^k)$

Buss: $\mathrm{PV}_1 \nvdash \mathrm{NP} = co\mathrm{NP}$ unless P=NP

"folklore": $V^0 \nvdash SAT \in \mathrm{P/poly}$

Razborov-Krajíček: Propositional systems with feasible interpolation property have no p-size proofs of $tt(f, n^k)$ unless cryptography breaks.

Raz: Resolution has no p-size proofs of $tt(f, n^k)$ (unconditionally).

Razborov: $Res(\epsilon \log n)$ does not have p-size proofs of $tt(f, n^{\omega(1)})$.

Previous results

Lower bounds:

Razborov: $S^2_2(\alpha) \nvdash$ "$LB_{tt}(SAT, n^k)$" unless cryptography breaks

P.: $\mathrm{VNC}^1 \nvdash LB(SAT, n^k)$ unless $SIZE(n^k) \subseteq_{approx}$ "subexp NC^1"

Krajíček-Oliveira: $\forall k\ \exists f \in \mathrm{P}$ s.t. $\mathrm{PV}_1 \nvdash f \in SIZE(cn^k)$

Buss: $\mathrm{PV}_1 \nvdash \mathrm{NP} = co\mathrm{NP}$ unless P=NP

"folklore": $V^0 \nvdash SAT \in \mathrm{P/poly}$

Razborov-Krajíček: Propositional systems with feasible interpolation property have no p-size proofs of $tt(f, n^k)$ unless cryptography breaks.

Raz: Resolution has no p-size proofs of $tt(f, n^k)$ (unconditionally).

Razborov: $Res(\epsilon \log n)$ does not have p-size proofs of $tt(f, n^{\omega(1)})$.

$tt(f, n^k)$ considered as cadidate hard tautologies for EF.

Upper bounds:

Razborov: $\mathrm{PV}_1 \vdash LB_{tt}(PARITY, \mathrm{AC}^0(n^k))$

- $\mathrm{AC}^0(n^k)$: constant depth circuits of size n^k

$\mathrm{PV}_1 \vdash LB_{tt}(MOD_q, \mathrm{AC}^0[p](n^k))$ for p, q distinct primes

- $\mathrm{AC}^0[p](n^k)$: $\mathrm{AC}^0(n^k)$ with mod_p gates

$\mathrm{PV}_1 \vdash LB_{tt}(CLI, mSIZE(n^k))$

- $mSIZE(n^k)$: monotone circuits of size n^k

Upper bounds:

Razborov: $\mathrm{PV}_1 \vdash LB_{tt}(PARITY, \mathrm{AC}^0(n^k))$

- $\mathrm{AC}^0(n^k)$: constant depth circuits of size n^k

$\mathrm{PV}_1 \vdash LB_{tt}(MOD_q, \mathrm{AC}^0[p](n^k))$ for p, q distinct primes

- $\mathrm{AC}^0[p](n^k)$: $\mathrm{AC}^0(n^k)$ with mod_p gates

$\mathrm{PV}_1 \vdash LB_{tt}(CLI, mSIZE(n^k))$

- $mSIZE(n^k)$: monotone circuits of size n^k

Corollary: **p-size** EF **proofs** of the corresponding $tt(f, n^k)$ formulas

In fact: Razborov's formalization are below PV_1 resp. EF

Upper bounds:

Razborov: $\mathrm{PV}_1 \vdash LB_{tt}(PARITY, \mathrm{AC}^0(n^k))$

- $\mathrm{AC}^0(n^k)$: constant depth circuits of size n^k

$\mathrm{PV}_1 \vdash LB_{tt}(MOD_q, \mathrm{AC}^0[p](n^k))$ for p, q distinct primes

- $\mathrm{AC}^0[p](n^k)$: $\mathrm{AC}^0(n^k)$ with mod_p gates

$\mathrm{PV}_1 \vdash LB_{tt}(CLI, mSIZE(n^k))$

- $mSIZE(n^k)$: monotone circuits of size n^k

Corollary: **p-size** EF **proofs** of the corresponding $tt(f, n^k)$ formulas

In fact: Razborov's formalization are below PV_1 resp. EF

Krajíček: $\mathrm{APC}_1 \vdash LB(PARITY, \mathrm{AC}^0(n^k))$

Complexity theory formalizable in PV_1 and APC_1

Theory	Theorem
PV_1	Cook-Levin's theorem
	the PCP theorem
	Hardness amplification
	...
APC_1	AC^0 lower bounds
	$\mathsf{AC}^0[p]$ lower bounds (with $2^{\log^{O(1)} n} \in Log$)
	Monotone circuit lower bounds
	Nisan-Wigderson's derandomization
	Impagliazzo-Wigderson's derandomization
	Goldreich-Levin's theorem
	Natural proofs barrier
	...

Table: A list of formalizations.

New results

$\mathrm{APC}_1 \vdash LB(PARITY, \mathrm{AC}^0(n^k))$

$\mathrm{APC}_1 \vdash LB(MOD_q, \mathrm{AC}^0[p](n^k))$ for p, q distinct primes

$\mathrm{APC}_1 \vdash LB(CLI, mSIZE(n^k))$

New results

$\mathrm{APC}_1 \vdash LB(PARITY, \mathrm{AC}^0(n^k))$

- ∘ standard proof using Jeřábek's machinery of approximate counting
- ∘ $\Pr[A] > p$, for $A \subseteq 2^n$, witnessed by a p-time surjection $s : A \mapsto p2^n$
- ∘ size of each set approximated by sampling $poly(n)$ elements
  e.g. there are $poly(n)$ restrictions $\rho_1, \ldots, \rho_t, t \leq poly(n)$ s.t.
  each n^k-size d-depth circuit is collapsed by some $\rho \in \{\rho_1, \ldots, \rho_t\}$
  (ρ leaving many variables unassigned)

$\mathrm{APC}_1 \vdash LB(MOD_q, \mathrm{AC}^0[p](n^k))$ for p, q distinct primes

$\mathrm{APC}_1 \vdash LB(CLI, mSIZE(n^k))$

New results

$\mathrm{APC}_1 \vdash LB(PARITY, \mathrm{AC}^0(n^k))$

- ∘ standard proof using Jeřábek's machinery of approximate counting
- ∘ $\Pr[A] > p$, for $A \subseteq 2^n$, witnessed by a p-time surjection $s : A \mapsto p2^n$
- ∘ size of each set approximated by sampling $poly(n)$ elements
  e.g. there are $poly(n)$ restrictions $\rho_1, \dots, \rho_t, t \leq poly(n)$ s.t.
  each n^k-size d-depth circuit is collapsed by some $\rho \in \{\rho_1, \dots, \rho_t\}$
  (ρ leaving many variables unassigned)

$\mathrm{APC}_1 \vdash LB(MOD_q, \mathrm{AC}^0[p](n^k))$ for p, q distinct primes

- ∘ standard proof infeasible: counts all 2^{2^n} functions with n inputs
- ∘ we scale the argument: count only functions with $\log^{O(1)} n$ inputs
- ∘ $\exists m, |m| = 2^{\log^{O(1)} n}$ needed

$\mathrm{APC}_1 \vdash LB(CLI, mSIZE(n^k))$

New results

$\mathrm{APC}_1 \vdash LB(PARITY, \mathrm{AC}^0(n^k))$

- ∘ standard proof using Jeřábek's machinery of approximate counting
- ∘ $\Pr[A] > p$, for $A \subseteq 2^n$, witnessed by a p-time surjection $s : A \mapsto p2^n$
- ∘ size of each set approximated by sampling $poly(n)$ elements
  e.g. there are $poly(n)$ restrictions $\rho_1, \ldots, \rho_t, t \leq poly(n)$ s.t.
  each n^k-size d-depth circuit is collapsed by some $\rho \in \{\rho_1, \ldots, \rho_t\}$
  (ρ leaving many variables unassigned)

$\mathrm{APC}_1 \vdash LB(MOD_q, \mathrm{AC}^0[p](n^k))$ for p, q distinct primes

- ∘ standard proof infeasible: counts all 2^{2^n} functions with n inputs
- ∘ we scale the argument: count only functions with $\log^{O(1)} n$ inputs
- ∘ $\exists m, |m| = 2^{\log^{O(1)} n}$ needed

$\mathrm{APC}_1 \vdash LB(CLI, mSIZE(n^k))$

- ∘ standard proof with p-time surjections witnessing probabilities

New results

$\mathrm{APC}_1 \vdash LB(PARITY, \mathrm{AC}^0(n^k))$

$\mathrm{APC}_1 \vdash LB(MOD_q, \mathrm{AC}^0[p](n^k))$ for p, q distinct primes

$\mathrm{APC}_1 \vdash LB(CLI, mSIZE(n^k))$

Corollary: p-size EF proofs of the corresponding lb_w formulas from the assumption that "$\exists g, tt(g, 2^{\epsilon n})$".

New results

$\mathrm{APC}_1 \vdash LB(PARITY, \mathrm{AC}^0(n^k))$
$\mathrm{APC}_1 \vdash LB(MOD_q, \mathrm{AC}^0[p](n^k))$ for p, q distinct primes
$\mathrm{APC}_1 \vdash LB(CLI, mSIZE(n^k))$

Corollary: p-size EF proofs of the corresponding lb_w formulas from the assumption that "$\exists g, tt(g, 2^{\epsilon n})$".

Problem: $\mathrm{APC}_1 \vdash LB(f, n^k) \Rightarrow \exists$ efficient witnessing w of $LB(f, n^k)$
but w is probabilistic resp. w depends on a hard function g
so unconditional WF proofs of $lb_w(f, n^k)$ do not follow directly

New results

$\mathrm{APC}_1 \vdash LB(PARITY, \mathrm{AC}^0(n^k))$
$\mathrm{APC}_1 \vdash LB(MOD_q, \mathrm{AC}^0[p](n^k))$ for p, q distinct primes
$\mathrm{APC}_1 \vdash LB(CLI, mSIZE(n^k))$

Corollary: p-size EF proofs of the corresponding lb_w formulas from the assumption that "$\exists g, tt(g, 2^{\epsilon n})$".

Problem: $\mathrm{APC}_1 \vdash LB(f, n^k) \Rightarrow \exists$ efficient witnessing w of $LB(f, n^k)$ but w is probabilistic resp. w depends on a hard function g so unconditional WF proofs of $lb_w(f, n^k)$ do not follow directly

◦ Possible solution (the road not taken): **Derandomize** the probabilistic witnessing of AC^0, $\mathrm{AC}^0[p]$ and monotone circuit lower bounds in APC_1.

New results

$\mathrm{APC}_1 \vdash LB(PARITY, \mathrm{AC}^0(n^k))$
$\mathrm{APC}_1 \vdash LB(MOD_q, \mathrm{AC}^0[p](n^k))$ for p, q distinct primes
$\mathrm{APC}_1 \vdash LB(CLI, mSIZE(n^k))$

Corollary: p-size EF proofs of the corresponding lb_w formulas
from the assumption that "$\exists g, tt(g, 2^{\epsilon n})$".

Problem: $\mathrm{APC}_1 \vdash LB(f, n^k) \Rightarrow \exists$ efficient witnessing w of $LB(f, n^k)$
but w is probabilistic resp. w depends on a hard function g
so unconditional WF proofs of $lb_w(f, n^k)$ do not follow directly

◦ Possible solution (the road not taken): **Derandomize** the probabilistic witnessing of AC^0, $\mathrm{AC}^0[p]$ and monotone circuit lower bounds in APC_1.

To get WF proofs of $lb_A(f, \mathrm{AC}^0[p](n^k))$ formulas (unconditionally) we give a **succinct naturalization** of Razborov-Smolensky's $\mathrm{AC}^0[p]$ lower bound.

Naturalization / automatizability

- want a p-time algorithm which given $lb_A(f, n^k)$ finds its proof if it exists
- i.e. succinct natural proof

Naturalization / automatizability

- want a p-time algorithm which given $lb_A(f, n^k)$ finds its proof if it exists
- i.e. succinct natural proof

Learning: - given bits $f(x_1), \dots, f(x_k)$ for k n-bit tuples $x_1, \dots, x_k$
- want to predict $f(x_{k+1})$ on a new input $x_{k+1} \in \{0,1\}^n$

○ minimal circuit C computing f on $x_1, \dots, x_k$ has to determine $f(x_{k+1})$

○ say that the size of the minimal circuit C is s

Naturalization / automatizability

- want a p-time algorithm which given $lb_A(f, n^k)$ finds its proof if it exists
- i.e. succinct natural proof

Learning: - given bits $f(x_1), \dots, f(x_k)$ for k n-bit tuples $x_1, \dots, x_k$
- want to predict $f(x_{k+1})$ on a new input $x_{k+1} \in \{0,1\}^n$

○ minimal circuit C computing f on $x_1, \dots, x_k$ has to determine $f(x_{k+1})$

○ say that the size of the minimal circuit C is s

To predict $f(x_{k+1})$ prove an s-size circuit lower bound (for $\epsilon \in \{0,1\}$)

$$\bigvee_{i=1,\dots,k} C(x_i) \neq f(x_i) \vee C(x_{k+1}) \neq \epsilon$$

Naturalization / automatizability

- want a p-time algorithm which given $lb_A(f, n^k)$ finds its proof if it exists
- i.e. succinct natural proof

Learning: - given bits $f(x_1), \ldots, f(x_k)$ for k n-bit tuples $x_1, \ldots, x_k$
- want to predict $f(x_{k+1})$ on a new input $x_{k+1} \in \{0,1\}^n$

∘ minimal circuit C computing f on $x_1, \ldots, x_k$ has to determine $f(x_{k+1})$
∘ say that the size of the minimal circuit C is s

To predict $f(x_{k+1})$ prove an s-size circuit lower bound (for $\epsilon \in \{0,1\}$)

$$\bigvee_{i=1,\ldots,k} C(x_i) \neq f(x_i) \vee C(x_{k+1}) \neq \epsilon$$

A more sophisticated connection between circuit lower bounds and learning algorithms recently demonstrated by Carmosino et al.

Naturalization / automatizability

- want a p-time algorithm which given $lb_A(f, n^k)$ finds its proof if it exists
- i.e. succinct natural proof

Learning: - given bits $f(x_1), \ldots, f(x_k)$ for k n-bit tuples $x_1, \ldots, x_k$
- want to predict $f(x_{k+1})$ on a new input $x_{k+1} \in \{0,1\}^n$

◦ minimal circuit C computing f on $x_1, \ldots, x_k$ has to determine $f(x_{k+1})$
◦ say that the size of the minimal circuit C is s

To predict $f(x_{k+1})$ prove an s-size circuit lower bound (for $\epsilon \in \{0,1\}$)

$$\bigvee_{i=1,\ldots,k} C(x_i) \neq f(x_i) \vee C(x_{k+1}) \neq \epsilon$$

A more sophisticated connection between circuit lower bounds and learning algorithms recently demonstrated by Carmosino et al.

Theorem: quasipolynomial-time algorithm generating WF proofs of $lb_A(f, \mathrm{AC}^0[p](n^k))$ for many functions f.

Problems

- $\circ$ Derandomize known circuit lower bounds, i.e. prove them inside PV_1.

  1st step: Derandomize witnessing of known circuit lower bounds.

- $\circ$ Prove $\mathrm{APC}_1 \vdash LB(MOD_q, \mathrm{AC}^0[p](n^k))$ without $\exists m, |m| = 2^{\log^{O(1)} n}$.

- $\circ$ $V^0 \vdash LB(PARITY, \mathrm{AC}^0(n^k))$?

Problems

- Derandomize known circuit lower bounds, i.e. prove them inside PV_1.

  1st step: Derandomize witnessing of known circuit lower bounds.

- Prove $\mathsf{APC}_1 \vdash LB(MOD_q, \mathsf{AC}^0[p](n^k))$ without $\exists m, |m| = 2^{\log^{O(1)} n}$.

- $V^0 \vdash LB(PARITY, \mathsf{AC}^0(n^k))$?

Thank You for Your Attention