Efficient Adversaries

JÁN PICH

UNIVERSITY OF OXFORD

joint work with

Erfan Khaniki
Oxford

Dmitry Sokolov
Montreal

$\exists f \in$ **NTIME[2^n], $f \notin$ Circuit[9n]**?

$\exists f \in$ **NTIME[2^n],** $f \notin$ **Circuit[9n]?**

Razborov '95:	$S_2^2(\alpha) \nvdash f \notin$ Circuit[$n^{O(1)}$] (if ∃PRG)	(natural proofs)
Raz '01:	Res $\nvdash f \notin$ DNF[$n^{O(1)}$]	(pseudo-width)
Razborov '03:	Res(Ω(logn)) $\nvdash f \notin$ Circuit[$n^{O(1)}$]	(pc generators)

$\exists f \in$ **NTIME[2^n],** $f \notin$ **Circuit[9n]?**

Razborov '95: $S_2^2(\alpha) \nvdash f \notin \text{Circuit}[n^{O(1)}]$ (if ∃PRG) (natural proofs)
Raz '01: $\text{Res} \nvdash f \notin \text{DNF}[n^{O(1)}]$ (pseudo-width)
Razborov '03: $\text{Res}(\Omega(\log n)) \nvdash f \notin \text{Circuit}[n^{O(1)}]$ (pc generators)

Razborov's conjecture

P/poly hard for NC^1 $\Rightarrow$ Frege $\nvdash f \notin \text{Circuit}[n^{O(1)}]$
NP∩coNP hard for P/poly $\Rightarrow$ EF $\nvdash f \notin \text{Rng}(\text{NW}_h)$

Razborov's conjecture

P/poly hard for NC^1 $\Rightarrow$ Frege $\nvdash f \notin$ Circuit$[n^{O(1)}]$

NP∩coNP hard for P/poly $\Rightarrow$ EF $\nvdash f \notin \mathrm{Rng}(\mathrm{NW}_h)$

Krajicek's conjecture

PRG $\Rightarrow$ EF $\nvdash f \notin$ Circuit$[2^{\Omega(n)}]$

proof complexity

$\neg\exists$ p-bounded pps $\Leftrightarrow$ NP $\neq$ coNP

Frege

AC^0-Frege

Resolution

proof complexity

$\neg\exists$ p-bounded pps $\Leftrightarrow$ NP $\neq$ coNP

Frege
AC^0-Frege
Resolution

lifting $\Rightarrow$ monotone P/poly lbs
IPS lb $\Rightarrow$ VP$\neq$VNP
R lb $\Rightarrow$ P$\neq$NP T_R -consistent

EF lower bounds $\overset{?}{\Rightarrow}$ P $\neq$ NP

Why is Razborov-Krajicek conjecture hard?

(Natural proofs in proof complexity?)

Goal

constructive proof complexity lower bounds

new algorithms

adversary for $\mathrm{P} \overset{s}{\nvdash} \phi$

∀ s-size P-refutation π of $\neg\phi$ ∃ A,
A doesn't lose when traversing π
from $\bot$ to an axiom, following 0s

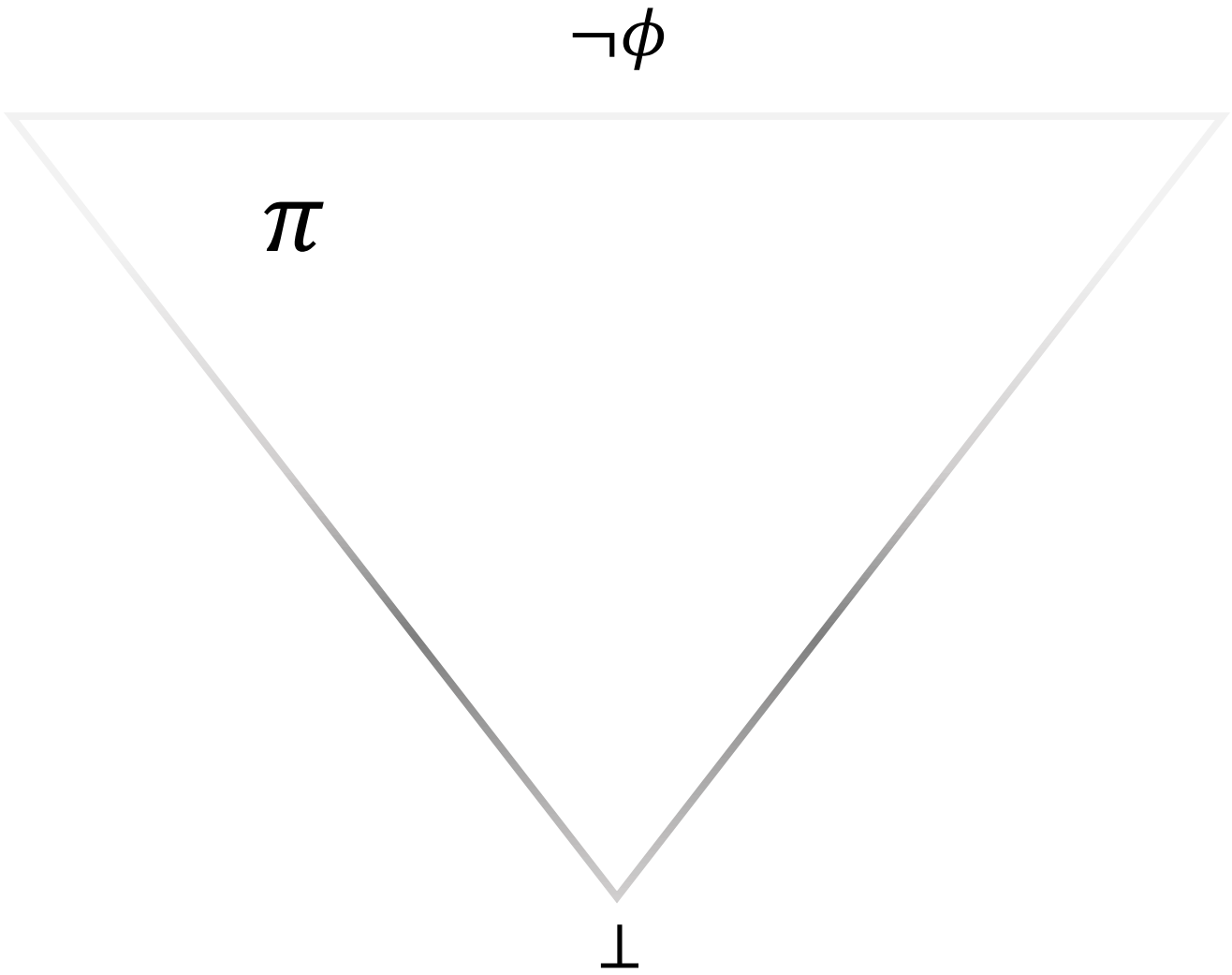
$$A(\neg\phi) = A(axiom) = 1$$

$$A(\bot) = 0$$

losing position

$$\frac{\begin{matrix}1 & 1\\ \psi_a & \psi_b\end{matrix}}{\psi_c}$$

0



adversary for $\mathrm{P} \overset{s}{\nvdash} \phi$

∀ s-size P-refutation π of $\neg\phi$ ∃ A,
A doesn't lose when traversing π
from $\perp$ to an axiom, following 0s

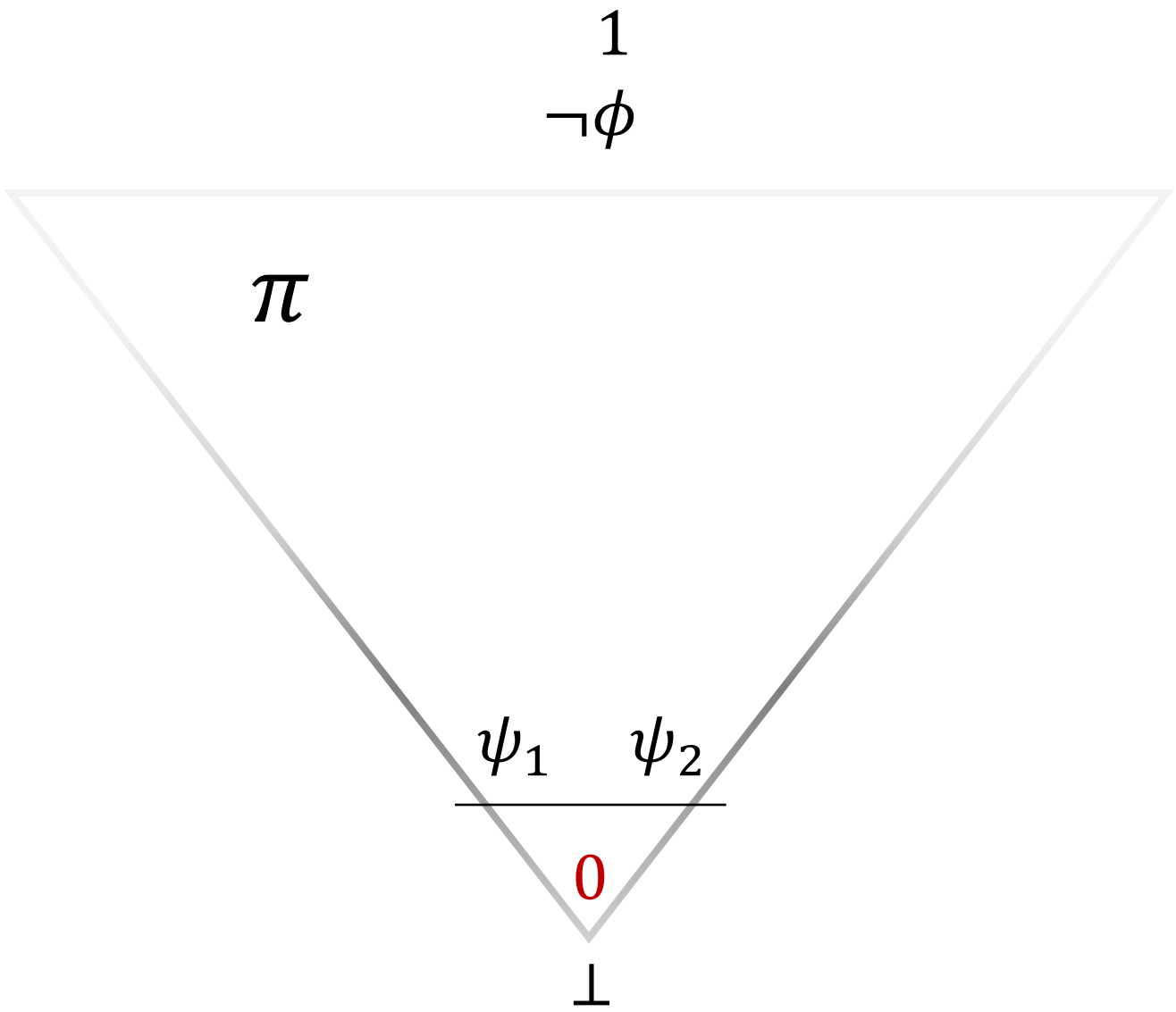
$$A(\neg\phi) = A(axiom) = 1$$

$$A(\perp) = 0$$

losing position

$$\frac{\begin{matrix}1 & 1\\ \psi_a & \psi_b\end{matrix}}{\psi_c}$$

0



adversary for $\mathrm{P} \overset{s}{\nvdash} \phi$

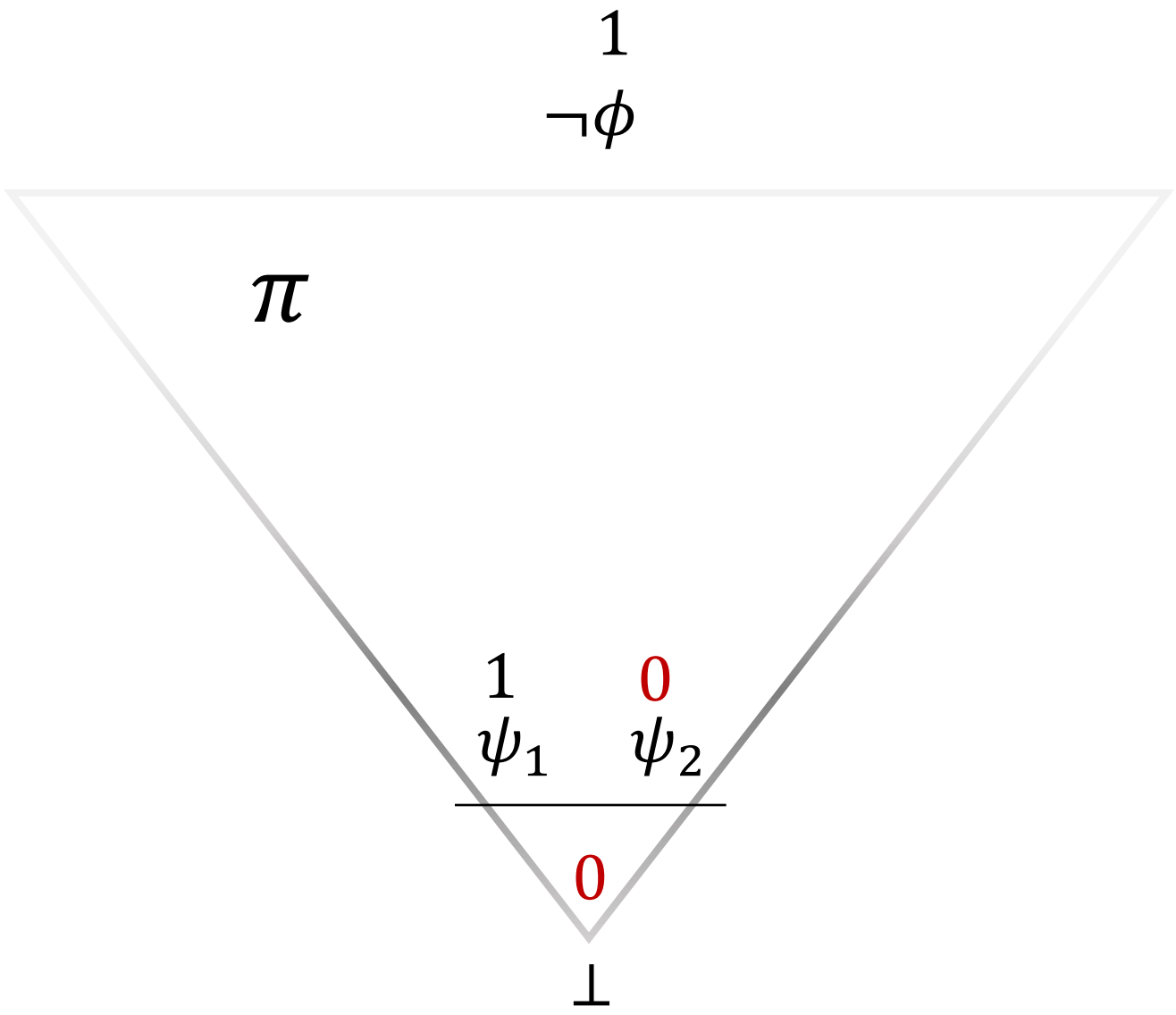
∀ s-size P-refutation π of $\neg\phi$ ∃ A,
A doesn't lose when traversing π
from $\perp$ to an axiom, following 0s

$$A(\neg\phi) = A(axiom) = 1$$

$$A(\perp) = 0$$

losing position

$$\frac{\begin{matrix}1 & 1\\ \psi_a & \psi_b\end{matrix}}{\begin{matrix}\psi_c\\ 0\end{matrix}}$$



adversary for $\mathrm{P} \overset{s}{\nvdash} \phi$

∀ s-size P-refutation π of $\neg\phi$ ∃ A,
A doesn't lose when traversing π
from $\perp$ to an axiom, following 0s

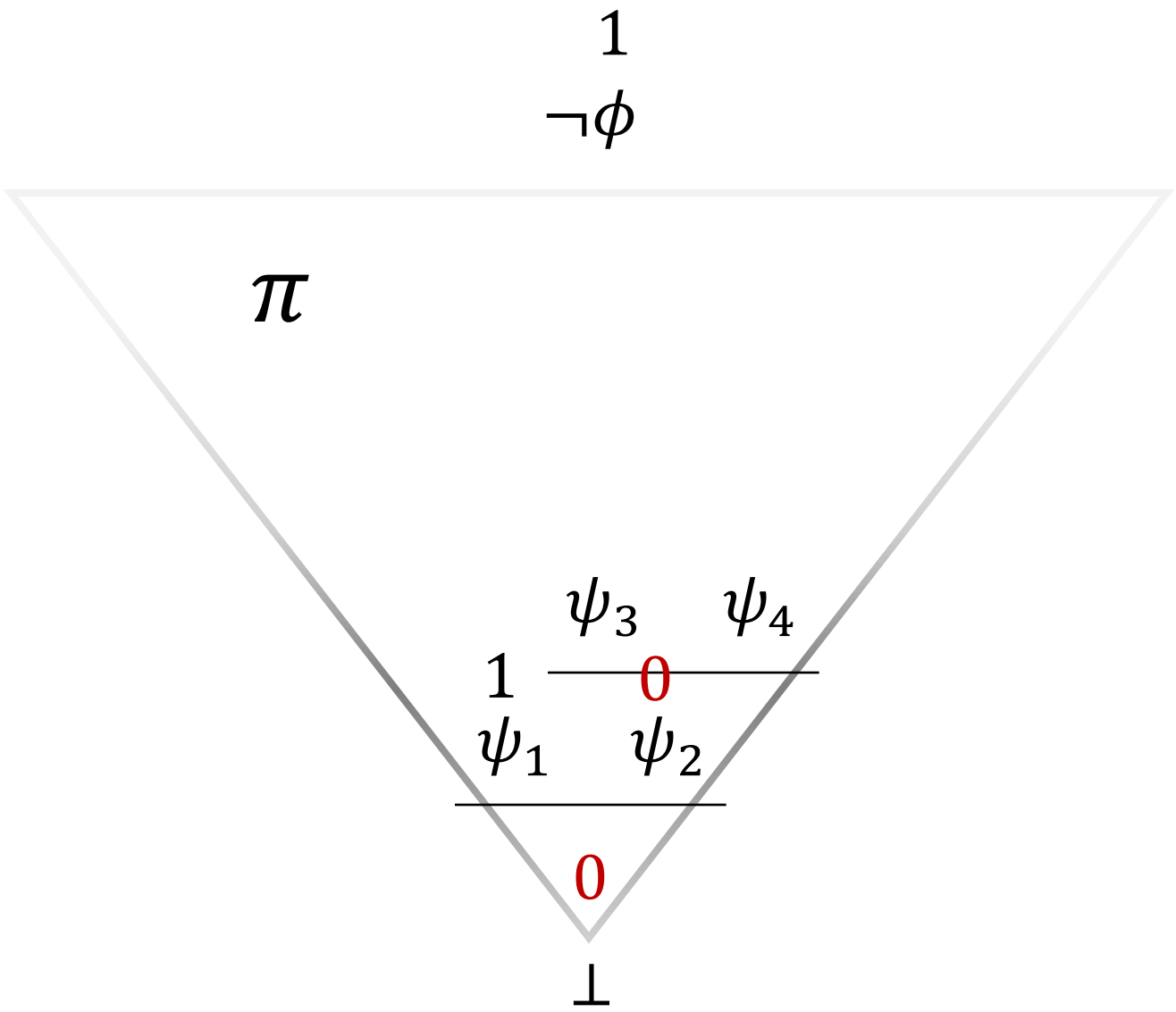
$$A(\neg\phi) = A(axiom) = 1$$

$$A(\perp) = 0$$

losing position

$$\frac{\begin{matrix}1 & 1\\ \psi_a & \psi_b\end{matrix}}{\psi_c}$$

0



adversary for $\mathrm{P} \overset{s}{\nvdash} \phi$

∀ s-size P-refutation π of $\neg\phi$ ∃ A,
A doesn't lose when traversing π
from $\perp$ to an axiom, following 0s

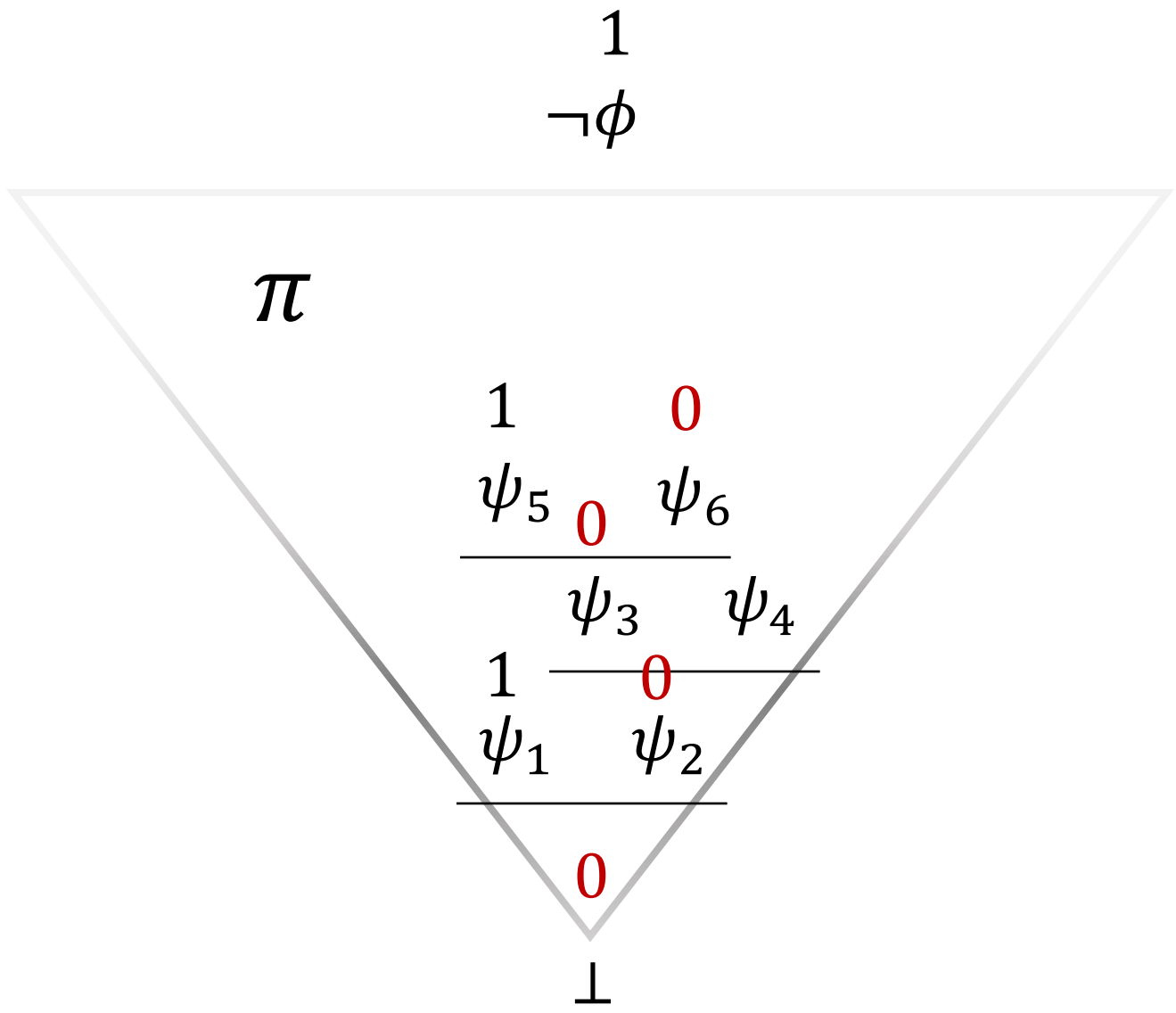
$$A(\neg\phi) = A(axiom) = 1$$

$$A(\perp) = 0$$

losing position

$$\frac{\begin{matrix}1 & 1\\ \psi_a & \psi_b\end{matrix}}{\psi_c}$$

0



efficient adversary for $\mathrm{P} \overset{s}{\nvdash} \phi$

∃ ef alg A s.t. ∀ s-size P-refutation π, A doesn't lose when traversing π from $\bot$ to an axiom, following 0s

$$A(\neg\phi) = A(axiom) = 1$$

$$A(\bot) = 0$$

losing position

$$\dfrac{\begin{matrix}1 & 1\\ \psi_a & \psi_b\end{matrix}}{\begin{matrix}\psi_c\\ 0\end{matrix}}$$

$$\begin{matrix}1 & 0\\ \neg\phi & \psi & \zeta\end{matrix}$$

π might not be a refutation of $\neg\phi$

$$\dfrac{\dfrac{\dfrac{\begin{matrix}1 & 0\\ \psi_5 & 0 & \psi_6\end{matrix}}{\begin{matrix}\psi_3 & \psi_4\\ 1 & 0\end{matrix}}}{\begin{matrix}\psi_1 & \psi_2\\ 0\end{matrix}}}{\bot}$$

Theorem 1 (From adversaries to algorithms – Informal, cf. Theorem 6)**.**
Assume 1 - 2:

1. (The canonical pair of EF is hard.) *For each $poly(n)$-size circuit D with n inputs, there is z such that $D(z) = 0$ but z is a satisfiable formula or $D(z) = 1$ but there is a $poly(n)$-size* EF*-refutation of z.*

Theorem 1 (From adversaries to algorithms – Informal, cf. Theorem 6)**.**
Assume 1 - 2:

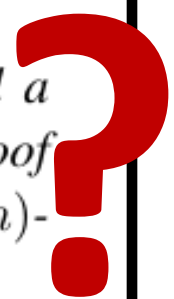
1. (The canonical pair of EF is hard.) *For each $poly(n)$-size circuit D with n inputs, there is z such that $D(z) = 0$ but z is a satisfiable formula or $D(z) = 1$ but there is a $poly(n)$-size* EF*-refutation of z.*

2. (Provably constructive anticheckers.) *There is $A \subseteq \{0,1\}^n$, $|A| = poly(n)$, and a $poly(n)$-size circuit F such that for each $z \in \{0,1\}^n$ there is a $poly(n)$-size* EF*-proof of the statement expressing that "if an n^2-size circuit B solves* SAT *on A, then a $poly(n)$-size circuit $F(B)$ solves* SAT *on z".*

Theorem 1 (From adversaries to algorithms – Informal, cf. Theorem 6)**.**
Assume 1 - 2:

1. (The canonical pair of EF is hard.) *For each $poly(n)$-size circuit D with n inputs, there is z such that $D(z) = 0$ but z is a satisfiable formula or $D(z) = 1$ but there is a $poly(n)$-size* EF*-refutation of z.*

2. (Provably constructive anticheckers.) *There is $A \subseteq \{0,1\}^n$, $|A| = poly(n)$, and a $poly(n)$-size circuit F such that for each $z \in \{0,1\}^n$ there is a $poly(n)$-size* EF*-proof of the statement expressing that "if an n^2-size circuit B solves* SAT *on A, then a $poly(n)$-size circuit $F(B)$ solves* SAT *on z".*

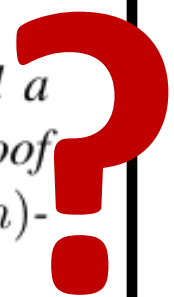


Theorem 1 (From adversaries to algorithms – Informal, cf. Theorem 6)**.**
Assume 1 - 2:

1. (The canonical pair of EF is hard.) *For each $poly(n)$-size circuit D with n inputs, there is z such that $D(z) = 0$ but z is a satisfiable formula or $D(z) = 1$ but there is a $poly(n)$-size* EF*-refutation of z.*

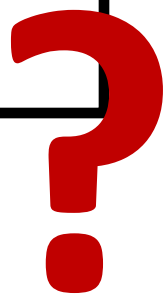
2. (Provably constructive anticheckers.) *There is $A \subseteq \{0,1\}^n$, $|A| = poly(n)$, and a $poly(n)$-size circuit F such that for each $z \in \{0,1\}^n$ there is a $poly(n)$-size* EF*-proof of the statement expressing that "if an n^2-size circuit B solves* SAT *on A, then a $poly(n)$-size circuit $F(B)$ solves* SAT *on z".*

Then for each randomized $poly(n)$-time EF*-adversary claiming that $\neg\mathsf{lb}_A(\mathsf{SAT}, n^2)$ is satisfiable, there is a $poly(n)$-size* EF*-refutation (not necessarily of $\neg\mathsf{lb}_A(\mathsf{SAT}, n^2)$) catching the adversary with probability $\geq 1/2 - 1/n$ over the randomness of the adversary.*



$\neg\mathsf{lb}_A(\mathsf{SAT}, n^2) :=$ *n^2-size circuit B solves* SAT *on* $A \subseteq \{0,1\}^n$

2. (Provably constructive anticheckers.) *There is* $A \subseteq \{0,1\}^n$, $|A| = poly(n)$, *and a* $poly(n)$*-size circuit* F *such that for each* $z \in \{0,1\}^n$ *there is a* $poly(n)$*-size* EF*-proof of the statement expressing that "if an* n^2*-size circuit* B *solves* SAT *on* A*, then a* $poly(n)$*-size circuit* $F(B)$ *solves* SAT *on* z*".*



- True if EF-provability not required
- True if EF $\vdash$ [E is hard & (OWF $\Leftarrow$ SAT $\notin$ P/poly)]
- Implies NP $\notin$ Size$[n^k]$

Theorem 1 (From adversaries to algorithms – Informal, cf. Theorem 6)**.**
Assume 1 - 2:

1. (The canonical pair of EF is hard.) *For each $poly(n)$-size circuit D with n inputs, there is z such that $D(z) = 0$ but z is a satisfiable formula or $D(z) = 1$ but there is a $poly(n)$-size* EF*-refutation of z.*

2. (Provably constructive anticheckers.) *There is $A \subseteq \{0,1\}^n$, $|A| = poly(n)$, and a $poly(n)$-size circuit F such that for each $z \in \{0,1\}^n$ there is a $poly(n)$-size* EF*-proof of the statement expressing that "if an n^2-size circuit B solves* SAT *on A, then a $poly(n)$-size circuit $F(B)$ solves* SAT *on z".*

Then for each randomized $poly(n)$-time EF*-adversary claiming that $\neg \mathsf{Ib}_A(\mathsf{SAT}, n^2)$ is satisfiable, there is a $poly(n)$-size* EF*-refutation (not necessarily of $\neg \mathsf{Ib}_A(\mathsf{SAT}, n^2)$) catching the adversary with probability $\geq 1/2 - 1/n$ over the randomness of the adversary.*

Proof: adversary claims to have a ckt solving SAT on A ⇒ force them to solve SAT □

Theorem 2 (Informal, cf. Theorem 6)**.**
Assume that SAT $\notin$ P/poly. *Then for each randomized p-time* EF*-adversary claiming that* $\neg\mathsf{tt}(\mathsf{SAT}, n^2)$ *is satisfiable, there is a* $2^{O(n)}$*-size* EF*-refutation catching the adversary with probability* $\geq 1/2 - 1/n$ *over the randomness of the adversary.*

$$\neg\mathsf{tt}(\mathsf{SAT}, n^2) := \neg\mathsf{lb}_{\{0,1\}^n}(\mathsf{SAT}, n^2)$$

Theorem 2 (Informal, cf. Theorem 6)**.**
Assume that SAT $\notin$ P/poly. *Then for each randomized p-time* EF*-adversary claiming that* $\neg\mathsf{tt}(\mathsf{SAT}, n^2)$ *is satisfiable, there is a* $2^{O(n)}$*-size* EF*-refutation catching the adversary with probability* $\geq 1/2 - 1/n$ *over the randomness of the adversary.*

$$\neg\mathsf{tt}(\mathsf{SAT}, n^2) := \neg\mathsf{lb}_{\{0,1\}^n}(\mathsf{SAT}, n^2)$$

- exploits that adversary is efficient w.r.t. the formula it receives

constructive proof complexity lower bounds

Theorem 3 (Constructive Res(k) lower bound of Razborov – Informal, cf. Theorem 7)**.** *For each sufficiently small $\delta > 0$, there is $\epsilon > 0$ and a $poly(t^{t^\delta})$-size randomized* Res(k)*-adversary C claiming that $\tau_W(A, b)$ is satisfiable, where $k = \epsilon \log t$ and $|W| = poly(t)$, such that for each $2^{t^{\Omega(\delta)}}$-size* Res(k)*-refutation π of any set of clauses, with probability $\geq 9/10$ over the randomness of C, π does not catch C.*

constructive proof complexity lower bounds

Theorem 3 (Constructive Res(k) lower bound of Razborov – Informal, cf. Theorem 7)**.** *For each sufficiently small $\delta > 0$, there is $\epsilon > 0$ and a $poly(t^{t^\delta})$-size randomized* Res(k)*-adversary C claiming that $\tau_W(A, b)$ is satisfiable, where $k = \epsilon \log t$ and $|W| = poly(t)$, such that for each $2^{t^{\Omega(\delta)}}$-size* Res(k)*-refutation π of any set of clauses, with probability $\geq 9/10$ over the randomness of C, π does not catch C.*

- doesn't work for $\neg\mathsf{tt}(\mathsf{SAT}, n^2)$
- in-depth analysis and twisting of the original proof

constructive proof complexity lower bounds

Theorem 3 (Constructive Res(k) lower bound of Razborov – Informal, cf. Theorem 7)**.**
For each sufficiently small $\delta > 0$, there is $\epsilon > 0$ and a $poly(t^{t^\delta})$-size randomized Res(k)*-adversary C claiming that $\tau_W(A, b)$ is satisfiable, where $k = \epsilon \log t$ and $|W| = poly(t)$, such that for each $2^{t^{\Omega(\delta)}}$-size* Res(k)*-refutation π of any set of clauses, with probability $\geq 9/10$ over the randomness of C, π does not catch C.*

Theorem 4 (Constructive pseudowidth lower bound – Informal, cf. Theorem 8)**.**
There is a $poly(m)$-size randomized Res*-adversary C claiming that $\neg\mathsf{PHP}_n^m$ with $m = 2^{n^{1/5}}$ is satisfiable such that for each $2^{\Omega(n^{1/4})}$-size* Res*-refutation π of any set of clauses, with probability $\geq 9/10$ over the randomness of C, π does not catch C.*

constructive proof complexity lower bounds

Theorem 3 (Constructive Res(k) lower bound of Razborov – Informal, cf. Theorem 7)**.**
For each sufficiently small $\delta > 0$, there is $\epsilon > 0$ and a $poly(t^{t^\delta})$-size randomized Res(k)*-adversary C claiming that $\tau_W(A, b)$ is satisfiable, where $k = \epsilon \log t$ and $|W| = poly(t)$, such that for each $2^{t^{\Omega(\delta)}}$-size* Res(k)*-refutation π of any set of clauses, with probability $\geq 9/10$ over the randomness of C, π does not catch C.*

Theorem 4 (Constructive pseudowidth lower bound – Informal, cf. Theorem 8)**.**
There is a $poly(m)$-size randomized Res*-adversary C claiming that $\neg\mathsf{PHP}_n^m$ with $m = 2^{n^{1/5}}$ is satisfiable such that for each $2^{\Omega(n^{1/4})}$-size* Res*-refutation π of any set of clauses, with probability $\geq 9/10$ over the randomness of C, π does not catch C.*

- new proof of a pseudo-width lower bound

constructive proof complexity lower bounds

Theorem 3 (Constructive $\mathsf{Res}(k)$ lower bound of Razborov – Informal, cf. Theorem 7)**.**
For each sufficiently small $\delta > 0$, there is $\epsilon > 0$ and a $poly(t^{t^\delta})$-size randomized $\mathsf{Res}(k)$-adversary C claiming that $\tau_W(A, b)$ is satisfiable, where $k = \epsilon \log t$ and $|W| = poly(t)$, such that for each $2^{t^{\Omega(\delta)}}$-size $\mathsf{Res}(k)$-refutation π of any set of clauses, with probability $\geq 9/10$ over the randomness of C, π does not catch C.

Theorem 4 (Constructive pseudowidth lower bound – Informal, cf. Theorem 8)**.**
There is a $poly(m)$-size randomized Res-adversary C claiming that $\neg\mathsf{PHP}_n^m$ with $m = 2^{n^{1/5}}$ is satisfiable such that for each $2^{\Omega(n^{1/4})}$-size Res-refutation π of any set of clauses, with probability $\geq 9/10$ over the randomness of C, π does not catch C.

Theorem 5 (Constructive AC^0-Frege lower bound – Informal, cf. Theorem 9)**.**
Let $\epsilon < 1/9^d$. There is a $poly(n^{n^\epsilon})$-size randomized AC^0_d-Frege-adversary C claiming that $\neg\mathsf{PHP}_n$ is satisfiable such that for each 2^{n^ϵ}-size AC^0_d-Frege-refutation π of any set of clauses, with probability $\geq 9/10$ over the randomness of C, π does not catch C.

constructive proof complexity lower bounds

Theorem 3 (Constructive Res(k) lower bound of Razborov – Informal, cf. Theorem 7)**.**
For each sufficiently small $\delta > 0$, there is $\epsilon > 0$ and a $poly(t^{t^\delta})$-size randomized Res(k)*-adversary C claiming that $\tau_W(A, b)$ is satisfiable, where $k = \epsilon$ l[illegible] and [illegible] $= poly(t)$, such that for each $2^{t^{\Omega(\delta)}}$-size* Res(k)*-refutation π of any set of cl[illegible]es, w[illegible] probability $\geq 9/10$ over the randomness of C, π does not catch C.*

Theorem 4 (Constructive pseudowidth lower [illegible]und – In[illegible]rma[illegible]. Theorem 8)**.**
There is a $poly(m)$-size randomized Res-[illegible]vers[illegible] *C cla[illegible]ng that $\neg\mathsf{PHP}_n^m$ with $m = 2^{n^{1/5}}$ is satisfiable such that for each $2^{\Omega(n^{1/4})}$-[illegible]e R[illegible]refu[illegible]tion π of any set of clauses, with probability $\geq 9/10$ over the randomness [illegible] do[illegible] not[illegible]tch C.*

Theorem 5 (Constr[illegible]ive AC[illegible]Freg[illegible]lower bound – Informal, cf. Theorem 9)**.**
Let $\epsilon < 1/9^d$. There[illegible] a p[illegible](n^{n^ϵ})-size randomized AC^0_d-Frege-adversary C claiming that $\neg\mathsf{PHP}_n$ is satisfiable suc[illegible]hat for each 2^{n^ϵ}-size AC^0_d-Frege-refutation π of any set of clauses, with probability $\geq 9/10$ over the randomness of C, π does not catch C.

UNIFIED

a lot of related work

open problems

- constructive Cutting Planes lower bounds
- avoid anticheckers in Thm 1