Upper and Lower Bounds for the Linear Ordering Principle

Edward A. Hirsch[1] Ilya Volkovich[2]

STACS 2026, Grenoble, France
March 11, 2026

[1]Ariel University
[2]Boston College

1- or 2-round protocols: probabilistic vs deterministic

Complexity classes (the result is determined in deterministic polynomial time):

- **NP**: the prover sends one message (a "proof").
- The prover tries to prove $x \in L$, the opponent tries to argue $x \notin L$.
  - "deterministic games": Σ_2^{P}, Π_2^{P}, $\mathbf{S_2^P}$, ...:
    the prover and the opponent send their proofs in a certain order.
  - "probabilistic games" $\mathbf{MA}$, $\mathbf{AM}$:
    the prover sends a proof, the opponent sends random bits.

In this talk we relate these two types.

Specific question:

A Boolean circuit $E(x, y)$ defines a linear order $x < y$.
What is the complexity of finding the minimum?

1- or 2-round protocols: probabilistic vs deterministic

Complexity classes (the result is determined in deterministic polynomial time):

- $\mathbf{NP}$: the prover sends one message (a "proof").
- The prover tries to prove $x \in L$, the opponent tries to argue $x \notin L$.
  - "deterministic games": Σ_2^{P}, Π_2^{P}, $\mathbf{S_2^P}$, ...:
    the prover and the opponent send their proofs in a certain order.
  - "probabilistic games" $\mathbf{MA}$, $\mathbf{AM}$:
    the prover sends a proof, the opponent sends random bits.

In this talk we relate these two types.

Specific question:

> A Boolean circuit $E(x, y)$ defines a linear order $x < y$.
> What is the complexity of finding the minimum?

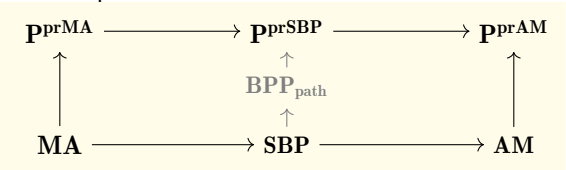
Complexity classes based on Arthur–Merlin protocols, and related

MA and **AM** classes (1980s):
Merlin (prover) and poly-time randomized Arthur (verifier) engage in a two-round protocol

Yes $x \in L \Rightarrow$ Merlin provides a proof that Arthur accepts.

No $x \notin L \Rightarrow$ Arthur will reject any Merlin's "proof" whp.

MA: First Merlin, then Arthur.
AM: First Arthur, then Merlin.



SBP: there is a poly-time NTM with same-length paths and some other polynomial p s.t.

Yes $x \in L \Rightarrow$ #accepting paths $\geqslant 2^{p(|x|)}$.

No $x \notin L \Rightarrow$ #accepting paths $\leqslant 2^{p(|x|)-1}$.

Contrary to **BPP**, this number can be small (say, $p(n) = 0$ provides **NP**).

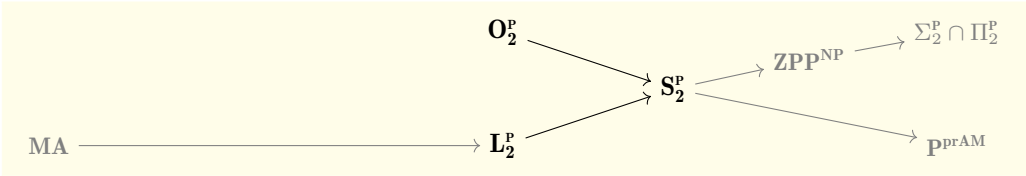
Promise problems (**prMA**, **prSBP**, **prAM**, ...): the algorithm separates a "yes" set and a "no" set, the remaining inputs are not solved and even class properties are not guaranteed.

"Loose" access to promise oracles:
the machine must work correctly irrespectively of oracle's answers outside "yes"/"no" sets.

Symmetric second level of the polynomial hierarchy

$\mathbf{S_2^P}$: Input x.
Yes-Prover provides w_Y, No-Prover provides w_N.
A poly-time verifier $V(x, w_Y, w_N)$ decides who wins.
Either Yes-Prover has a "universal" w_Y that beats every w_N,
or No-Prover has a "universal" w_N that beats every w_Y.

$\mathbf{O_2^P}$: Like $\mathbf{S_2^P}$, but the "universal" proof depends on $|x|$ and not on x.



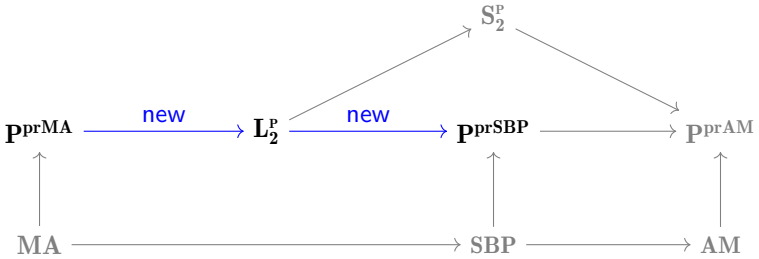
$\mathbf{L_2^P}$: [Korten, Pitassi, 2024]
Like $\mathbf{S_2^P}$, but w_Y,w_N start with the answer (1/0) and
the whole space is linearly ordered (so Verifier can compare also w_Y to w'_Y and w_N to w'_N).

Alternative definition: languages poly-time Turing-reducible to

LINEAR ORDERING PRINCIPLE: given a circuit $E(u, v)$ defining an order, find the minimum (or provide a counterexample to totality)

New containments

"Normal" classes (not input-oblivious)



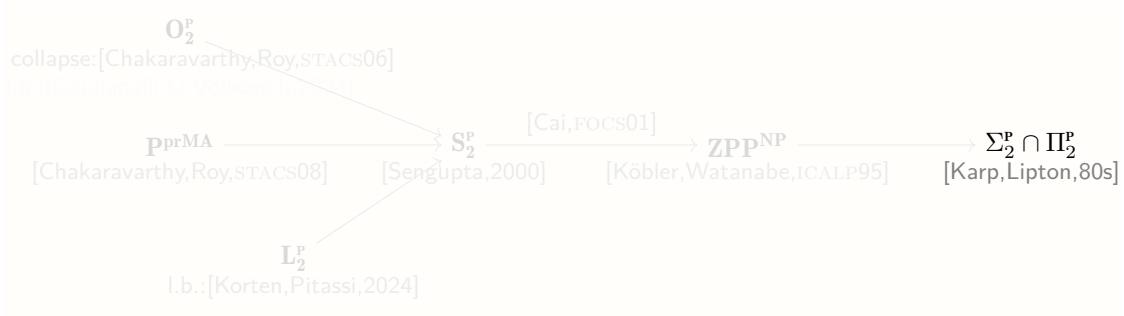
Open questions resolved:

- $\mathbf{P}^{\mathrm{prMA}} \subseteq \mathbf{S}_2^{\mathrm{p}}$? [Chakaravarthy, Roy, STACS-2008]
  (It was known that $\mathbf{P}^{\mathrm{MA}} \subseteq \mathbf{S}_2^{\mathrm{p}}$ [Russell, Sundaram, Comput. Compl. 1998].)
- Karp–Lipton collapse to $\mathbf{L}_2^{\mathrm{p}}$? [Korten, Pitassi, 2024]
  (A collapse to $\mathbf{P}^{\mathrm{prMA}}$ was known [Chakaravarthy, Roy, STACS-2008], the containment was not.)

Karp–Lipton theorems and fixed-polynomial circuit size lower bounds

Win–win argument when a collapse theorem to a class $\mathcal{C} \supseteq \mathbf{NP}$ is known $\boxed{\mathcal{C} \in \mathbf{P/poly} \Rightarrow \mathbf{PH} = \mathcal{C}}$:

if $\mathbf{NP} \subseteq \mathbf{P/poly}$, then $\mathcal{C}$ has no size-n^k circuits because $\mathbf{PH}$ has none [Kannan, 1982],
if $\mathbf{NP} \not\subseteq \mathbf{P/poly}$, then $\mathcal{C} \supseteq \mathbf{NP}$ has no size-n^k circuits trivially.



Currently smallest classes:

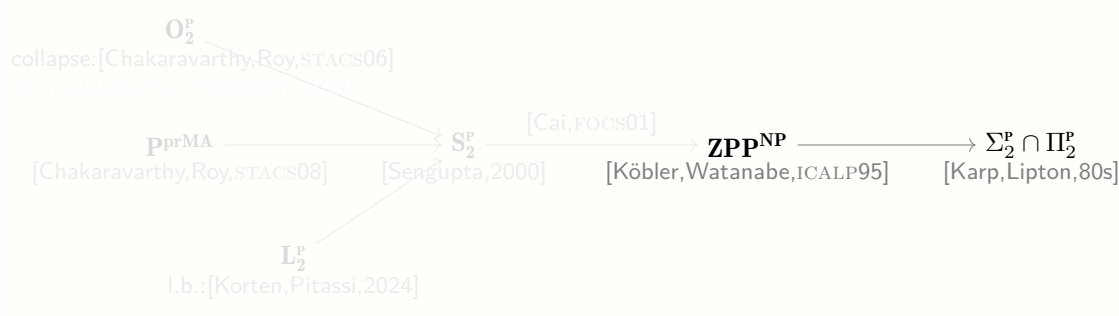
w.r.t. n^k-lower bound results: $\mathbf{O}_2^{\mathbf{p}}$ (range avoidance [CHR24,Li24,GLV24]) and $\mathbf{P}^{\mathbf{prMA}}$ (collapse),

w.r.t. collapse: $\mathbf{P}^{\mathbf{prQMA}}$ ($\mathbf{P}^{\mathbf{prQMA}} \subseteq \mathbf{O}_2^{\mathbf{p}}$ this paper, requires proving $\mathbf{P}^{\mathbf{prO}_2^{\mathbf{p}}} = \mathbf{O}_2^{\mathbf{p}}$).

Karp–Lipton theorems and fixed-polynomial circuit size lower bounds

Win–win argument when a collapse theorem to a class $\mathcal{C} \supseteq \mathbf{NP}$ is known $\boxed{\mathcal{C} \in \mathbf{P/poly} \Rightarrow \mathbf{PH} = \mathcal{C}}$:

if $\mathbf{NP} \subseteq \mathbf{P/poly}$, then $\mathcal{C}$ has no size-n^k circuits because $\mathbf{PH}$ has none [Kannan, 1982],
if $\mathbf{NP} \not\subseteq \mathbf{P/poly}$, then $\mathcal{C} \supseteq \mathbf{NP}$ has no size-n^k circuits trivially.



Currently smallest classes:

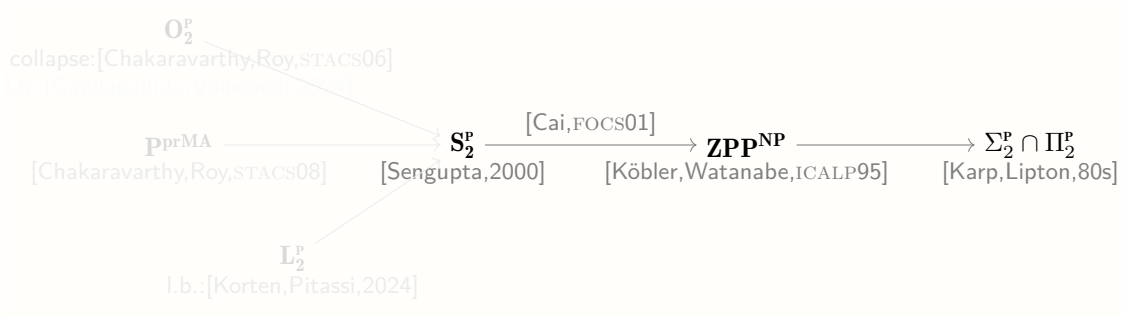
w.r.t. n^k-lower bound results: $\mathbf{O}_2^{\mathrm{p}}$ (range avoidance [CHR24,Li24,GLV24]) and $\mathbf{P}^{\mathbf{prMA}}$ (collapse),

w.r.t. collapse: $\mathbf{P}^{\mathbf{prOMA}}$ ($\mathbf{P}^{\mathbf{prOMA}} \subseteq \mathbf{O}_2^{\mathrm{p}}$ this paper, requires proving $\mathbf{P}^{\mathbf{prO}_2^{\mathrm{p}}} = \mathbf{O}_2^{\mathrm{p}}$).

Karp–Lipton theorems and fixed-polynomial circuit size lower bounds

Win–win argument when a collapse theorem to a class $\mathcal{C} \supseteq \mathbf{NP}$ is known $\boxed{\mathcal{C} \in \mathbf{P/poly} \Rightarrow \mathbf{PH} = \mathcal{C}}$:

if $\mathbf{NP} \subseteq \mathbf{P/poly}$, then $\mathcal{C}$ has no size-n^k circuits because $\mathbf{PH}$ has none [Kannan, 1982],
if $\mathbf{NP} \not\subseteq \mathbf{P/poly}$, then $\mathcal{C} \supseteq \mathbf{NP}$ has no size-n^k circuits trivially.



Currently smallest classes:

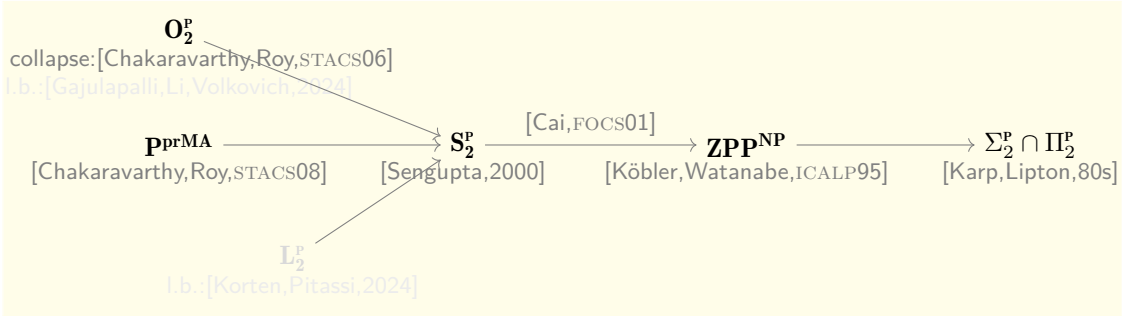
w.r.t. n^k-lower bound results: $\mathbf{O_2^p}$ (range avoidance [CHR24,Li24,GLV24]) and $\mathbf{P^{prMA}}$ (collapse),

w.r.t. collapse: $\mathbf{P^{prOMA}}$ ($\mathbf{P^{prOMA}} \subseteq \mathbf{O_2^p}$ this paper, requires proving $\mathbf{P^{prO_2^p}} = \mathbf{O_2^p}$).

Karp–Lipton theorems and fixed-polynomial circuit size lower bounds

Win–win argument when a collapse theorem to a class $\mathcal{C} \supseteq \mathbf{NP}$ is known $\boxed{\mathcal{C} \in \mathbf{P/poly} \Rightarrow \mathbf{PH} = \mathcal{C}}$:

if $\mathbf{NP} \subseteq \mathbf{P/poly}$, then $\mathcal{C}$ has no size-n^k circuits because $\mathbf{PH}$ has none [Kannan, 1982],
if $\mathbf{NP} \not\subseteq \mathbf{P/poly}$, then $\mathcal{C} \supseteq \mathbf{NP}$ has no size-n^k circuits trivially.



Currently smallest classes:

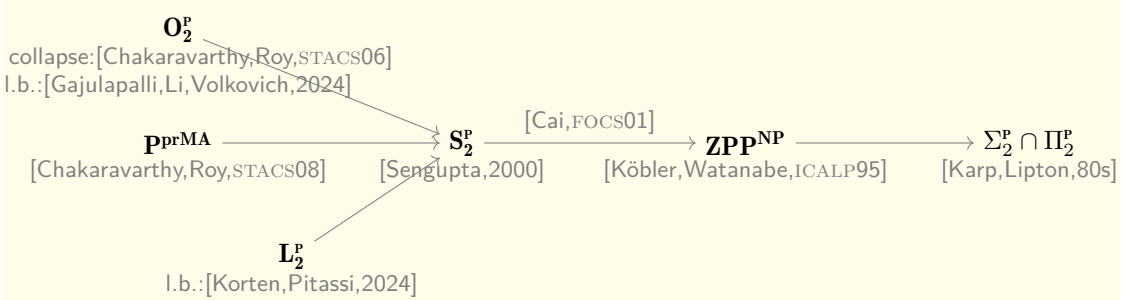
w.r.t. n^k-lower bound results: $\mathbf{O_2^p}$ (range avoidance [CHR24,Li24,GLV24]) and $\mathbf{P^{prMA}}$ (collapse),

w.r.t. collapse: $\mathbf{P^{prOMA}}$ ($\mathbf{P^{prOMA}} \subseteq \mathbf{O_2^p}$ this paper, requires proving $\mathbf{P^{prO_2^p}} = \mathbf{O_2^p}$).

Karp–Lipton theorems and fixed-polynomial circuit size lower bounds

Win–win argument when a collapse theorem to a class $\mathcal{C} \supseteq \mathbf{NP}$ is known $\boxed{\mathcal{C} \in \mathbf{P/poly} \Rightarrow \mathbf{PH} = \mathcal{C}}$:

if $\mathbf{NP} \subseteq \mathbf{P/poly}$, then $\mathcal{C}$ has no size-n^k circuits because $\mathbf{PH}$ has none [Kannan, 1982],
if $\mathbf{NP} \not\subseteq \mathbf{P/poly}$, then $\mathcal{C} \supseteq \mathbf{NP}$ has no size-n^k circuits trivially.



Currently smallest classes:

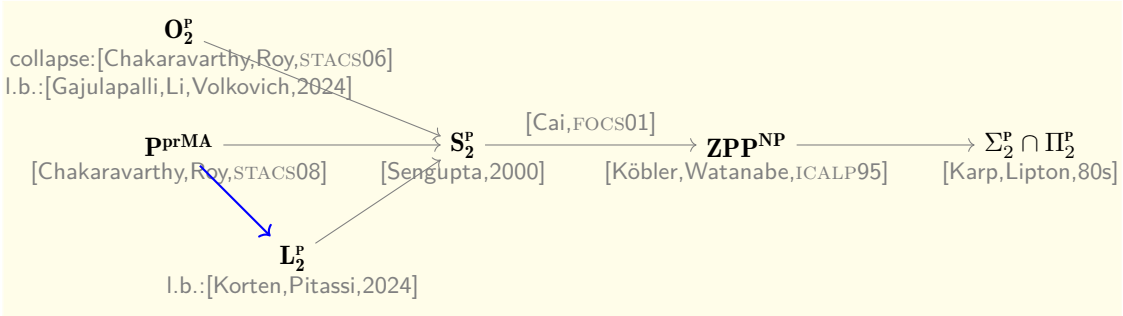
w.r.t. n^k-lower bound results: $\mathbf{O_2^p}$ (range avoidance [CHR24,Li24,GLV24]) and $\mathbf{P^{prMA}}$ (collapse),

w.r.t. collapse: $\mathbf{P^{prOMA}}$ ($\mathbf{P^{prOMA}} \subseteq \mathbf{O_2^p}$ this paper, requires proving $\mathbf{P^{prO_2^p}} = \mathbf{O_2^p}$).

Karp–Lipton theorems and fixed-polynomial circuit size lower bounds

Win–win argument when a collapse theorem to a class $\mathcal{C} \supseteq \mathbf{NP}$ is known $\boxed{\mathcal{C} \in \mathbf{P/poly} \Rightarrow \mathbf{PH} = \mathcal{C}}$:

if $\mathbf{NP} \subseteq \mathbf{P/poly}$, then $\mathcal{C}$ has no size-n^k circuits because $\mathbf{PH}$ has none [Kannan, 1982],
if $\mathbf{NP} \not\subseteq \mathbf{P/poly}$, then $\mathcal{C} \supseteq \mathbf{NP}$ has no size-n^k circuits trivially.



Currently smallest classes:

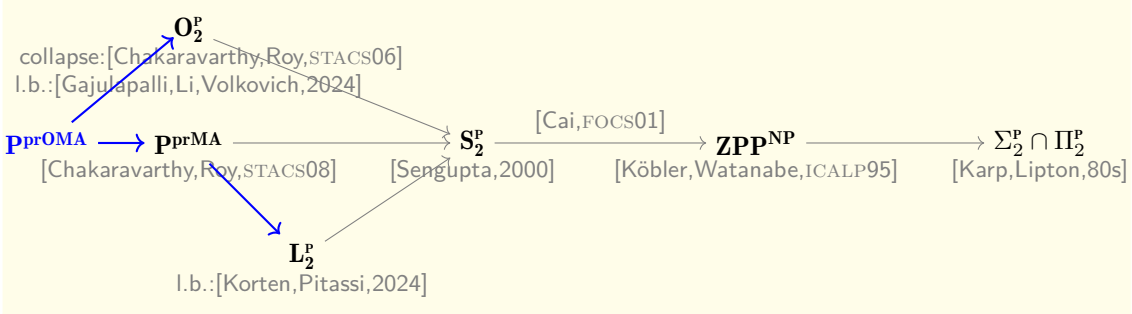
w.r.t. n^k-lower bound results: $\mathbf{O_2^p}$ (range avoidance [CHR24,Li24,GLV24]) and $\mathbf{P^{prMA}}$ (collapse),

w.r.t. collapse: $\mathbf{P^{prOMA}}$ ($\mathbf{P^{prOMA}} \subseteq \mathbf{O_2^p}$ this paper, requires proving $\mathbf{P^{prO_2^p}} = \mathbf{O_2^p}$).

Karp–Lipton theorems and fixed-polynomial circuit size lower bounds

Win–win argument when a collapse theorem to a class $\mathcal{C} \supseteq \mathbf{NP}$ is known $\boxed{\mathcal{C} \in \mathbf{P/poly} \Rightarrow \mathbf{PH} = \mathcal{C}}$:

if $\mathbf{NP} \subseteq \mathbf{P/poly}$, then $\mathcal{C}$ has no size-n^k circuits because $\mathbf{PH}$ has none [Kannan, 1982],
if $\mathbf{NP} \not\subseteq \mathbf{P/poly}$, then $\mathcal{C} \supseteq \mathbf{NP}$ has no size-n^k circuits trivially.



Currently smallest classes:

w.r.t. n^k-lower bound results: $\mathbf{O_2^p}$ (range avoidance [CHR24,Li24,GLV24]) and $\mathbf{P^{prMA}}$ (collapse),

w.r.t. collapse: $\mathbf{P^{prOMA}}$ ($\mathbf{P^{prOMA}} \subseteq \mathbf{O_2^p}$ this paper, requires proving $\mathbf{P^{prO_2^p}} = \mathbf{O_2^p}$).

Technique: Modern tools and syntactic classes for proving $\mathbf{P}^{\mathbf{prMA}} \subseteq \mathbf{L}_2^{\mathbf{P}}$

Dual Weak Pigeon-Hole Principle, nowadays known as Range Avoidance:
Given a circuit $C\colon \{0,1\}^n \to \{0,1\}^{n+1}$, find $y \in \{0,1\}^{n+1}$ outside its image.

Paris–Wilkie–Woods 1980s, Jeřabek 2000s, Korten 2021:

- Finding a Hard-Truth-Table is $\mathbf{P}^{\mathbf{NP}}$-equivalent to Range Avoidance.
- Finding a PRG reduces to it (cf. Nisan–Wigderson, 1990s).

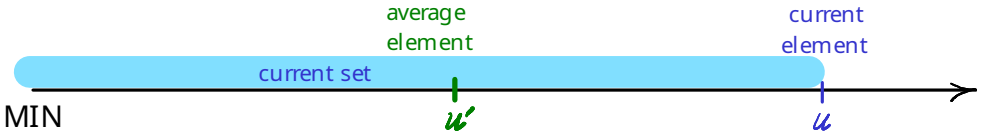
Korten–Pitassi 2024:
Range Avoidance reduces to Linear Ordering Principle (early known as MIN [Krajíček]).

Putting all that together:

- Find a PRG using Linear Ordering Principle,
- Thus derandomize $\mathbf{prMA}$ in $\mathbf{L}_2^{\mathbf{P}}$,
- Notice that for syntactic $\mathbf{L}_2^{\mathbf{P}} = \mathbf{P}^{\mathbf{L}_2^{\mathbf{P}}}$ one can drop "$\mathbf{pr}$".
- Conclude $\mathbf{P}^{\mathbf{prMA}} \subseteq \mathbf{L}_2^{\mathbf{P}}$.

Technique: Approximate counting for $\mathbf{L}_2^{\mathbf{P}} \subseteq \mathbf{P}^{\mathbf{prSBP}}$

Idea: Find the minimum of a linear order by finding an average element in $\{v : v < u\}$.



ApproxCount (received much attention in logic [Jeřabek] and quantum computation [many!]):
Given a circuit C, approximate the number of satisfying assignments *up to a multiplicate constant*.

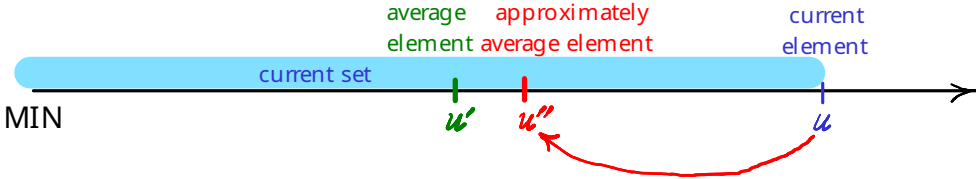
SBP almost captures its power: $\mathbf{P}^{\text{ApproxCount}} = \mathbf{P}^{\mathbf{prSBP}}$.

Consider a linear order computed by a circuit: $u < v \iff E(u, v) = 1$.

- Given some u,
  the element u' corresponding to the average rank in $\{v : v < u\}$ is much smaller than u.
- ApproxCount allows to *approximate* the size of preimage $C^{-1}(1)$.
- ... thus the average rank (the number in the order) of a subset *(not necessarily continuous)*.
- Perform search–to–approximate_decision to find u'' closer to the minimum.
- Repeat it until the minimum is found.

Technique: Approximate counting for $\mathbf{L}_2^{\mathrm{P}} \subseteq \mathbf{P}^{\mathbf{prSBP}}$

Idea: Find the minimum of a linear order by finding an average element in $\{v : v < u\}$.



ApproxCount (received much attention in logic [Jeřabek] and quantum computation [many!]):
Given a circuit C, approximate the number of satisfying assignments *up to a multiplicate constant*.

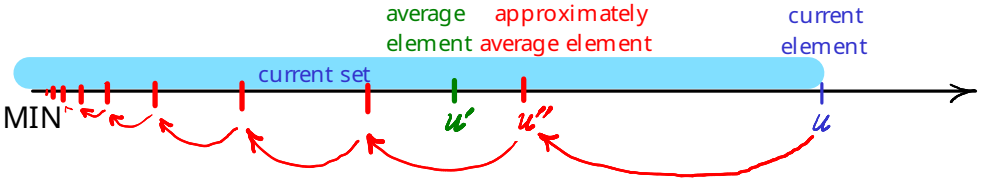
SBP almost captures its power: $\mathbf{P}^{\text{ApproxCount}} = \mathbf{P}^{\mathbf{prSBP}}$.

Consider a linear order computed by a circuit: $u < v \iff E(u, v) = 1$.

- Given some u,
  the element u' corresponding to the average rank in $\{v : v < u\}$ is much smaller than u.
- ApproxCount allows to *approximate* the size of preimage $C^{-1}(1)$.
- ... thus the average rank (the number in the order) of a subset *(not necessarily continuous)*.
- Perform search–to–approximate_decision to find u'' closer to the minimum.
- Repeat it until the minimum is found.

Technique: Approximate counting for $\mathbf{L}_2^{\mathbf{P}} \subseteq \mathbf{P}^{\mathbf{prSBP}}$

Idea: Find the minimum of a linear order by finding an average element in $\{v : v < u\}$.



ApproxCount (received much attention in logic [Jeřabek] and quantum computation [many!]):
Given a circuit C, approximate the number of satisfying assignments *up to a multiplicate constant*.

SBP almost captures its power: $\mathbf{P}^{\text{ApproxCount}} = \mathbf{P}^{\mathbf{prSBP}}$.

Consider a linear order computed by a circuit: $u < v \iff E(u, v) = 1$.

- Given some u,
  the element u' corresponding to the average rank in $\{v : v < u\}$ is much smaller than u.
- ApproxCount allows to *approximate* the size of preimage $C^{-1}(1)$.
- ... thus the average rank (the number in the order) of a subset *(not necessarily continuous)*.
- Perform search–to–approximate_decision to find u'' closer to the minimum.
- Repeat it until the minimum is found.

Open questions

- Fixed-polynomial lower bounds for $\mathbf{P}^{\mathbf{prOMA}}$ or for $\mathbf{ZPP}^{\mathbf{ONP}}$.
- $\mathbf{P}^{\mathbf{prOMA}}$ vs $\mathbf{ZPP}^{\mathbf{ONP}}$ (another collapse), what is smaller originally?

  Note: $\mathbf{S}_2^{\mathbf{P}} \subseteq \mathbf{ZPP}^{\mathbf{NP}}$, but $\mathbf{ZPP}^{\mathbf{ONP}} \subseteq \mathbf{O}_2^{\mathbf{P}}$. There's something here!
- The power of approximate counting: what else is contained in $\mathbf{P}^{\mathbf{prSBP}}$ &co?
- A lot of work yet to be done w.r.t. new total search classes of the second level [Kleinberg,Korten,Mitropolsky,Papadimitriou,2021] + follow-ups.