On Exponential-Time Hypotheses, Derandomization, and Circuit Lower Bounds

Lijie Chen, Ron Rothblum, Roei Tell, and Eylon Yogev

Theory Seminar @ TAU, December 2019

מכון ויצמן למדע
WEIZMANN INSTITUTE OF SCIENCE

Background and Context

the main questions

Exponential-Time Hypothesis

- ETH: “Exponential” P ≠ NP

  - **Exponential-Time Hypothesis (ETH):**
    There exist $\varepsilon>0$ and $c>1$ such that 3-SAT on n vars and $c \cdot n$ clauses can’t be decided in time $2^{\varepsilon \cdot n}$ [IP’01, IPZ’01]

Exponential-Time Hypothesis

- ETH: "Exponential" P ≠ NP

- **Exponential-Time Hypothesis (ETH):**
  There exist $\varepsilon>0$ and $c>1$ such that 3-SAT on n vars and $c \cdot n$ clauses can't be decided in time $2^{\varepsilon \cdot n}$ [IP'01, IPZ'01]

- **Strong Exponential-Time Hypothesis (SETH):**
  There exist $\varepsilon_k \to 0$ and $c_k \to \infty$ such that k-SAT on n vars and $c_k \cdot n$ clauses can't be decided in time $2^{(1-\varepsilon_k) \cdot n}$ [IP'01]

Exponential-Time Hypothesis

- ETH: “Exponential” P ≠ NP

  - **Exponential-Time Hypothesis (ETH):**
    There exist $\varepsilon>0$ and $c>1$ such that 3-SAT on n vars and $c \cdot n$ clauses can’t be decided in time $2^{\varepsilon \cdot n}$ [IP’01, IPZ’01]

  - **Strong Exponential-Time Hypothesis (SETH):**
    There exist $\varepsilon_k \to 0$ and $c_k \to \infty$ such that k-SAT on n vars and $c_k \cdot n$ clauses can’t be decided in time $2^{(1-\varepsilon_k) \cdot n}$ [IP’01]

Randomized ETH

- rETH: "Exponential" NP ⊄ BPP

- **Randomized Exponential-Time Hypothesis (rETH):** There exist ε>0 and c>1 such that 3-SAT on n vars and $c \cdot n$ clauses can't be decided in randomized time $2^{\varepsilon \cdot n}$ [DHMTM'14]

Non-Deterministic ETH

- NETH: "Exponential" coNP $\not\subset$ NP

  - **Non-Deterministic Exponential-Time Hypothesis (NETH):** There exist $\varepsilon>0$ and $c>1$ such that co-3-SAT on n vars and $c \cdot n$ clauses can't be decided by non-deterministic machines that run in time $2^{\varepsilon \cdot n}$ [CGIMPS'18]

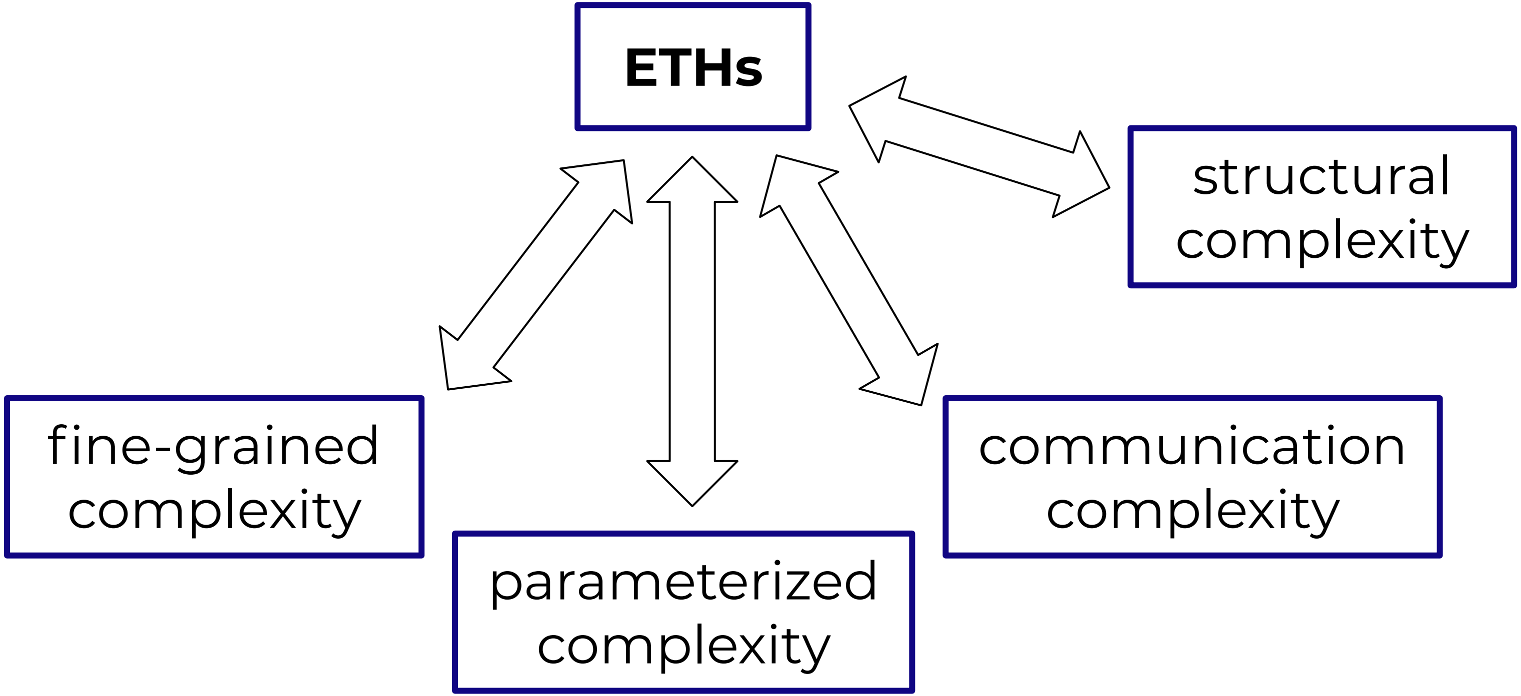
Exponential-Time Hypothese**s**

- ETHs: “Exponential” versions of classical conjectures

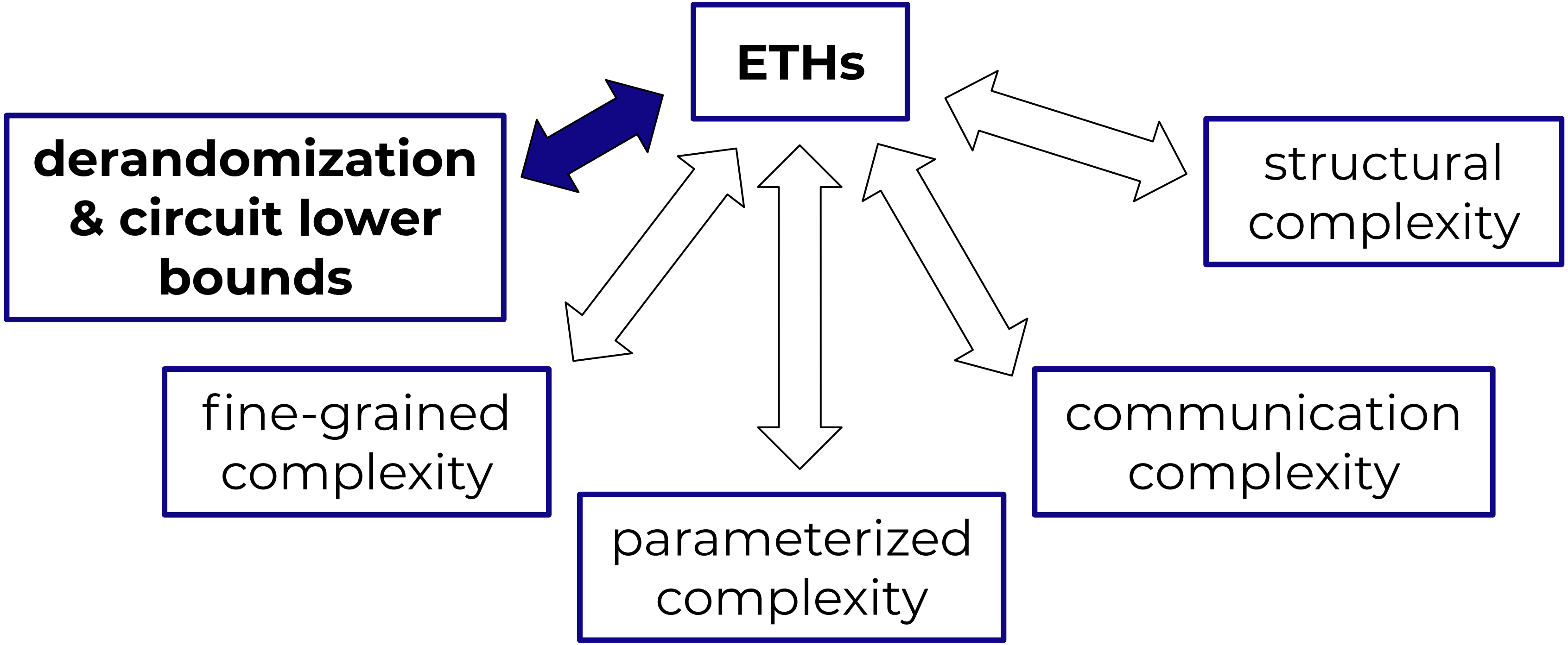
  - ETH: “Exponential” $P \neq NP$ [IP’01, IPZ’01]
  - rETH: “Exponential” $NP \not\subset BPP$ [DHMTM’14]
  - NETH: “Exponential” $coNP \not\subset NP$ [CGIMPS’18]
  - AMETH: “Exponential” $coNP \not\subset AM$ [Wil’16]
  - #ETH: “Exponential” $\#P \not\subset P$ [DHMTM’14]
  - …

1 as far as we know all ETHs above might be true (only Strong MAETH refuted [Wil’16])

Broad influence of ETHs in complexity



Broad influence of ETHs in complexity



Derandomization

› randomness in computation

- Randomness crucial for crypto, learning, sublinear-time…
- Can randomness help solve decision problems?
- **Conj 1** [Gill'77]: BPP = P
  - randomness can save at most a poly runtime factor
  - might still allow simpler & mildly faster algs

1 throughout the talk, complexity classes always refer to promise-problems

Circuit lower bounds

› uniform vs non-uniform computational models

- Can we solve problems more efficiently using a different algorithm for each input length?
- **Conj 2:** $\forall s$, $\mathrm{DTIME}[s^{O(1)}] \not\subset \text{io-SIZE}[s]$
  - some problems can't be solved faster using non-uniformity
  - might still allow mildly faster algs (and other speedups)

Derandomization vs ckt lbs

- uniform vs non-uniform computational models

- **Thm** [IW'99]: Conj 2 ⇒ Conj 1
  - "hardness to randomness"
- **Thms:** Conj 1 ⇒ weak versions of Conj 2
  - "derandomization implies circuit lower bounds"
- array of bidirectional connections between weak versions

1 e.g., [BFT'98,IKW'02,KI'04,...,Wil'13,MW'18,T'19,Che'19,CR'20,...]

Important reminder

› ETHs are uniform

- ETHs refer to lower bounds for uniform algorithms
  - … rather than for non-uniform circuits
- The question is how uniform lower bounds affect
  1. derandomization
  2. circuit lower bounds

Key takeaways

- Even relatively-mild variants of ETHs have far-reaching implications to derandomization & ckt lbs
- Results of independent interest for long-standing qs

Key takeaways

- Even relatively-mild variants of ETHs have far-reaching implications to derandomization & ckt lbs
- Results of independent interest for long-standing qs
- **An exponentially-hard (uniform) world encompasses strong answers to the central qs in derand & ckts lbs**

Main Contributions

and their meaning

A technicality

› ETHs refer to “almost-exp” hardness

› A 3-SAT instance with v vars and O(v) clauses is represented by $n = O(v \cdot \log(v))$ bits

› **ETHs:** Solving 3-SAT requires $2^{\varepsilon \cdot v} = \mathbf{2^{\varepsilon' \cdot (n/\log(n))}}$ time

Landscape of ETHs

- ascending strength (morally)

  - ETH: “Exponential” $P \neq NP$
  - rETH: “Exponential” $NP \not\subseteq BPP$
  - NETH: “Exponential” $coNP \not\subseteq NP$
  - MAETH: “Exponential” $coNP \not\subseteq MA$
  - AMETH: “Exponential” $coNP \not\subseteq AM$
  - …

Landscape of ETHs

- ascending strength (morally)

- ETH: “Exponential” $\mathsf{P} \neq \mathsf{NP}$
- rETH: “Exponential” $\mathsf{NP} \not\subseteq \mathsf{BPP}$
- NETH: “Exponential” $\mathsf{coNP} \not\subseteq \mathsf{NP}$
- **MAETH: “Exponential” $\mathsf{coNP} \not\subseteq \mathsf{MA}$**
- AMETH: “Exponential” $\mathsf{coNP} \not\subseteq \mathsf{AM}$
- …

Assuming MAETH

Assuming MAETH

Assuming MAETH

- Essentially optimal derand & ckt lbs
- **Thm 1:** Assuming MAETH,[1]
  - $\forall s$, $\mathrm{SIZE}[s^{O(1)}] \not\subset \text{io-DTIME}[s]$
  - BPP = P
- Follows easily from known Karp-Lipton thms [BFNW'93]

1 for these specific statements we actually need to assume $E \not\subset \text{i.o.-MA}[2^{\varepsilon \cdot n}]$, but MAETH implies similar ones

Landscape of ETHs

- area of focus: beneath MAETH

- ETH: “Exponential” $P \neq NP$
- rETH: “Exponential” $NP \not\subset BPP$
- NETH: “Exponential” $coNP \not\subset NP$
- MAETH: “Exponential” $coNP \not\subset MA$
- AMETH: “Exponential” $coNP \not\subset AM$
- ...

Landscape of ETHs

- area of focus: beneath MAETH

- ETH: “Exponential” $P \neq NP$
- **rETH: “Exponential” $NP \not\subset BPP$**
- NETH: “Exponential” $coNP \not\subset NP$
- MAETH: “Exponential” $coNP \not\subset MA$
- AMETH: “Exponential” $coNP \not\subset AM$
- ...

rETH ⇒ derandomization of BPP

- informal

  - **Thm 2:**

    rETH ⇒ BPP ⊆ "almost P" in average-case

rETH ⇒ derandomization of BPP

- informal

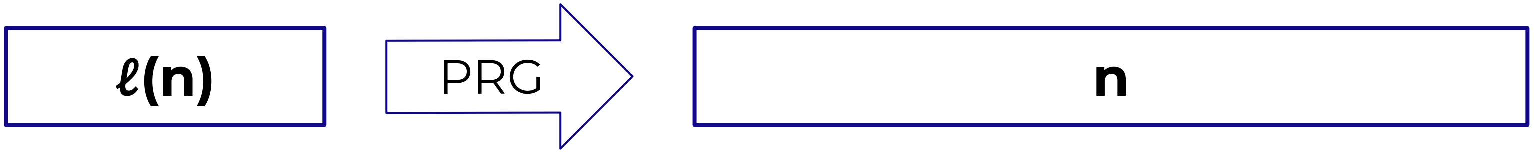
- **Thm 2:**

  rETH ⇒ BPP ⊆ “almost P” in average-case

- Very fast “effective” derandomization of BPP
- Technically: Significant strengthening of state-of-the-art uniform hardness-to-randomness results

Background

› pseudorandom generators (PRGs)



› output "looks random" to class of distinguishers

› simulate random algorithm with $\ell(n) \ll n$ coins

› enumerate over $2^{\ell(n)}$ possibilities to eliminate randomness

  › large "stretch" ⇒ fast derandomization

Background

› standard (non-uniform) hardness-to-randomness

› **Standard hardness-to-randomness (non-uniform):**

Lower bounds for non-uniform circuits

⇒ PRGs for non-uniform distinguishers

⇒ worst-case derandomization of BPP

› e.g., [Yao'82, BM'84, Nis'91, NW'94, IW'99, SU'01, Uma'03]

Background

- standard (non-uniform) hardness-to-randomness

- Essentially optimal results [IW'99, Uma'03]
  - $E \not\subset SIZE[T] \Rightarrow$ stretch $\approx T$
  - $E \not\subset io\text{-}SIZE[2^{\varepsilon \cdot n}] \Rightarrow BPP=P$
- Better lower bounds ⇒ faster derandomization
- Required hardness is against E

Background

› uniform hardness-to-randomness

› **Analogous uniform hardness-to-randomness:**

Lower bounds for uniform probabilistic algs

$\Rightarrow$ PRGs for uniform distinguishers

$\Rightarrow$ average-case derandomization of BPP

› e.g., [IW’98,CNS’99,Kab’01,GST’03,TV’07,SU’07,GV’08,Gol’11,CIS’18]

Background

› uniform hardness-to-randomness

- Ideally:
  - $E \not\subset BPTIME[T] \Rightarrow$ stretch $\approx T$
  - $E \not\subset BPTIME[2^{\varepsilon \cdot n}] \Rightarrow BPP = P$ in average case
- What we know:
  - Better lower bounds $\not\Rightarrow$ faster derandomization
  - Need hardness is against PSPACE

Background

› uniform hardness-to-randomness

	hypothesis	PRG stretch
IW'98	$E \not\subset BPTIME[T]$	half-T (i.e., $T \approx S \circ S$)
CNS'98	$\#P \not\subset BPTIME[T]$	$T(n^{\Omega(1)})^{\Omega(1)}$
Kab'01	$E \not\subset ZPTIME[T]$	half-T (HSG)
TV'07	$PSPACE \not\subset BPTIME[T]$	$T(n^{\Omega(1)})^{\Omega(1)}$
GV'07	$PSPACE \not\subset$ io-$BPTIME[T]$	$T(n^{\Omega(1)})^{\Omega(1)}$ (HSG, aa)
CIS'18	k-OV $\not\subset$ io-$BPTIME[n^{(1/2+\varepsilon) \cdot k}]$	$BPP \subseteq$ uni-P (not PRG)

Background

› “high-end” uniform hardness-to-randomness

- Previous ways to bypass the challenge:
  - stronger hypotheses (prBPP=prP [Gol’11]; OV/SETH [CIS’18])
  - non-deterministic settings (AM [GST’03] or MA [this work])
- We want to start “only” from a lower bound of $2^{n/\text{polylog}(n)}$ for probabilistic algorithms…

rETH ⇒ derandomization of BPP

- **Thm 2.1:** Assume that **TQBF ∉ BPTIME[$2^{n/polylog(n)}$]**. Then, there exists a PRG with stretch $2^{n/polylog(n)}$ that "fools" ppt distinguishers (infinitely-often).

L ∈ BPP ⇒ deterministic **algorithm A_L** time $n^{polyloglog(n)}$ ⇒ **∀ distribution X** (polytime samplable) $Pr_{x \sim X}[A_L(x)=L(x)]>1-1/|x|$

(for infinitely-many |x| ∈ N)

1 recall: 3-SAT reducible to TQBF in linear time

rETH ⇒ derandomization of BPP

- "High-end" uniform hardness-to-randomness
  - Near-exp hardness ⇒ near-exp stretch
  - Significant technical strengthening of state-of-the-art
- Remaining gap to optimal result:
  - Stretch isn't purely exponential
  - Need hardness against a PSPACE problem

rETH ⇒ derandomization of BPP

- **Thm 2.2:** Assume **TQBF $\notin$ io-BPTIME[$2^{n/polylog(n)}$]**. Then,
  1. There exists a PRG with stretch $2^{n/polylog(n)}$ that "fools" ppt distinguishers on almost all input lengths using logloglog(n) advice bits.
  2. There exists a HSG with stretch $2^{n/polylog(n)}$ that "hits" ppt distinguishers on almost all input lengths.

1 overcoming an "infinitely-often" vs "almost-always" barrier

A taste of the proof

- Classical proof approach:
  - base PRG on “hard” function $f:\{0,1\}^* \to \{0,1\}^*$
  - distinguisher for PRG ⇒ efficient alg/ckt that computes f
  - no efficient alg/ckt for f ⇒ PRG fools distinguisher class
- Essentially optimal non-uniform transformations known
  - distinguisher of size T ⇒ non-uniform ckt of size ≈ T
  - crucially relies on non-uniformity

A taste of the proof

- In the uniform setting:
  - uniform distinguisher ⇒ efficient alg that computes f
- Idea: Require more structure from f [IW'98]
  - e.g., downward self-reducible & random self-reducible
  - allows for not-too-costly transformation
  - function with such structure must be in PSPACE

A taste of the proof

- Key issue: Transformation overhead
  - large overhead ⇒ limited stretch of PRG
- Pivots for progress:
  1. show a well-structured candidate “hard” function
  2. prove that it supports an efficient transformation

A taste of the proof

- State-of-the-art idea [TV'07]:
  - construct an artificial well-structured func
  - show a reduction from a natural problem (3-SAT, TQBF…)
  - use its properties to show an efficient transformation
- Our approach: Design artificial func with more structure,
  show very efficient reduction & transformation

A taste of the proof

- Func of [TV'07] based on IP=PSPACE proof
  - PSPACE-complete
  - low-degree polynomials
  - downward self-reducible
- Our func: Based on highly optimized IP=PSPACE proof
  - round reduction
  - optimized arithmetization
  - suitable for very efficient reduction from TQBF

A taste of the proof

- That's it
- No technicalities in the talk

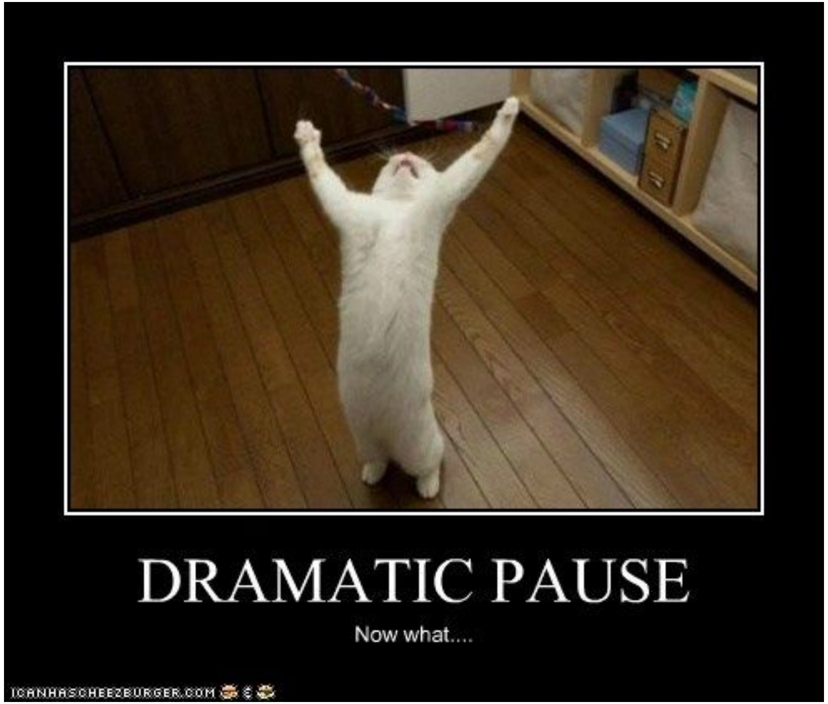
Landscape of ETHs

› area of focus: beneath MAETH

- ETH: “Exponential” P $\neq$ NP
- rETH: “Exponential” NP $\not\subset$ BPP
- **NETH: “Exponential” coNP $\not\subset$ NP**
- MAETH: “Exponential” coNP $\not\subset$ MA
- AMETH: “Exponential” coNP $\not\subset$ AM
- …

Switching gears...

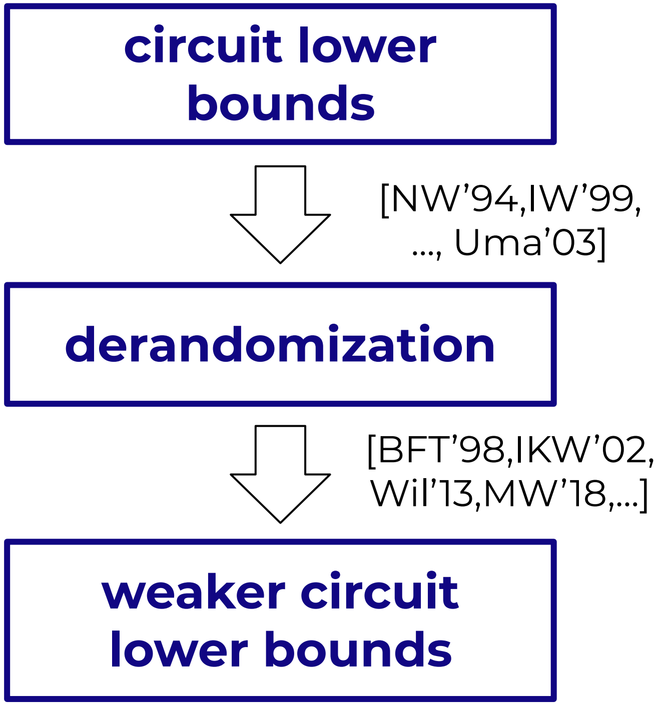
Switching gears...



Switching gears...

- Context switch
- Our conclusions will lie in the non-uniform setting:
  - worst-case derandomization of BPP
  - circuit lower bounds

Background


circuit lower bounds
[NW'94,IW'99, ..., Uma'03]
derandomization
[BFT'98,IKW'02, Wil'13,MW'18,...]
weaker circuit lower bounds

Background

circuit lower bounds

⇓ [NW'94,IW'99, ..., Uma'03]

derandomization

⇓ [BFT'98,IKW'02, Wil'13,MW'18,...]

weaker circuit lower bounds

E ⊄ P/poly

⇓

BPP ⊆ SUBEXP

⇓

NP ⊄ SIZE[n^{100}]

E ⊄ SIZE[$2^{\varepsilon n}$]

⇓

BPP=P

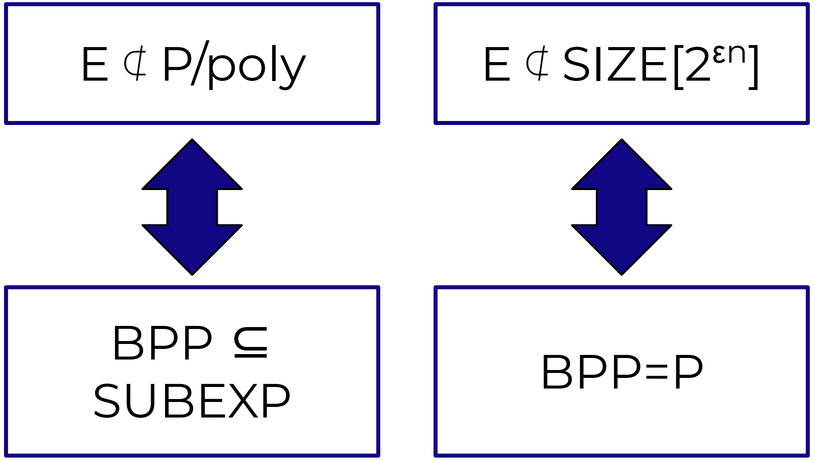
⇓

NTIME[s] ⊄ SIZE[s∘s]

The equivalence conjecture

- <u>**Conj:**</u> Derandomization of BPP is equivalent to specific corresponding circuit lower bounds

- Impl: Canonical “black-box“ derandomization (via PRG)
- Mentioned “in passing” in the past [IKW’02, TV’07]; seems more realistic now [MW’18]; explicitly raised in [T’19]



Very weak NETH ⇒ equivalence conj

- informal
  - **Thm 3:**
    - very weak variant of NETH ⇒ conj is true
    - add’l implication in converse direction

Very weak NETH ⇒ equivalence conj

- informal
  - **Thm 3:**
    - very weak variant of NETH ⇒ conj is true
    - add’l implication in converse direction
  - Evidence that conj is true, suitable pathway

Background

› NTIME-uniform circuits

- **Def:** $L \subseteq \{0,1\}^*$ has **NTIME[T]-uniform circuits** if exists non-deterministic machine M that gets input 1^n, runs in time T(n), and for some guesses outputs a circuit $C:\{0,1\}^n \to \{0,1\}$ that computes L_n (otherwise: $\perp$)
- **Def:** $L \subseteq \{0,1\}^*$ has **NTIME[T]-uniform circuits of size S(n)**

  $\Rightarrow$ the output ckt is of size $S(n) \ll T(n)$

Background

- NTIME-uniform circuits

- Notion refers to uniform complexity
- Subclass of NTIME[T] ∩ SIZE[S] (seems strict)
  - Single proof per input length
  - Can efficiently verify the (per-input-length) circuit
- Known lower bounds [SW'13]

Background

› NTIME-uniform circuits

› NETH means "co-3-SAT $\notin$ NTIME[$2^{\varepsilon \cdot n/\log(n)}$]"

› Our hypotheses will be of the form:

"co-3-SAT can't be solved by NTIME[$2^{\varepsilon \cdot n/\log(n)}$]-uniform ckts"

› seem weaker than classical "NP $\neq$ coNP" conjs

› we'll even replace co-3-SAT with potentially harder probs

Very weak NETH ⇒ equivalence conj

- "low-end": subexp derandomization and weak lower bounds

- **Thm 3.1:** If E does not have NTIME[2^{n^δ}]-uniform circuits of polynomial size (for some δ>0), then

$$BPP \subseteq \text{i.o.-}SUBEXP \Leftrightarrow E \not\subseteq P/poly$$

where SUBEXP = $\cap_{\varepsilon>0} TIME[2^{n^\varepsilon}]$.

Very weak NETH ⇒ equivalence conj

- "low-end": subexp derandomization and weak lower bounds

- **Thm 3.1:** If E does not have NTIME[2^{n^δ}]-uniform circuits of polynomial size (for some δ>0), then

$$BPP \subseteq \text{i.o.-SUBEXP} \Leftrightarrow E \not\subset P/poly$$

where SUBEXP = $\cap_{\varepsilon>0}$TIME[2^{n^ε}].

- Moreover, can replace "SUBEXP" by "NSUBEXP"

Very weak NETH ⇒ equivalence conj

› ”high-end”: polytime derandomization and strong lower bounds

› **Thm 3.2:** If E does not have NTIME[$2^{\delta \cdot n}$]-uniform circuits even infinitely-often (for some δ>0), then

$$BPP = P \Leftrightarrow \exists\, \varepsilon>0 : E \not\subseteq \text{i.o. } SIZE[2^{\varepsilon \cdot n}]$$

Very weak NETH ⇒ equivalence conj

- ”high-end”: polytime derandomization and strong lower bounds

- **Thm 3.2:** If E does not have NTIME[$2^{\delta \cdot n}$]-uniform circuits even infinitely-often (for some δ>0), then

$$BPP = P \Leftrightarrow \exists\, \varepsilon>0 : E \not\subset \text{i.o. } SIZE[2^{\varepsilon \cdot n}]$$

- (scaling is non-trivial & non-smooth, requires diff techs)

Very weak NETH ⇐ equivalence conj

› the converse direction, informal

› **Thm 3.3:** Assume that the “moreover” conclusion of Thm 3.1 holds. Then, E doesn’t have NP-uniform circuits.

1 can improve the conclusion from NP-uniform to NTIME[T]-uniform, for $T(n)=2^{n^{o(1)}}$

A taste of the proof

- of Thm 3.1

- **Obs:** Classical KL result [BFNW’93] implies

$$\text{NETH} \Rightarrow (\quad \text{BPP} \subseteq \text{SUBEXP} \Leftrightarrow \text{EXP} \not\subseteq \text{P/poly} \quad)$$

  - follows as logical consequence (albeit not transparent)

A taste of the proof

- of Thm 3.1

- **<u>Obs:</u>** Classical KL result [BFNW'93] implies

$$\text{NETH} \Rightarrow (\quad \text{BPP} \subseteq \text{SUBEXP} \Leftrightarrow \text{EXP} \not\subseteq \text{P/poly} \quad)$$

- <u>**Pf** (" ⇒ direction"):</u> Assume tac EXP ⊆ P/poly. Then,

1. EXP = MA (by EXP ⊆ P/poly & [BFNW'93])
2. EXP ⊆ NSUBEXP (BPP ⊆ SUBEXP)
3. Contradicts NETH (3SAT should be hard for time $2^{\varepsilon' \cdot n/\log(n)}$)

A taste of the proof

- of Thm 3.1

- **Obs:** Classical KL result [BFNW'93] implies

$$\text{NETH} \Rightarrow (\quad \text{BPP} \subseteq \text{SUBEXP} \Leftrightarrow \text{EXP} \not\subset \text{P/poly} \quad)$$

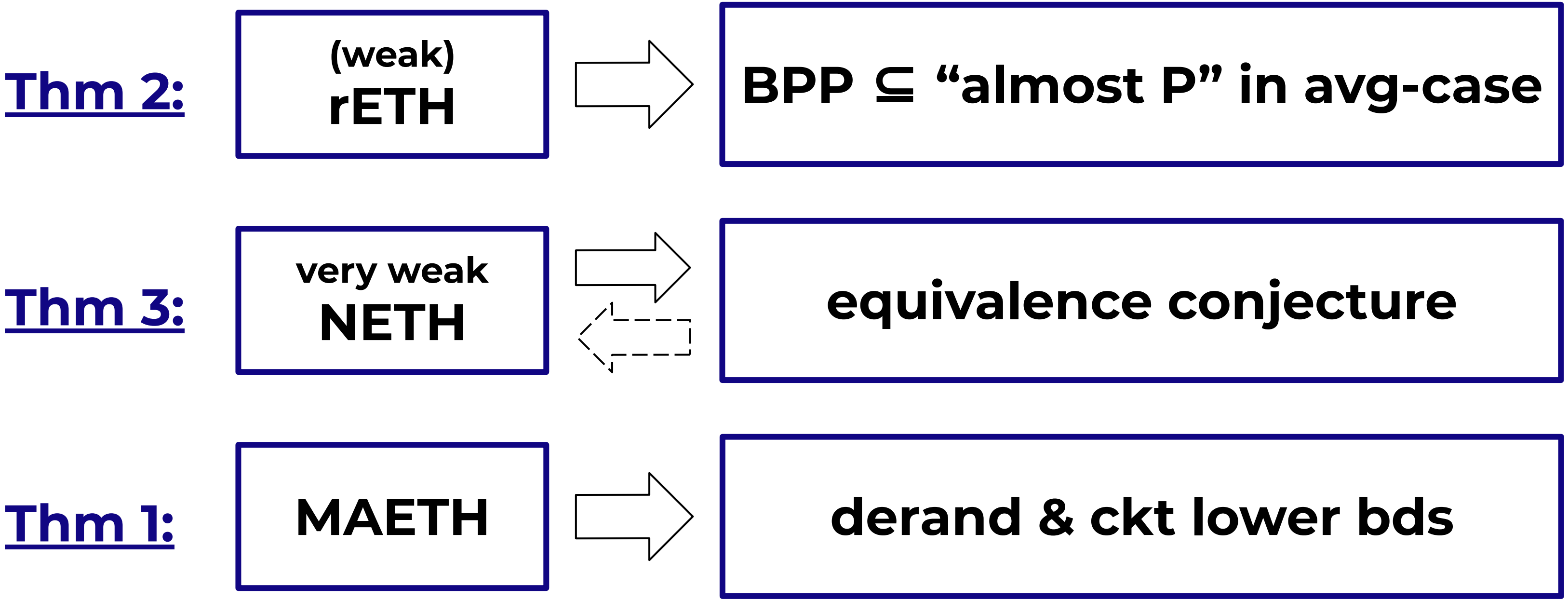
- Our tech contribution: Weaken the hypothesis to refer to lower bds for NTIME[T]-uniform ckts of bounded size
  - same logical structure of pf
  - pivotal step: strengthen the KL result

A taste of the proof

- of Thm 3.1

- **Prop:** If EXP ⊆ P/poly and BPP=NSUBEXP then
  EXP has NSUBEXP-uniform ckts of poly size
- **Clm 1:** EXP has MA-uniform randomized ckts of poly size
  - Idea: Refine original construction using modern tools
- **Clm 2:** Verifier and ckt can be derandomized
  - Idea: Apply to original KL thm to find fixed random string

Our main results



Some additional results in the paper

- Refuting a weak version of rETH requires new ckt lbs
  - probabilistic circuit-analysis alg ⇒ ckt lbs
- Additional new Karp-Lipton thms
  - collapse of BPE to quasilin-ckts ⇒ BPP ⊆ “almost P” in avg-case
- Based on techs developed on the way to main results

Key takeaways

- Even relatively-mild variants of ETHs have far-reaching implications to derandomization & ckt lbs
- Results of independent interest for long-standing qs
- **An exponentially-hard (uniform) world encompasses strong answers to the central qs in derand & ckts lbs**

Thank you!

$\Rightarrow$ rETH implies BPP $\subseteq$ "almost P" in avg-case
$\Rightarrow$ very weak NETH closely-related to equivalence conj