Average-Case Hardness of NP from Exponential Worst-Case Hardness Assumptions

Shuichi Hirahara

National Institute of Informatics, Tokyo, Japan

Full version: https://eccc.weizmann.ac.il/report/2021/058/

NII Inter-University Research Institute Corporation / Research Organization of Information and Systems
National Institute of Informatics

@Oxford Warwick complexity meetings

June 10, 2021

Overview

Main Theorem

$$\mathrm{UP} \not\subseteq \mathrm{DTIME}\left(2^{o(n)}\right) \quad \Longrightarrow \quad \mathrm{DistNP} \not\subseteq \mathrm{AvgP}$$

- This was a long-standing open question with good reason.
- Standard proof techniques do not work!
  - Hardness amplification procedure [Viola'05]
  - Black-box reductions [Feigenbaum-Fortnow'93, Bogdanov-Trevisan'06]
- New proof techniques: analyzing **average-case complexity** by **meta-complexity**

Outline

1. Average-Case Complexity
2. Barrier Results
3. Our Results
4. Proof Techniques
5. Open Problems

Motivations of Average-Case Complexity

1. To understand the practical performance of algorithms.

   Example: the Hamiltonian path problem (NP-complete)

   - Cannot be solved in P (unless $\mathrm{P} = \mathrm{NP}$)
   - Can be solved in expected linear time
     on an Erdős–Rényi random graph. [Gurevich & Shelah (1987)]

2. To understand the security of cryptographic primitives.

   ➢ One-way functions cannot exist unless NP is hard on average.

Basics of Average-Case Complextiy

[Levin'86],[Impagliazzo'95],[Ben-David, Chor, Goldreich & Luby '92],[Bogdanov & Trevisan'06],...

- A distributional problem $(L, \mathcal{D})$ $\quad L: \{0,1\}^* \to \{0,1\}$, a decision problem

  $\mathcal{D} = \{\mathcal{D}_n\}_{n \in \mathbb{N}}$, a family of (input) distributions

  Polynomial-time samplable distribution

- $\mathrm{DistNP} = \{(L, \mathcal{D}) \mid L \in \mathrm{NP},\ \mathcal{D} \in \mathrm{PSamp}\}$ an average-case analogue of NP

  Equivalent to *errorless heuristic scheme*

- $(L, \mathcal{D}) \in \mathrm{AvgP}$ average-case polynomial-time

  $\iff$ $\exists$ an algorithm A and $\exists$ a time bound $t: \{0,1\}^* \to \mathbb{N}$ such that

  1. $A(x) = L(x)$ for every x,
  2. $A(x)$ runs in time $\leq t(x)$ for every x, and
  3. $\mathbb{E}_{x \sim \mathcal{D}_n}[t(x)^{\epsilon}] \leq n^{O(1)}$ for some constant $\epsilon > 0$.

Basics of Average-Case Complextiy

[Levin'86],[Impagliazzo'95],[Ben-David, Chor, Goldreich & Luby '92],[Bogdanov & Trevisan'06],…

- A distributional problem $(L, \mathcal{D})$ $\quad L: \{0,1\}^* \to \{0,1\}$, a decision problem

  $\mathcal{D} = \{\mathcal{D}_n\}_{n \in \mathbb{N}}$, a family of (input) distributions

- $\mathrm{DistNP} = \{(L, \mathcal{D}) \mid L \in \mathrm{NP},\ \mathcal{D} \in \mathrm{PSamp}\}$ $\quad$ an average-case analogue of NP

- $(L, \mathcal{D}) \in \mathrm{Avg}_{\mathbf{P}}\mathrm{P}$ $\quad$ P-computable average-case polynomial-time

  $\Longleftrightarrow$ $\exists$ an algorithm A and $\exists$ a time bound $t: \{0,1\}^* \to \mathbb{N}$ such that

  1. $A(x) = L(x)$ for every x,
  2. $A(x)$ runs in time $\le t(x)$ for every x,
  3. $\mathbb{E}_{x \sim \mathcal{D}_n}[t(x)^{\epsilon}] \le n^{O(1)}$ for some constant $\epsilon > 0$, and
  4. t is computable in polynomial time.

Example: $(\mathrm{HamiltonianPath}, \text{Erdős–Rényi}) \in \mathrm{Avg}_{\mathrm{P}}\mathrm{P} \subseteq \mathrm{AvgP}$

Hamiltonian Path

- Let $G(n,p)$ denote the n-vertex Erdős–Rényi random graph with edge probability p.

Theorem [Alon & Krivelevich 2020]

For every $p \geq \frac{1}{o(\sqrt{n})}$, $\quad (\mathrm{HamiltonianPath}, G(n,p)) \in \mathrm{AvgP}.$

Proposition

For every $p \geq \frac{1}{O(\log n)}$, $\quad (\mathrm{HamiltonianPath}, G(n,p)) \in \mathrm{Avg_P P}.$

Big and Frontier Open Questions

Big Open Question

$$\mathrm{NP} \neq \mathrm{P} \overset{?}{\Longrightarrow} \mathrm{DistNP} \not\subseteq \mathrm{AvgP}$$

- Equivalently: Can we rule out Heuristica? [Impagliazzo'95]
  (a world where NP is hard in the worst case but easy on average)

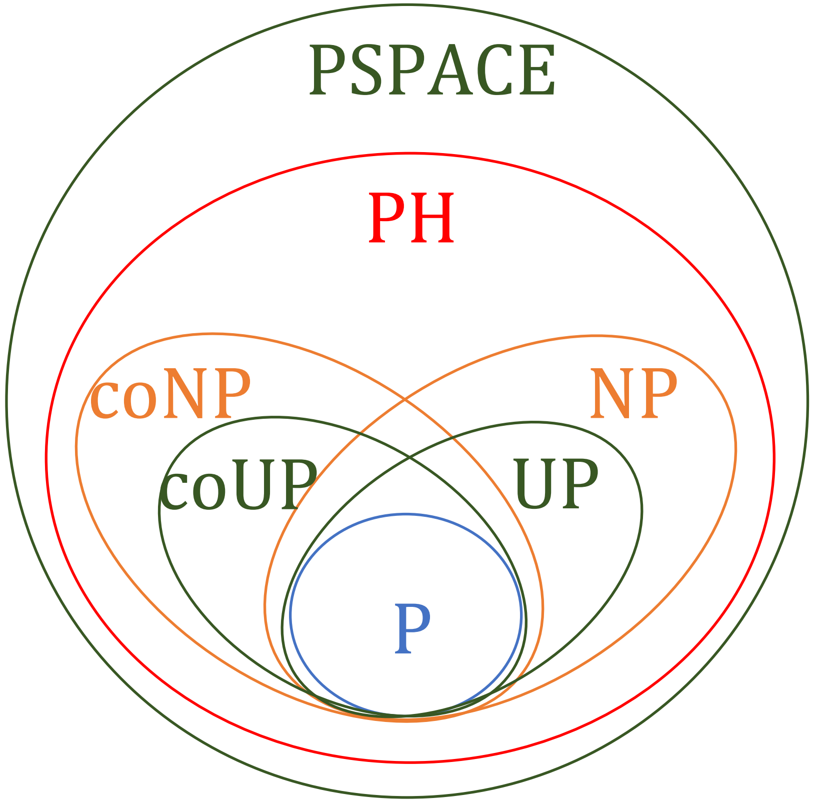
Frontier Question

$$\mathrm{UP} \not\subseteq \mathrm{DTIME}\left(2^{o(n)}\right) \overset{?}{\Longrightarrow} \mathrm{DistPH} \not\subseteq \mathrm{AvgP}$$

- Difficulty: Any proof must bypass **three barriers!**

(1) "Impossibility" of hardness amplification, (2) limits of black-box reductions, and (3) relativization barriers

Complexity Classes



PSPACE : polynomial space

PH : polynomial(-time) hierarchy

NP : non-deterministic polynomial-time

UP : unambiguous polynomial-time
(solvable by a non-deterministic polynomial-time machine with at most one accepting path for each input.)

P : polynomial time

[Ko'85, Grollmann & Selman'88]

$\mathrm{UP} \neq \mathrm{P} \iff$ There is a one-to-one one-way function that is hard to invert in the worst case.

Outline

1. Average-Case Complexity
2. Barrier Results
3. Our Results
4. Proof Techniques
5. Open Problems

(Worst-Case) Hardness Amplification

- A general proof technique that shows a worst-case-to-average-case connection:

  A worst-case hardness amplification procedure $\mathrm{Amp}^{(\cdot)}$ maps $f\colon\{0,1\}^n \to \{0,1\}$ to $\mathrm{Amp}^f\colon\{0,1\}^m \to \{0,1\}$ and satisfies

  "f is worst-case hard $\Longrightarrow$ Amp^f is average-case hard"

- There is a PSPACE-computable $\mathrm{Amp}^{(\cdot)}$. (e.g., [Sudan-Trevisan-Vadhan'01])

- In particular, $\mathrm{PSPACE} \neq \mathrm{P} \Longleftrightarrow \mathrm{Dist}(\mathrm{PSPACE}) \not\subseteq \mathrm{AvgP}$ [Kobler-Schuler'04]

“Impossibility” of Hardness Amplification

[Viola’05]

- Can we prove “$\mathrm{UP} \not\subseteq \mathrm{DTIME}\left(2^{0.99n}\right) \Longrightarrow \mathrm{DistPH} \not\subseteq \mathrm{AvgP}$” by constructing $\mathrm{Amp}^f \in \mathrm{PH}^f$?

No! (or at least very difficult) [Viola’05]

Theorem [Viola (CC’05)]

There is no Amp^f computable in PH^f

(if the relationship between f and Amp^f is proved by black-box reductions)

Theorem [Viola (CCC’05)]

If $\exists\ \mathrm{Amp}^f \in \mathrm{PH}^f$, then $\mathrm{P} \neq \mathrm{NP}$.

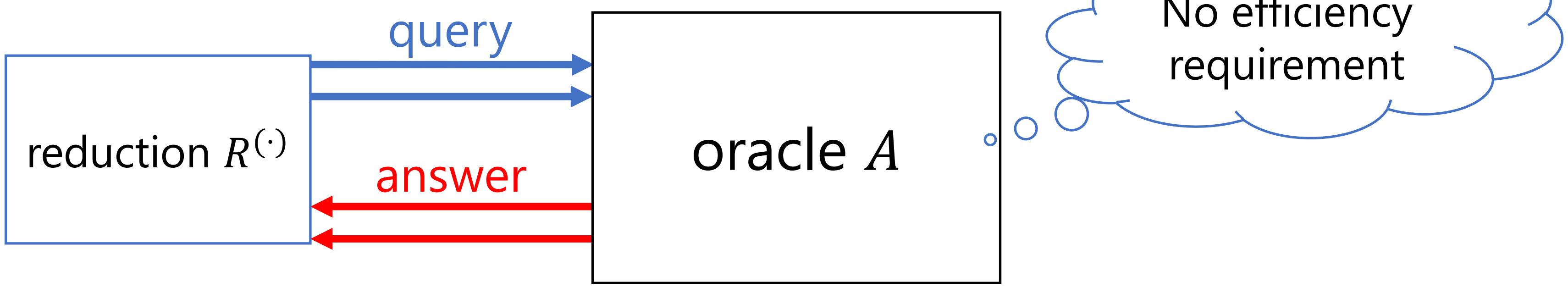
(The property of Amp^f: $f \notin \mathrm{SIZE}\left(2^{0.99n}\right) \Longrightarrow \mathrm{Amp}^f \notin \mathrm{HeurSIZE}\left(n^{O(1)}\right)$)

(Black-Box) Reductions

Theorems:

- $\mathrm{GapSVP} \notin \mathrm{BPP} \Longrightarrow \mathrm{DistNP} \not\subseteq \mathrm{HeurBPP}$ [Ajtai'96,...]
- $\mathrm{SZK} \neq \mathrm{P} \Longrightarrow \mathrm{DistNP} \not\subseteq \mathrm{AvgP}$ [Ostrovsky'91,Hastad-Impagliazzo-Levin-Luby'99,...,H.'18]
- $\mathrm{NP} \not\subseteq \mathrm{DTIME}\left(2^{O(n)}\right) \Longrightarrow \mathrm{DistNP} \not\subseteq \mathrm{AvgP}$ [Ben-David, Chor, Goldreich & Luby '92]

➢ These are proved by black-box reductions:



$\forall L \in \mathrm{SZK}$, a reduction R^A solves L for any oracle A that solves some $(L', \mathcal{D}) \in \mathrm{DistNP}$.

Limits of Black-Box Reductions

➢ Can we use a (black-box) reduction technique to prove "$\mathrm{UP} \not\subseteq \mathrm{DTIME}\left(2^{o(n)}\right) \Longrightarrow \mathrm{DistNP} \not\subseteq \mathrm{AvgP}$"?

No!

Theorem [Feigenbaum & Fortnow'93, Bogdanov & Trevisan'06]

There is no nonadaptive black-box reduction showing "$\mathrm{UP} \not\subseteq \mathrm{DTIME}\left(2^{o(n)}\right) \Longrightarrow \mathrm{DistNP} \not\subseteq \mathrm{AvgP}$"
unless $\mathrm{UP} \subseteq \mathrm{coNTIME}\left(2^{o(n)}\right)/2^{o(n)}$.

➢ We need to use either non-black-box or adaptive reductions!

Relativization Barriers

Theorem [Impagliazzo'11]

There is an oracle A such that $\mathrm{UP}^A \not\subseteq \mathrm{DTIME}^A\left(2^{n^{0.1}}\right)$ and $\mathrm{DistNP}^A \subseteq \mathrm{AvgP}^A$.

- A relativizing proof technique cannot achieve the time bound of $2^{n^{0.1}}(\ll 2^{o(n)})$.
- Remark: Our proof is non-relativizing because
  a result of [Buhrman, Fortnow, Pavan'05] does not seem to relativize.

Outline

1. Average-Case Complexity
2. Barrier Results
3. Our Results
4. Proof Techniques
5. Open Problems

Our Results

Any proof of (1) must *overcome* the barrier results of [Viola] & [Bogdanov-Trevisan].

Main Theorems

This rules out a variant of Heuristica

(1) $\mathrm{UP} \not\subseteq \mathrm{DTIME}\left(2^{O(n/\log n)}\right) \implies \mathrm{DistNP} \not\subseteq \mathrm{AvgP}$

(2) $\mathrm{PH} \not\subseteq \mathrm{DTIME}\left(2^{O(n/\log n)}\right) \implies \mathrm{DistPH} \not\subseteq \mathrm{AvgP}$

(3) $\mathrm{NP} \not\subseteq \mathrm{DTIME}\left(2^{O(n/\log n)}\right) \implies \mathrm{DistNP} \not\subseteq \mathrm{Avg_P P}$

P-computable average-case polynomial-time

- (1) and (2) resolve the frontier open question.
- We also prove that $\mathrm{DistPH} \not\subseteq \mathrm{Avg_P P} \Leftrightarrow \mathrm{DistPH} \not\subseteq \mathrm{AvgP}$.

Our Results

Inverting a *size-verifiable* one-way function in the worst-case

Main Theorems (Stronge

The hard distribution is the uniform distribution $\mathcal{U}$ or the tally distribution $\mathcal{T}$.

every constant $\delta > 0$ and $c \in \mathbb{N}$,

(1) $\mathrm{NTIME_{sv}}\left(2^{n^{1-\delta}}\right) \not\subseteq \mathrm{DTIME}\left(2^{O(n/\log n)}\right) \implies \mathrm{coNP} \times \{\mathcal{U}, \mathcal{T}\} \not\subseteq \mathrm{Avg}^{1}_{1-n^{-c}}\mathrm{P}$

(2) $\mathrm{PHTIME}\left(2^{n^{1-\delta}}\right) \not\subseteq \mathrm{DTIME}\left(2^{O(n/\log n)}\right) \implies \mathrm{PH} \times \{\mathcal{U}, \mathcal{T}\} \not\subseteq \mathrm{Avg}^{1}_{1-n^{-c}}\mathrm{P}$

(3) $\mathrm{NTIME}\left(2^{n^{1-\delta}}\right) \not\subseteq \mathrm{DTIME}\left(2^{O(n/\log n)}\right) \implies \mathrm{NP} \times \{\mathcal{U}, \mathcal{T}\} \not\subseteq \mathrm{Avg_P P}$

$2^{n^{1-\delta}}$-time version of NP

One-sided-error heuristics with success probability n^{-c}.

n is the input length.

A candidate that witnesses $\mathrm{NP} \not\subseteq \mathrm{DTIME}\left(2^{o(n)}\right)$

- 3SAT is not a candidate: $3\mathrm{SAT} \in \mathrm{NP} \cap \mathrm{DTIME}\left(2^{O(n/\log n)}\right)$.

  An m-clause 3CNF on $O(m)$ variables is encoded by $n = O(m \log m)$ bits and can be solved in time $2^{O(m)} = 2^{O(n/\log n)}$.

- DNF-MCSP is an NP-complete problem conjectured to be outside $\mathrm{DTIME}\left(2^{o(n)}\right)$.

Corollary (of the Main Theorems)

$$\text{DNF-MCSP} \notin \mathrm{DTIME}\left(2^{O(n/\log n)}\right) \Longrightarrow \mathrm{DistNP} \not\subseteq \mathrm{Avg_P P} \ \ \& \ \ \mathrm{DistPH} \not\subseteq \mathrm{AvgP}.$$

- This is the first result connecting average-case hardness of NP and worst-case hardness of NP-complete problems.

Minimum Circuit Size Problem (MCSP)

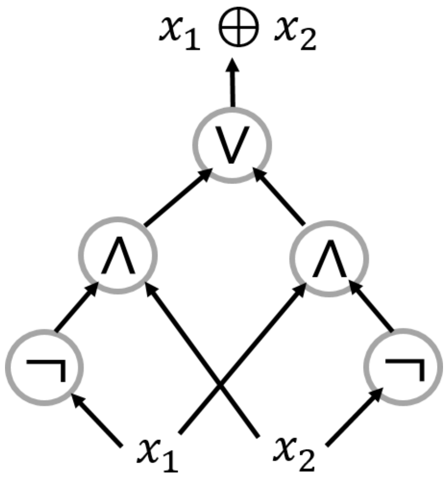
[Kabanets & Cai '00]

Input

- The truth table of a Boolean function $f: \{0,1\}^n \to \{0,1\}$
- A size parameter $s \in \mathbb{N}$

Output

Is there a circuit of size $\leq s$ computing f.



Example $\mathrm{truthtable}(\oplus_2) = 0110$ $\mathrm{size}(\oplus_2) = 3$

➢ MCSP is a *meta-computational* problem.

MCSP = "the problem of computing the circuit complexity of f"

Fact: MCSP ∈ NP

Open: NP-hardness of MCSP

Minimum DNF Size Problem (DNF-MCSP)

Input

- The truth table of a Boolean function $f : \{0,1\}^n \to \{0,1\}$
- A size parameter $s \in \mathbb{N}$

Output

Is there a DNF formula of size $\leq s$ computing f.

$x_1 \oplus x_2 = (x_1 \wedge \neg x_2) \vee (\neg x_1 \wedge x_2)$

Example $\quad \mathrm{truthtable}(\oplus_2) = 0110 \qquad \mathrm{DNFsize}(\oplus_2) = 4$

Theorem [Masek'79]: DNF-MCSP is NP-complete.

Theorem [H.-Oliveira-Santhanam'18]: $(\mathrm{DNF} \circ \mathrm{XOR})$-MCSP is NP-complete.

Theorem [Ilango'20]: AC^0 formula-MCSP is NP-complete.

- The fastest algorithm is an exhaustive search running in time $2^{O(N)}$ on input length $N = 2^n$.
- It is reasonable to conjecture that $\mathcal{C}$-MCSP $\notin \mathrm{DTIME}\left(2^{o(N)}\right)$.

Minimum DNF Size Problem (DNF-MCSP)

Corollary (of the Main Theorems)

$$\mathcal{C}\text{-MCSP} \notin \mathrm{DTIME}\left(2^{o(N/\log N)}\right) \Longrightarrow \mathrm{DistNP} \not\subseteq \mathrm{Avg_P P} \text{ and } \mathrm{DistPH} \not\subseteq \mathrm{AvgP}.$$

$x_1 \oplus x_2 = (x_1 \wedge \neg x_2) \vee (\neg x_1 \wedge x_2)$

Example $\mathrm{truthtable}(\oplus_2) = 0110$ $\mathrm{DNFsize}(\oplus_2) = 4$

Theorem [Masek'79]: DNF-MCSP is NP-complete.

Theorem [H.-Oliveira-Santhanam'18]: $(\mathrm{DNF} \circ \mathrm{XOR})$-MCSP is NP-complete.

Theorem [Ilango'20]: AC^0 formula-MCSP is NP-complete.

- The fastest algorithm is an exhaustive search running in time $2^{O(N)}$ on input length $N = 2^n$.
- It is reasonable to conjecture that $\mathcal{C}\text{-MCSP} \notin \mathrm{DTIME}\left(2^{o(N)}\right)$.

Outline

1. Average-Case Complexity
2. Barrier Results
3. Our Results
4. Proof Techniques
5. Open Problems

Meta-Complexity – Complexity of Complexity

- Examples of meta-computational problems: $\mathrm{MCSP}, \mathrm{MKTP}, \mathrm{MINKT}, \ldots$

MINKT [Ko'91] = "Compute the time-bounded Kolmogorov complexity"

- t-time-bounded Kolmogorov complexity of x

$$\mathrm{K}^t(x) := (\text{the length of a shortest program that prints } x \text{ in } t \text{ steps})$$

- $\mathrm{MINKT} = \{(x, 1^t, 1^s) \mid \mathrm{K}^t(x) \leq s\}.$

Meta-Complexity – Complexity of Complexity

- Examples of meta-computational problems: $\mathrm{MCSP}, \mathrm{MKTP}, \mathrm{MINKT}, \ldots$

MINKT^{A} [Ko'91] = "Compute the A-oracle time-bounded Kolmogorov complexity"

- A-oracle t-time-bounded Kolmogorov complexity of x

  $\mathrm{K}^{t,A}(x) :=$ (the length of a shortest program M^{A} that prints x in t steps)

- $\mathrm{MINKT}^{A} = \left\{(x, 1^{t}, 1^{s}) \mid \mathrm{K}^{t,A}(x) \leq s\right\}.$

Remark: In general, we may have $A \not\leq_{m}^{p} \mathrm{MINKT}^{A}$.

It is easy to see $\mathrm{MINKT}^{A} \in \mathrm{NP}^{A}$.

Average-Case Complexity = Meta-Complexity

Theorem [H. (FOCS'20)]

$$\mathrm{DistPH} \subseteq \mathrm{AvgP} \quad \Longleftrightarrow \quad \mathrm{GapMINKT}^{\mathrm{PH}} \in \mathrm{P}$$

For every $A \in \mathrm{PH}$, $\mathrm{GapMINKT}^{A} \in \mathrm{P}$

- $\mathrm{GapMINKT}^{A}$: an $O(\log n)$-additive approximation version of MINKT^{A}.
- **Corollary:** A new technique of analyzing **average-case complexity** by **meta-complexity.**

Average-Case Complexity

Worst-Case Meta-Complexitry

$\mathrm{DistPH} \subseteq \mathrm{Avg}^{1}_{1-1/\mathrm{poly}(n)}\mathrm{P}$ $\xRightarrow{\text{[H. FOCS'18, CCC'20]}}$ $\mathrm{Gap}(\mathrm{K}^{\mathrm{PH}} \text{ vs } \mathrm{K}) \in \mathrm{P}$

obvious

Easier to analyze worst-case complexity!

Corollary
average-case hardness amplification for PH

$\mathrm{DistPH} \subseteq \mathrm{AvgP}$ $\xLeftarrow{\text{[H. ITCS'20, STOC'20]}}$ $\mathrm{GapMINKT}^{\mathrm{PH}} \in \mathrm{P}$

Theorem [H. STOC'21]

(2') $\mathrm{NP} \not\subseteq \mathrm{DTIME}\left(2^{O(n/\log n)}\right) \Longrightarrow \mathrm{DistPH} \not\subseteq \mathrm{AvgP}$

Average-Case Complexity

Worst-Case Meta-Complexitry

$\mathrm{DistPH} \subseteq \mathrm{AvgP}$ $\Longrightarrow$ [H. FOCS'18, CCC'20] $\mathrm{GapMINKT}^{\mathrm{NP}} \in \mathrm{P}$

$\Downarrow$ **Goal**

$\Downarrow$ [H. STOC'21] based on [H. ITCS'20, STOC'20]

$\mathrm{NP} \subseteq \mathrm{DTIME}\left(2^{O(n/\log n)}\right)$ $\Longleftarrow$ [H. STOC'21] $\forall L \in \mathrm{NP}$ has a *universal heuristic scheme*.

Universal Heuristic Scheme — A key notion in this work

➢ A universal heuristic scheme is "universal" in the following sense.

Proposition (universality of universal heuristic schemes)

Assume $\mathrm{DistNP} \subseteq \mathrm{AvgP}$.

For every $L: \{0,1\}^* \to \{0,1\}$, the following are equivalent.

1. There is a universal heuristic scheme for L.
2. $\{L\} \times \mathrm{PSamp} \subseteq \mathrm{Avg_P P}$.

The notion of P-computable average-case poly-time appears naturally!

The Definition of Universal Heuristic Scheme

- Computational Depth [Antunes, Fortnow, van Melkebeek, Vinodchandran'06]

$$\mathrm{cd}^t(x) \coloneqq \mathrm{K}^t(x) - \mathrm{K}^\infty(x)$$

- (t, s)-Time-Bounded Computational Depth

$$\mathrm{cd}^{t,s}(x) \coloneqq \mathrm{K}^t(x) - \mathrm{K}^s(x)$$

- An algorithm A is called a <u>universal heuristic scheme</u> for L if for some polynomial p,

(Simplified, weak definition)

1. $A(x, t) = L(x)$ and
2. $A(x, t)$ halts in time $2^{O\left(\mathrm{cd}^{t,p(t)}(x) + \log t\right)}$ for all large $t \in \mathbb{N}$.

The Definition of Universal Heuristic Scheme

- Computational Depth [Antunes, Fortnow, van Melkebeek, Vinodchandran'06]

$$\mathrm{cd}^t(x) := \mathrm{K}^t(x) - \mathrm{K}^\infty(x)$$

- (t, s)-Time-Bounded Computational Depth

$$\mathrm{cd}^{t,s}(x) := \mathrm{K}^t(x) - \mathrm{K}^s(x)$$

- A pair (C, S) of algorithms is called a <u>universal heuristic scheme</u> for L if for some polynomial p, for every $t \geq p(n)$ and every $x \in \{0,1\}^n$,
  1. $\mathrm{cd}^{t,p(t)}(x) \leq k \implies C(x,t,k) = 1$
  2. $C(x,t,k) = 1 \implies S(x,t,k) = L(x)$
  3. C runs in time $\mathrm{poly}(t)$ and S runs in time $\mathrm{poly}(t, 2^k)$.

C: checker, S: solver

Theorem [H. STOC'21]

(2') $\mathrm{NP} \not\subseteq \mathrm{DTIME}\left(2^{O(n/\log n)}\right) \Longrightarrow \mathrm{DistPH} \not\subseteq \mathrm{AvgP}$

Average-Case Complexity

Worst-Case Meta-Complexitry

$\mathrm{DistPH} \subseteq \mathrm{AvgP}$ $\xRightarrow{\text{[H. FOCS'18, CCC'20]}}$ $\mathrm{GapMINKT}^{\mathrm{NP}} \in \mathrm{P}$

Goal

[H. STOC'21]

based on [H. ITCS'20, STOC'20]

$\mathrm{NP} \subseteq \mathrm{DTIME}\left(2^{O(n/\log n)}\right)$ $\xLeftarrow{\text{[H. STOC'21]}}$ $\forall\, L \in \mathrm{NP}$ has

a *universal heuristic scheme.*

Easy to prove

(Next slide)

Fast Algorithms from Universal Heuristic Schemes

Lemma

If there is some universal heuristic scheme A for L, then
$L \in \mathrm{DTIME}\left(2^{O(n/\log n)}\right)$.

Proof Idea: Find a parameter t so that the input x is "computationally shallow" (i.e., $\mathrm{cd}^{t,p(t)}(x) = O(n/\log n)$).

Proof: Consider the following telescoping sum for a parameter $I = \epsilon \log n$ ($\epsilon > 0$, constant):

$$\mathrm{cd}^{t,p(t)}(x) + \mathrm{cd}^{p(t),p\circ p(t)}(x) + \cdots + \mathrm{cd}^{p^{I-1}(t),p^{I}(t)}(x) = \mathrm{K}^{t}(x) - \mathrm{K}^{p^{I}(t)}(x) \le n + O(1)$$

$$\Longrightarrow \text{ for some } i \in \{1,2,\dots,I\}, \text{ we have } \mathrm{cd}^{p^{i-1}(t),p^{i}(t)}(x) \le \frac{n+O(1)}{I} = O\left(\frac{n}{\log n}\right).$$

Algorithm B:

Run $A(x,t), A(x,p(t)), A(x,p^2(t)), \dots, A(x,p^{I-1}(t))$ in parallel.
Take the first one that halts, and output what it outputs.

Correctness: $B(x) = L(x)$ for every input x.

$$(\text{The running time of } B) \lesssim \min_i\left\{2^{O\left(\mathrm{cd}^{p^{i-1}(t),p^{i}(t)}(x)+\log p^{i}(t)\right)}\right\} \le 2^{O(n/\log n)}$$

$$\left(p^{I}(t) \lesssim n^{c^{I}} \le 2^{O(n/\log n)} \text{ for } I = \epsilon \log n\right)$$

A universal heuristic scheme A for L: $\exists\, p(t) = t^{O(1)}$,

1. $A(x,t) = L(x)$
2. $A(x,t)$ runs in time $2^{O(\mathrm{cd}^{t,p(t)}(x)+\log t)}$.

Theorem [H. STOC'21]

$$\text{(2')}\quad \mathrm{NP} \not\subseteq \mathrm{DTIME}\left(2^{O(n/\log n)}\right) \Longrightarrow \mathrm{DistPH} \not\subseteq \mathrm{AvgP}$$

Average-Case Complexity

Worst-Case Meta-Complexitry

[H. FOCS'18, CCC'20]

$\mathrm{DistPH} \subseteq \mathrm{AvgP} \Longrightarrow \mathrm{GapMINKT}^{\mathrm{NP}} \in \mathrm{P}$

G

- Direct product generator [H. STOC'20]
- Weak symmetry of information [H. STOC'21]

[H. STOC'21]

based on [H. ITCS'20, STOC'20]

$\forall L \in \mathrm{NP}$ has
a *universal heuristic scheme.*

[H. STOC'21]

$\mathrm{NP} \subseteq \mathrm{DTIME}\left(2^{O(n/\log n)}\right)$

Constructing Universal Heuristics

Lemma [H. STOC'21]

$\mathrm{GapMINKT}^{\mathrm{NP}} \in \mathrm{P} \implies \forall L \in \mathrm{NP}$ admits a universal heuristic scheme.

[H. FOCS'20]

$$\mathrm{GapMINKT}^{\mathrm{NP}} \in \mathrm{P} \Leftrightarrow \mathrm{Gap}\left(\mathrm{K}^{\mathrm{NP}} \text{ vs } \mathrm{K}\right) \in \mathrm{P}$$

A harder problem,
but equivalent.

The $\mathrm{Gap}\left(\mathrm{K}^{\mathrm{NP}} \text{ vs } \mathrm{K}\right)$ Problem [H. CCC'20]

$$\Pi_{\mathrm{Yes}} = \left\{(x, 1^t, 1^s) \mid \mathrm{K}^{t,\mathrm{NP}}(x) \le s\right\}.$$
$$\Pi_{\mathrm{No}} = \left\{(x, 1^t, 1^s) \mid \mathrm{K}^{p(|x|+t)}(x) > s + \log p(|x| + t)\right\}.$$

(p: some polynomial)

Lemma [H. STOC'21]

$\mathrm{Gap}(\mathrm{K}^{\mathrm{NP}} \text{ vs } \mathrm{K}) \in \mathrm{P} \implies \forall L \in \mathrm{NP}$ admits a universal heuristic scheme.

- Main Tool: *k-wise direct product generator* [H. STOC'20]

$$\mathrm{DP}_k(y; z) = \left(z_1, \dots, z_k, \mathrm{Enc}(y)_{z_1}, \dots, \mathrm{Enc}(y)_{z_k}\right)$$

A pseudorandom generator construction based on a "hard" truth table y

$\mathrm{Enc}(\cdot)$: an arbitrary list-decodable error correcting code (e.g., Hadamard code)

$\mathrm{DP}_k(y; Z) = (Z, Zy)$, where $Z \in \mathrm{GF}(2)^{k\times n}$ and $y \in \mathrm{GF}(2)^n$ for Hadamard code.

Reconstruction Algorithm $R^{(\cdot)}$ of DP_k:

Given any D that ϵ-distinguishes $\mathrm{DP}_k(y;\cdot)$ from the uniform distribution, there exists an advice string $\alpha \in \{0,1\}^{k+O(\log n)}$ such that $R^D(\alpha) = y$.

Key Point: (The advice complexity of DP_k) $= k + O(\log n)$

Symmetry of Information [Levin-Kolmogorov]

$$\mathrm{K}^{\infty}(x, w) \geq \mathrm{K}^{\infty}(x) + \mathrm{K}^{\infty}(w|x) - O(\log n)$$

Lemma [H. STOC'21]

$\mathrm{Gap}(\mathrm{K}^{\mathrm{NP}} \text{ vs } \mathrm{K}) \in \mathrm{P} \implies \forall L \in \mathrm{NP}$ admits a universal heuristic scheme.

- Let y_x be the lexicographically first certificate for $x \in L$, if any.
  - Want to distinguish $\mathrm{DP}_k(y_x; z)$ from $w \sim \{0,1\}^{|z|+k}$

$$\mathrm{K}^{2t,\,\mathrm{NP}}\big(x, \mathrm{DP}_k(y_x; z)\big) \leq \mathrm{K}^{t}(x) + |z| + O(\log n)$$

Weak symmetry of information [H. STOC'21]

$$\mathrm{K}^{p(2t)}(x, w) \geq \mathrm{K}^{q(p(2t))}(x) + \underset{\substack{\parallel \\ |z|+k}}{|w|} - O(\log n)$$

with high prob. over $w \sim \{0,1\}^{|z|+k}$

If $k \geq \mathrm{K}^{t}(x) - \mathrm{K}^{q(p(2t))}(x) + O(\log n) = \mathrm{cd}^{t, q\circ p(2t)}(x) + O(\log n)$,

then we get $\underbrace{\mathrm{K}^{p(2t)}(x, w)}_{\Pi_{\mathrm{No}}} \gg \underbrace{\mathrm{K}^{2t,\mathrm{NP}}\big(x, \mathrm{DP}_k(y_x; z)\big)}_{\Pi_{\mathrm{Yes}}}$.

Can be distinguished using $\mathrm{Gap}(\mathrm{K}^{\mathrm{NP}} \text{ vs } \mathrm{K}) \in \mathrm{P}$

Lemma [H. STOC'21]

$\mathrm{Gap}\left(\mathrm{K}^{\mathrm{NP}} \text{ vs } \mathrm{K}\right) \in \mathrm{P} \implies \forall L \in \mathrm{NP}$ admits a universal heuristic scheme.

- Let M be a poly-time algorithm for $\mathrm{Gap}\left(\mathrm{K}^{\mathrm{NP}} \text{ vs } \mathrm{K}\right)$

Randomized algorithm, but can be derandomized using [Buhrman-Fortnow-Pavan'05]

<u>Universal heuristic scheme (C, S) for L</u>

- Input: $x \in \{0,1\}^n, t \in \mathbb{N}, k \in \mathbb{N}$
- Define $D_x(w) \coloneqq M\left(xw, 1^{2t}, 1^s\right)$ for some threshold s.
- Checker C accepts iff $\Pr_w[D_x(w) = 1] \leq \frac{1}{4}$.
- Solver S computes a list $Y \coloneqq \{R^{D_x}(\alpha) \mid \alpha \in \{0,1\}^{k+O(\log n)}\}$ and accepts iff $\exists y \in Y$ is a certificate for $x \in L$.

The size of list $\leq \mathrm{poly}\left(n, 2^k\right)$

Correctness of C: $\mathrm{cd}^{t, q \circ p(2t)}(x) \leq k - O(\log n) \implies \left(xw, 1^{2t}, 1^s\right) \in \Pi_{\mathrm{No}}$ w.h.p. $\implies C$ accepts.

Correctness of S: C accepts $\implies D_x$ distinguishes $\mathrm{DP}_k(y_x; \cdot)$ from $w \implies y_x \in Y$ (if any).

Theorem [H. STOC'21]

$$(2') \quad \mathrm{NP} \not\subseteq \mathrm{DTIME}\left(2^{O(n/\log n)}\right) \Longrightarrow \mathrm{DistPH} \not\subseteq \mathrm{AvgP}$$

Average-Case Complexity

Worst-Case Meta-Complexitry

Direct product generator

[H. FOCS'18, CCC'20]

$\mathrm{DistPH} \subseteq \mathrm{AvgP} \Longrightarrow \mathrm{GapMINKT}^{\mathrm{NP}} \in \mathrm{P}$

- Direct product generator [H. STOC'20]
- Weak symmetry of information [H. STOC'21]

[H. STOC'21]

based on [H. ITCS'20, STOC'20]

$\forall L \in \mathrm{NP}$ has a *universal heuristic scheme.*

[H. STOC'21]

$\mathrm{NP} \subseteq \mathrm{DTIME}\left(2^{O(n/\log n)}\right)$

Easy ("computationally shallow")

How we overcame limits of black-box reductions

Let $p(n)$ be the runtime of AvgP.

$\mathrm{DistPH} \subseteq \mathrm{AvgP}$

[H. FOCS'18, CCC'20]

$\mathrm{GapMINKT}^{\mathrm{NP}} \in \mathrm{P}$

Goal

The algorithm runs in time $2^{O\left(\mathrm{cd}^{t,p'(t)}(x)\right)}$.

[H. STOC'21]

based on [H. ITCS'20, STOC'20]

$\forall L \in \mathrm{NP}$ has a *universal heuristic scheme.*

$\mathrm{NP} \subseteq \mathrm{DTIME}\left(2^{O(n/\log n)}\right)$

[H. STOC'21]

- The reduction is non-black-box because we exploit the efficiency of AvgP.

  i.e., the proof is not subject to the barrier of [Bogdanov & Trevisan'06].

How we overcame [Viola'05]

- One can regard our proof as a "hardness amplification procedure $\mathrm{Amp}^{(\cdot)}$" in a sense, but $\mathrm{Amp}^f : \{0,1\}^* \to \{0,1\}$ must be defined on all input lengths.

$$
\begin{tikzcd}[column sep=huge, row sep=huge]
\mathrm{Amp}^{f} \in \mathrm{AvgP} \arrow[r, Rightarrow, "\text{[H. FOCS'18, CCC'20]}"] \arrow[d, Rightarrow, "\underline{\textbf{Goal}}"] & \mathrm{GapMINKT}^{\mathrm{NP}^{f}} \in \mathrm{P} \arrow[d, Rightarrow, "\substack{\text{[H. STOC'21]} \\ \text{based on [H. ITCS'20, STOC'20]}}"] \\
\mathrm{NP}^{f} \subseteq \mathrm{DTIME}^{f}\left(2^{O(n/\log n)}\right) & \substack{\forall L \in \mathrm{NP}^{f} \text{ has} \\ \text{a \textit{universal heuristic scheme}.}} \arrow[l, Rightarrow, "\text{[H. STOC'21]}"']
\end{tikzcd}
$$

- [Viola'05]'s proof techniques can be applied only when $\mathrm{Amp}^f : \{0,1\}^m \to \{0,1\}$.

(Extending it to $\{0,1\}^*$ would resolve $\mathrm{P} \neq \mathrm{NP}$.)

Proof Ideas for other results

Main Theorems

(1) $\mathrm{UP} \not\subseteq \mathrm{DTIME}\left(2^{O(n/\log n)}\right) \implies \mathrm{DistNP} \not\subseteq \mathrm{AvgP}$

Already explained

(2) $\mathrm{PH} \not\subseteq \mathrm{DTIME}\left(2^{O(n/\log n)}\right) \implies \mathrm{DistPH} \not\subseteq \mathrm{AvgP}$

(3) $\mathrm{NP} \not\subseteq \mathrm{DTIME}\left(2^{O(n/\log n)}\right) \implies \mathrm{DistNP} \not\subseteq \mathrm{Avg_P P}$

Proof Ideas for other results

Main Lemmas

"Algorithmic language compression" that generalizes [H. FOCS'18, CCC'20]

(1) $\forall L \in \mathrm{UP}$ has universal heuristic schemes if $\mathrm{DistNP} \subseteq \mathrm{AvgP}$.

(2) $\forall L \in \mathrm{PH}$ has universal heuristic schemes if $\mathrm{DistPH} \subseteq \mathrm{AvgP}$.

(3) $\forall L \in \mathrm{NP}$ has universal heuristic schemes if $\mathrm{DistNP} \subseteq \mathrm{Avg_P P}$.

"Universality" of universal heuristic schemes
Based on the ideas of [Antunes & Fortnow '09]

Why UP?

<u>Algorithmic language compression</u> [H. STOC'21]

If $(L_1, \mathcal{U}) \in \mathrm{AvgP}$, then $(\Pi_{\mathrm{Yes}}, \Pi_{\mathrm{No}}) \in \text{promise-P}$, where

$$\Pi_{\mathrm{Yes}} := L_0, \Pi_{\mathrm{No}} := \left\{x \middle| \mathrm{K}^{p(t)}(x) \geq \log \#L_0 + \log p(t)\right\}$$

- Consider a language $L \in \mathrm{UP}$ and a verifier V for L.

$$x \in L \Longrightarrow \exists!\, y, V(x,y) = 1$$
$$x \notin L \Longrightarrow \forall y, V(x,y) = 0$$

- A hard distributional problem $(L_1, \mathcal{U})$ in DistNP is (roughly) as follows.

$$L_0 := \{(x\ \mathrm{DP}_k(y;z), 1^t, 1^s) | \mathrm{K}^t(x) \leq s, V(x,y) = 1\}$$

$\Downarrow$ "Algorithmic language compression"

$$L_1 := \{(\mathrm{DP}_\ell(w;z'), 1^t, 1^s) | (w, 1^t, 1^s) \in L_0\}$$
$$:= \{(\mathrm{DP}_\ell(x\ \mathrm{DP}_k(y;z);z'), 1^t, 1^s) | \mathrm{K}^t(x) \leq s, V(x,y) = 1\} \in \mathrm{NP}$$

- We exploit the property that

$$\#\{(x,y) | \mathrm{K}^t(x) \leq s, V(x,y) = 1\} \leq 2^{s+1}.$$

[Valiant-Vazilani'86]
isn't sufficient.

Summary and Open Questions

- Meta-complexity is a powerful tool to analyze average-case complexity.
- A lot of interesting questions remain open:
  - Can we prove $\mathrm{NP} \not\subseteq \mathrm{DTIME}\left(2^{o(n)}\right) \Longrightarrow \mathrm{DistNP} \not\subseteq \mathrm{AvgP}$?
  - Does the exponential-time hypothesis (ETH) imply $\mathrm{DistPH} \not\subseteq \mathrm{AvgP}$?
  - Can we prove $\mathrm{PH} \not\subseteq \text{io-DTIME}\left(2^{o(n)}\right) \Longrightarrow \mathrm{DistPH} \not\subseteq \text{io-AvgP}$?

    Viola's barrier comes into play in this setting!
  - Can our results relativize?

Subsequent Work

Theorem [H. and Nanashima]

There exists an oracle A such that

$$\mathrm{DistPH}^A \subseteq \mathrm{AvgP}^A \text{ and } \mathrm{UP}^A \cap \mathrm{coUP}^A \nsubseteq \mathrm{DTIME}\left(2^{n/\omega(\log n)}\right).$$

- Surprisingly, our time bound $2^{O(n/\log n)}$ is nearly optimal for relativizing proof techniques.

Thank you!