Analyzing Average-Case Complexity by Meta-Complexity

Shuichi Hirahara

National Institute of Informatics, Tokyo, Japan

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

National Institute of Informatics

@Simons Institute

Nov 9, 2021

Outline

1. Toward Excluding Heuristica
2. Limits of Black-Box Reductions
3. Our Results, Meta-Complexity, and Proof Techniques

The $\mathbf{P} \neq \mathbf{NP}$ Conjecture and Cryptography

$\mathbf{P} = \mathbf{NP}$	or	$\mathbf{P} \neq \mathbf{NP}$
☺ Any problem in **NP** can be solved efficiently.		☹ There is a problem in **NP** that can't be solved efficiently.
☺ Automated theorem proving can be done efficiently.		☺ There <u>might be</u> a secure cryptosystem (?)
☹ Any public-key cryptosystem can be broken.		
☹ Bitcoin loses its value.		

Using a public-key cryptosystem,
Bitcoin prevents those who do not own a secret key from spending a coin.

Impagliazzo's Five Possible Worlds

[Impagliazzo '95] classified five possible worlds consistent with our current knowledge.

Cryptomania

Minicrypt

Pessiland

Heuristica

$$\left.\begin{array}{l}\text{Cryptomania}\\ \text{Minicrypt}\\ \text{Pessiland}\\ \text{Heuristica}\end{array}\right\} \mathrm{P} \neq \mathrm{NP}$$

Algorithmica

$$\mathrm{P} = \mathrm{NP}$$

Impagliazzo's Five Possible Worlds

[Impagliazzo '95] classified five possible worlds consistent with our current knowledge.

Cryptomania

Minicrypt

Pessiland

Heuristica

$P \neq NP$

☺ Any problem in **NP** can be solved efficiently.
Automated theorem proving is possible.
☹ Impossible to construct a secure cryptosystem.

Algorithmica

$P = NP$

Impagliazzo's Five Possible Worlds

[Impagliazzo '95] classified five possible worlds consistent with our current knowledge.

Cryptomania

∃ public-

em.

Minicrypt

Impossible to construct a public-key cryptosystem.
Possible to construct a secret-key cryptosystem.

∃ secret-key crypto & ∄ public-key crypto

Pessiland

The "worst" possible world (a pessimistic world)
Impossible to construct a secret-key cryptosystem.
NP can't be solved efficiently (on average).

DistNP ⊈ AvgP & ∄ secret-key crypto

("P ≠ NP

Heuristica

A world where heuristics are efficient
There are efficient heuristics that solve **NP** on average.
Impossible to construct a cryptosystem.

$\mathrm{P} \neq \mathrm{NP}$ & $\mathrm{DistNP} \subseteq \mathrm{AvgP}$

("P = NP on average")

Algorithmica

$$\mathrm{P} = \mathrm{NP}$$

Impagliazzo’s Five Possible Worlds

[Impagliazzo ’95] classified five possible worlds consistent with our current knowledge.

Cryptomania

∃ public-key crypto.

Minicrypt

<u>The Ultimate Goal of Complexity Theory</u>

is to decide which world corresponds to our world.

(In particular, we would like to resolve the conjecture that our world is Cryptomania.)

Heuristica

$\mathrm{P} \neq \mathrm{NP}$ & $\mathrm{DistNP} \subseteq \mathrm{AvgP}$

(“$\mathrm{P} = \mathrm{NP}$ on average”)

Algorithmica

$\mathrm{P} = \mathrm{NP}$

Known Facts and Open Questions

$\Rightarrow$: Known facts

$\overset{?}{\dashrightarrow}$: Open questions

Cryptomania

$\exists$ public-key crypto.

$\Downarrow \quad \Uparrow ?$

Minicrypt

$\exists$ secret-key crypto.

$\Downarrow \quad \Uparrow ?$

Pessiland

$\mathrm{DistNP} \not\subseteq \mathrm{AvgP}$

(“$\mathrm{P} \neq \mathrm{NP}$ on average”)

$\Downarrow \quad \Uparrow ?$

Heuristica

$\mathrm{P} \neq \mathrm{NP}$

$\Uparrow ?$

Algorithmica

Toward Public-key Crypto.

⇨ : Known facts

⇢? : Open questions

Cryptomania

∃ public-key crypto.

Minicrypt

Important Open Question
Can we exclude Minicrypt?

∃ secret-key crypto.

Pessiland

Important Open Question
Can we exclude Pessiland?

$\mathrm{DistNP} \not\subseteq \mathrm{AvgP}$

("$\mathrm{P} \neq \mathrm{NP}$ on average")

Heuristica

Important Open Question
Can we exclude Heuristica?

$\mathrm{P} \neq \mathrm{NP}$

Algorithmica

Important Open Question
$\mathrm{P} \neq \mathrm{NP}$ (Can we exclude Algorithmica?)

Proving the four implications

$\Longleftrightarrow$

Our world is Cryptomania!

Proving one implication

$\Longleftrightarrow$

Excluding one world

Limits of Current Proof Techniques

$\Rightarrow$: Known facts

? : Open questions

: Barrier results

Several types of proof techniques are insufficient to resolve the open question.

Cryptomania

$\exists$ public-key crypto.

Minicrypt

$\exists$ secret-key crypto.

Pessiland

$\mathrm{DistNP} \not\subseteq \mathrm{AvgP}$

("$\mathrm{P} \neq \mathrm{NP}$ on average")

Heuristica

$\mathrm{P} \neq \mathrm{NP}$

Algorithmica

Relativization barrier [Baker-Gill-Solovay'75]

Algebrization barrier [Aaronson-Wigderson'09]

Natural proof barrier [Razborov-Rudich'97]

Locality barrier [Chen-H.-Oliveira-Pich-Rajgopal-Santhanam (ITCS'20)]

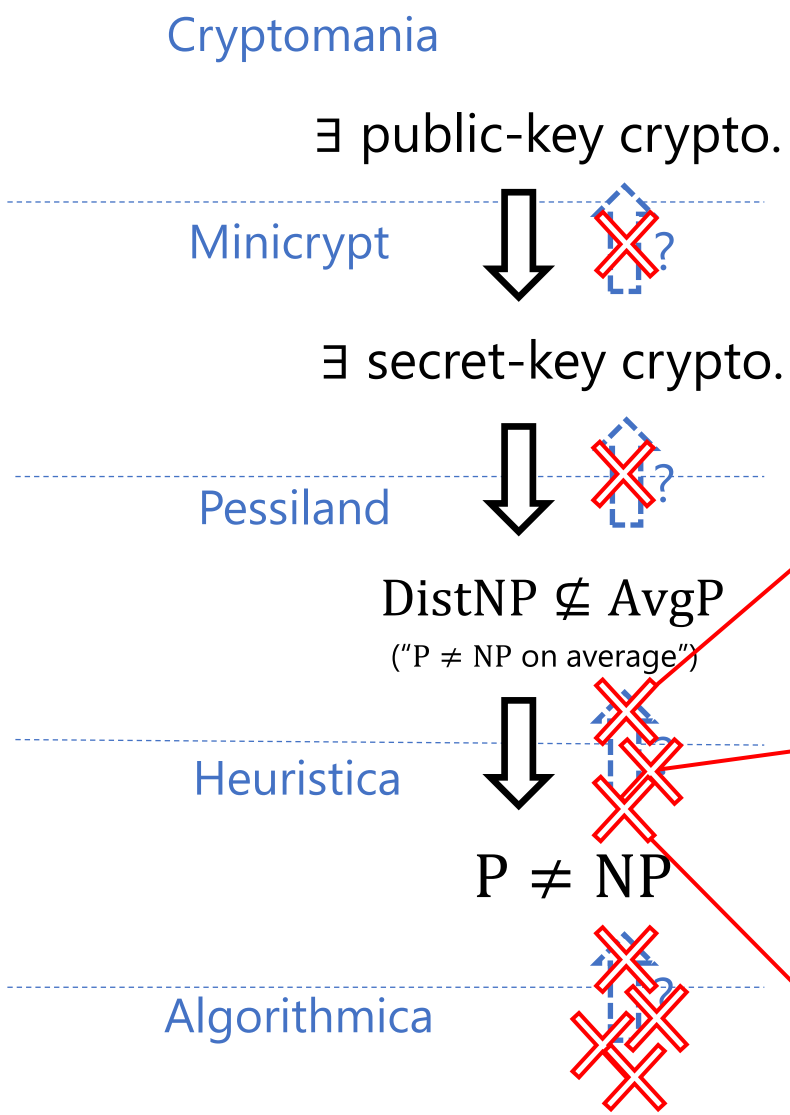
Limits of Current Proof Techniques

: Known facts

: Open questions

: Barrier results

Several types of proof techniques are insufficient to resolve the open question.



Relativization barrier

[Impagliazzo (2011)]

Limits of black-box reductions

[Feigenbaum & Fortnow (1993)]
[Bogdanov & Trevisan (2006)]

"Impossibility" of hardness amplification

[Viola (2005)]

A New Paradigm: Meta-Complexity

$\Rightarrow$: Known facts

$\overset{?}{\Rightarrow}$: Open questions

The **complexity** of problems asking for **complexity**

Cryptomania

∃ public-key crypto.

Minicrypt

∃ secret-key crypto.

Pessiland

DistNP $\not\subseteq$ AvgP

("P ≠ NP on average")

Heuristica

$\mathrm{P} \neq \mathrm{NP}$

Algorithmica

MINKT (Minimum Time-Bounded Kolmogorov Complexity Problem)

The problem of **computing** the minimum program to **compute** x efficiently

MINKT

Overcoming Limits of Black-box Reductions

Cryptomania

$\exists$ public-key crypto.

Minicrypt

$\exists$ secret-key crypto.

Pessiland

$\text{DistNP} \not\subseteq \text{AvgP}$

(“P ≠ NP on average”)

Heuristica

$\text{P} \neq \text{NP}$

Algorithmica

Theorem [H. (FOCS 2018)]
Worst- and **average-case** complexities of MINKT are equivalent.

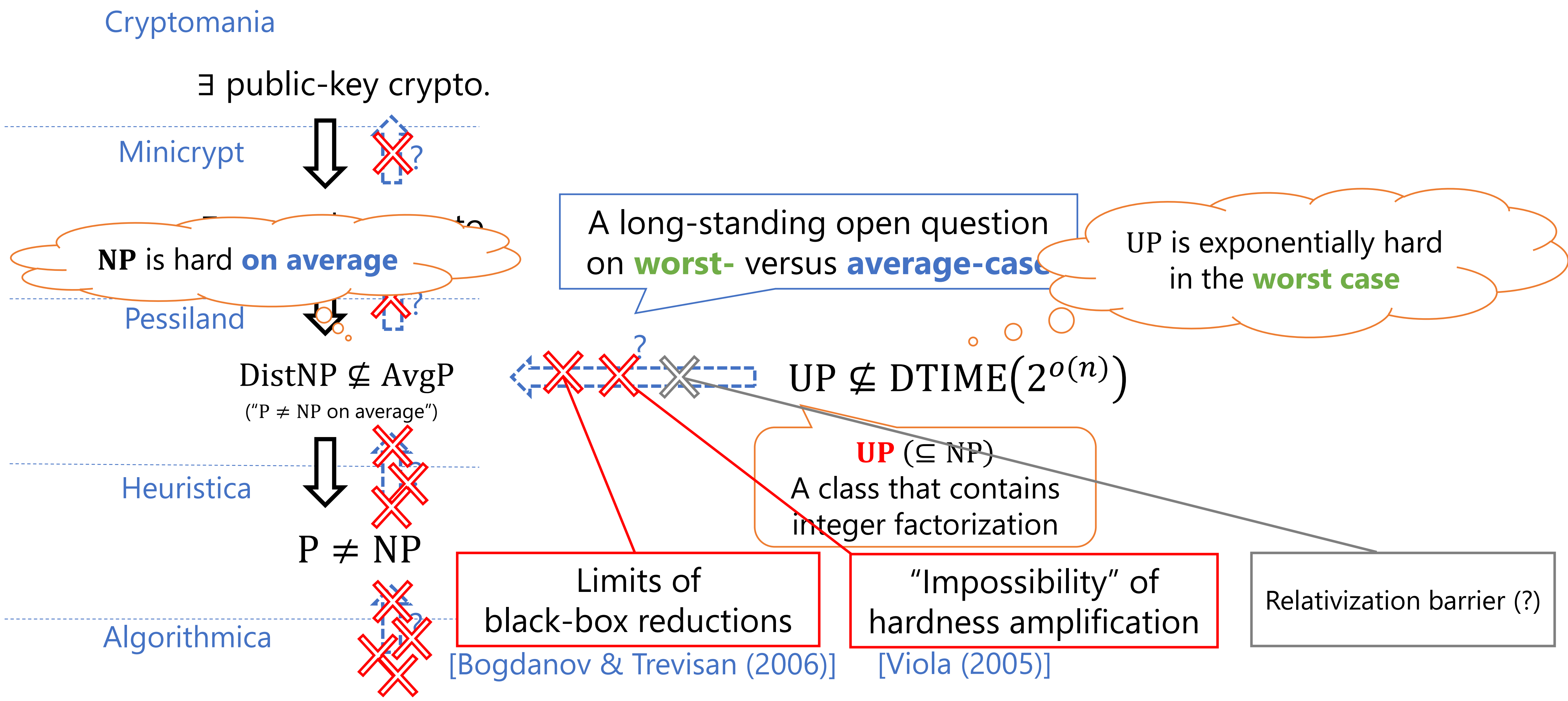
$(\text{MINKT}, \mathcal{U}) \notin \text{AvgP} \Leftrightarrow \text{GapMINKT} \notin \text{P}$

Limits of
black-box reductions

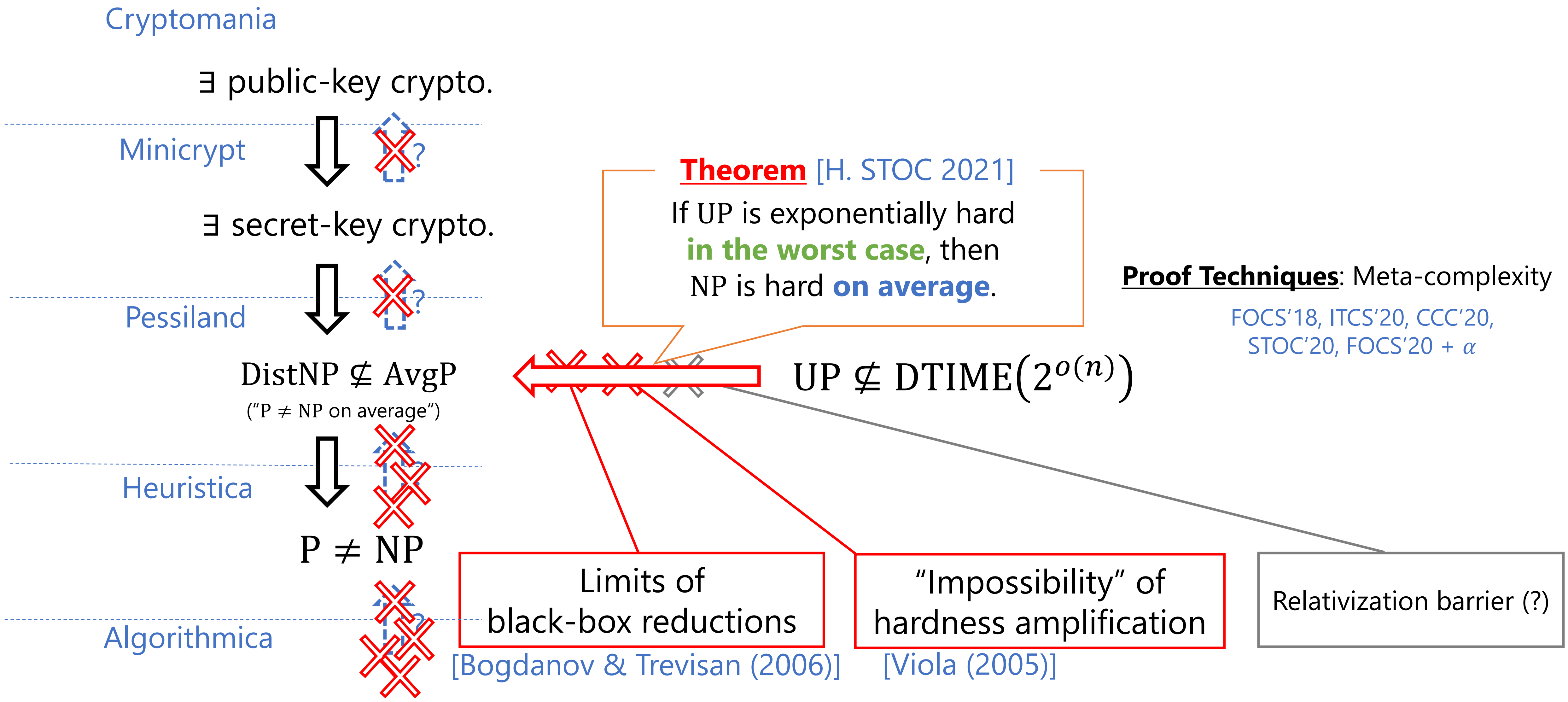
[Bogdanov & Trevisan (2006)]

- Limits: $\text{NP/poly} \cap \text{coNP/poly}$
- Conjecture [Rudich’97]: $\text{GapMINKT} \notin \text{coNP/poly}$
- This is the first result that goes beyond the limits!

A Long-Standing Open Question



Overcoming two barriers simultaneously



Overcoming two barriers simultaneously

Cryptomania

∃ public-key crypto.

Minicrypt

∃ secret-key crypto.

Pessiland

$\mathrm{DistNP} \not\subseteq \mathrm{AvgP}$

(“P ≠ NP on average”)

Heuristica

$\mathrm{P} \neq \mathrm{NP}$

Algorithmica

Theorem [H. STOC 2021]

If UP is exponentially hard **in the worst case**, then NP is hard **on average**.

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

Proof Techniques: Meta-complexity

FOCS’18, ITCS’20, CCC’20, STOC’20, FOCS’20 + α

Limits of black-box reductions

[Bogdanov & Trevisan (2006)]

“Impossibility” of hardness amplification

[Viola (2005)]

Relativization barrier (?)

A New Relativization Barrier

Cryptomania

∃ public-key crypto.

Minicrypt

?

∃ secret-key crypto.

?

Pessiland

DistNP $\not\subseteq$ AvgP

("P ≠ NP on average")

Heuristica

P ≠ NP

?

Algorithmica

Theorem [H. STOC 2021]

If UP is exponentially hard **in the worst case**, then NP is hard **on average**.

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

$\mathrm{UP} \not\subseteq \mathrm{DTIME}\left(2^{o(n/\log n)}\right)$

Proof Techniques: Meta-complexity

FOCS'18, ITCS'20, CCC'20, STOC'20, FOCS'20 + α

Limits of black-box reductions

[Bogdanov & Trevisan (2006)]

"Impossibility" of hardness amplification

[Viola (2005)]

Relativization barrier (?)

Relativization barrier [H. & Nanashima (FOCS'21)]

"Fine-Grained" Five Worlds [Chen-H.-Vafa (ITCS'22)]

Cryptomania

Poly.-time adversary

∃ public-key crypto.

Minicrypt

?

∃ secret-key crypto.

?

Pessiland

DistNP $\not\subseteq$ AvgP

("P ≠ NP on average")

?

Heuristica

P ≠ NP

?

Algorithmica

[H. (STOC'21)]

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

$\mathrm{UP} \not\subseteq \mathrm{DTIME}\left(2^{O(\sqrt{n \log n})}\right)$

[Chen-H.-Vafa (ITCS'22)]

Fine-grained Cryptomania

$\tilde{O}(n \log n)$-time adversary

∃ fine-grained public-key crypto.

Fine-grained Minicrypt

?

∃ fine-grained secret-key crypto.

?

Fine-grained Pessiland

$\mathrm{NTIME}(n) \times \{\mathcal{U}'\} \not\subseteq \mathrm{AvgDTIME}(\tilde{\mathrm{O}}(n))$

(NP is slightly hard on average.)

?

Fine-grained Heuristica

$\mathrm{NTIME}(n) \not\subseteq \mathrm{DTIME}\left(\tilde{\mathrm{O}}(n)\right)$

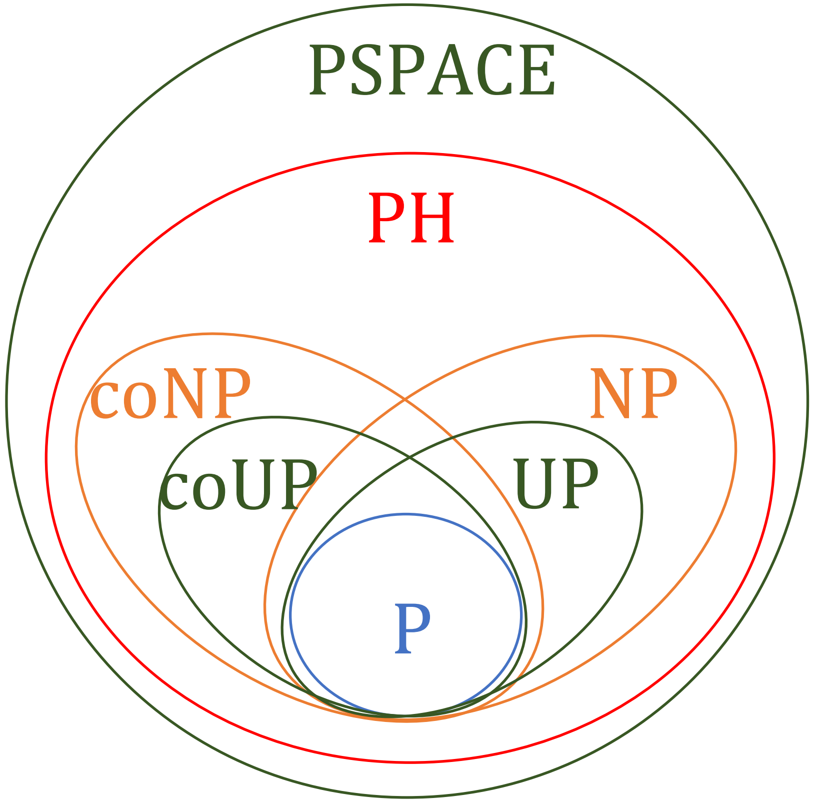
?

Fine-grained Algorithmica

Outline

1. Toward Excluding Heuristica
2. Limits of Black-Box Reductions
3. Our Results, Meta-Complexity, and Proof Techniques

Complexity Classes



[Ko'85, Grollmann & Selman'88]

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

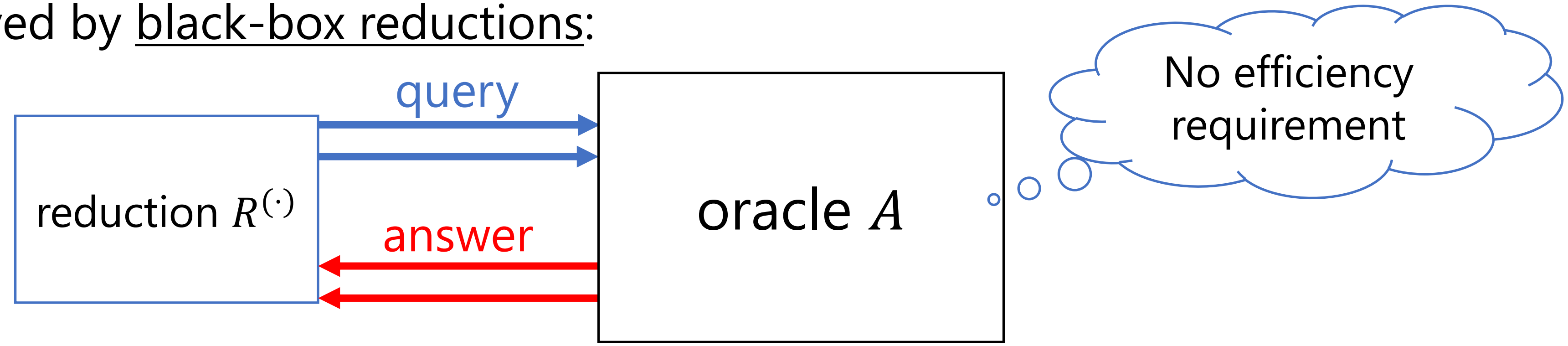
$\mathrm{UP} \neq \mathrm{P} \iff$ There is a one-to-one one-way function that is hard to invert in the worst case.

(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:



$\forall L \in \mathrm{SZK}$, there is a reduction $R^{(\cdot)}$ such that for any oracle A that solves some $(L', \mathcal{D}) \in \mathrm{DistNP}$, $R^A(x)$ outputs the correct answer $L(x)$ for every input x.

A "non-black-box" reduction $\Leftrightarrow$ The reduction might fail if the oracle is inefficient.

Limits of Black-Box Reductions

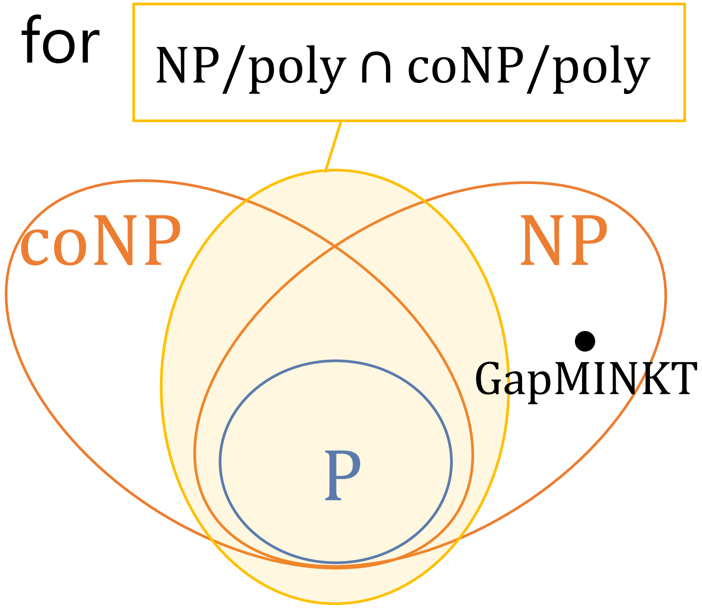
Theorem [Feigenbaum & Fortnow'93, Bogdanov & Trevisan'06]

There is no nonadaptive black-box reduction from L to DistNP, for any $L \notin \mathrm{NP/poly} \cap \mathrm{coNP/poly}$.

- Nonadaptive black-box reductions are too strong to be useful for worst-case-to-average-case connections outside $\mathrm{coNP/poly}$.

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

  We exploit the efficiency of an oracle using "meta-complexity".



Outline

1. Toward Excluding Heuristica

2. Limits of Black-Box Reductions

3. Our Results, Meta-Complexity, and Proof Techniques

Our Results

Main Theorems [H. STOC'21]

(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

- n denotes the length of inputs (encoded as binary strings).
- $\mathrm{Avg_P P}$ ($\subseteq \mathrm{AvgP}$): the class of $(L, \mathcal{D})$ solvable by average-case polynomial-time algorithms whose running time can be "estimated."

Our Results

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

in Theorems ([H. STOC'21], a

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

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

(1) $\mathrm{NTIME}_{\mathrm{sv}}\left(2^{n^{1-\delta}}\right) \nsubseteq \mathrm{DTIME}\left(2^{O(n/\log n)}\right) \implies \mathrm{coNP} \times \{\mathcal{U}, \mathcal{T}\} \nsubseteq \mathrm{Avg}^{1}_{1-n^{-c}}\mathrm{P}$

(2) $\mathrm{PHTIME}\left(2^{n^{1-\delta}}\right) \nsubseteq \mathrm{DTIME}\left(2^{O(n/\log n)}\right) \implies \mathrm{PH} \times \{\mathcal{U}, \mathcal{T}\} \nsubseteq \mathrm{Avg}^{1}_{1-n^{-c}}\mathrm{P}$

(3) $\mathrm{NTIME}\left(2^{n^{1-\delta}}\right) \nsubseteq \mathrm{DTIME}\left(2^{O(n/\log n)}\right) \implies \mathrm{NP} \times \{\mathcal{U}, \mathcal{T}\} \nsubseteq \mathrm{Avg}_{\mathrm{P}}\mathrm{P}$

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

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

$\mathcal{T} \coloneqq \{\mathcal{T}_n\}_{n\in\mathbb{N}}$; $\mathcal{T}_n$ is the singleton distribution on 1^n.

Time-Bounded Kolmogorov Complexity

- t-time-bounded Kolmogorov complexity of x

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

Examples

$$\mathrm{K}^t(\underbrace{00 \ldots 0}_{n \text{ times}}) = \log n + O(1) \quad \text{for } t \gg n.$$ ← print "0" × n

$$\mathrm{K}^t(x) \leq n + O(1) \quad \text{for } t \gg n \text{ and for every } x \in \{0,1\}^n.$$ ← print "x"

$$\mathrm{K}^\infty(x) \geq n - 2 \quad \text{with probability} \geq \frac{3}{4} \text{ over a random } x \sim \{0,1\}^n.$$

← a simple counting argument

Meta-Complexity – Complexity of Complexity

➢ Examples of meta-computational problems: MCSP, MKTP, MINKT, ...

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

- t-time-bounded Kolmogorov complexity of x

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

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

- $\mathrm{GapMINKT} = (\Pi_{\mathrm{Yes}}, \Pi_{\mathrm{No}})$ An "$O(\log n)$-additive approximation" version

  $\Pi_{\mathrm{Yes}} = \{(x, 1^t, 1^s) \mid \mathrm{K}^t(x) \le s\}.$ p: some polynomial

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

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)

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

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

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

Open: $\mathrm{NP} \leq \mathrm{MINKT}$? $\mathrm{NP} \leq \mathrm{MINKT}^{\mathrm{PH}}$?

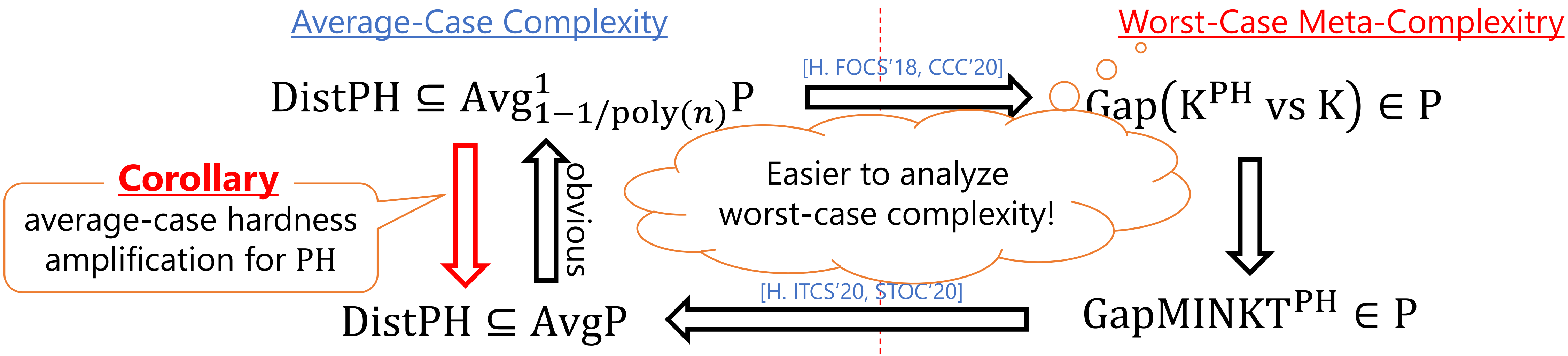
Average-Case Complexity = Meta-Complexity

Theorem [H. (FOCS'20)]

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

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.**



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

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

$\Downarrow$ **Goal**

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

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

P-computable average-case poly-time

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, for every $x \in \{0,1\}^*$ and every $t \geq p(|x|)$,
  1. $A(x,t) = L(x)$ and
  2. $A(x,t)$ halts in time $2^{O\left(\mathrm{cd}^{t,p(t)}(x) + \log t\right)}$.

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

[H. FOCS'18, CCC'20]

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

Goal

[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 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):

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

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

Algorithm B:

Run $A(x,t), A(x,p(t)), A(x,p^2(t)), \ldots, A(x,p^{I-1}(t))$ 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 $2^{O\left(\mathrm{cd}^{t,p(t)}(x)+\log t\right)}$.

How we overcame limits of black-box reductions

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

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

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

Goal

[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].

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

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]

G

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

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

[H. STOC'21]

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

k-Wise Direct Product Generator [H. STOC'20]

$$\mathrm{DP}_k\colon \{0,1\}^n \times (\{0,1\}^n)^k \to \{0,1\}^{nk+k}$$

$$\mathrm{DP}_k(x; z_1, \ldots, z_k) = (z_1, \ldots, z_k, \langle z_1, x\rangle, \ldots, \langle z_k, x\rangle)$$

A pseudorandom generator construction based on a "hard" truth table x that extends seed z by k bits.

$\langle z_i, x\rangle$: the inner product between z_i and x modulo 2.

A Reconstruction Property of DP_k: (under $\mathrm{DistNP} \subseteq \mathrm{AvgP}$ or a derandomization assumption)

For every oracle $D\colon \{0,1\}^{nk+k} \to \{0,1\}$ and every $x \in \{0,1\}^n$,
if $\mathrm{K}^{t,D}(x) \geq k + O(\log n)$, then $\mathrm{DP}_k(x; -)$ is pseudorandom against D; that is,

$$\Pr_{z\sim\{0,1\}^{nk}}\left[D\left(\mathbf{DP}_k(\boldsymbol{x};\boldsymbol{z})\right) = 1\right] \approx \Pr_{w\sim\{0,1\}^{nk+k}}[D(\boldsymbol{w}) = 1].$$

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

This is nearly optimal [Trevisan & Vadhan '07].

Claim: $\mathrm{DistNP} \subseteq \mathrm{AvgP} \Longrightarrow \mathrm{GapMINKT} \in \mathrm{P}$

- For simplicity, $t \coloneqq n^2$.
- Consider the following distributional problem $(\mathrm{MINKT}, \mathcal{U}') \in \mathrm{DistNP}$:

  Given $x \sim \{0,1\}^n$ as input, decide whether $\mathrm{K}^t(x) < n - 2$ or not.
- Let A be an errorless heuristic algorithm that solves $(\mathrm{MINKT}, \mathcal{U}')$ with probability $\geq 1 - o(1)$.

  $A(x)$ outputs the correct answer or $\perp$ ("time out").

  $$\mathrm{K}^t(x) < n - 2 \Longrightarrow A(x) \in \{1, \perp\} \qquad \Pr_{x \sim \{0,1\}^n}[A(x) = \perp] \leq o(1)$$
- A randomized algorithm B for solving GapMINKT:

$$B(x, 1^s) \coloneqq 1 \iff A\big(\mathrm{DP}_k(x; z)\big) \in \{1, \perp\} \text{ for a random } z \sim \{0,1\}^{nk+k} \text{ and } k \coloneqq s + O(\log n).$$

(YES case) $\quad \mathrm{K}^t(x) \leq s \Longrightarrow \mathrm{K}^{2t}\big(\mathrm{DP}_k(x; z)\big) \leq \mathrm{K}^t(x) + |z| + O(1) \leq s + nk + O(1) \ll k + nk - 2.$

$\Longrightarrow A\big(\mathrm{DP}_k(x; z)\big) \in \{1, \perp\}$ with probability 1

(No case) $\quad \mathrm{K}^{t'}(x) \gg s + O(\log n) = k \Longrightarrow \Pr_z[A(\mathrm{DP}_k(x; z)) \in \{1, \perp\}] \approx \Pr_w[A(w) \in \{1, \perp\}] \leq \frac{1}{4} + o(1)$

This is a non-black-box reduction: $t' \approx$ (the running time of A) $= \mathrm{poly}(t, n)$.

GapMINKT is a meta-computational problem!

Summary and Open Questions

- **Meta-complexity** is a powerful tool to analyze **average-case complexity**.
  - Especially because it allows us to overcome the limits of black-box reductions

- A lot of interesting questions remain open:
  - Non-relativizing proof techniques in this context?
    - NP-hardness of $\mathrm{GapMINKT}$
  - 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 $\mathrm{PH} \not\subseteq \text{io-}\mathrm{DTIME}\left(2^{o(n)}\right) \Longrightarrow \mathrm{DistPH} \not\subseteq \text{io-}\mathrm{AvgP}$?

    Viola's barrier comes into play in this setting!