Meta-Complexity Theoretic Approach to Complexity Theory

Shuichi Hirahara
National Institute of Informatics

Oxford-Warwick Complexity Meeting
Meta-Complexity

➢ refers to the (meta-)complexity of problems asking for complexity.

Examples

• Minimum Circuit Size Problem (MCSP)  [Kabanets & Cai ’00]
  ≈ “the problem of computing the circuit complexity of a given function $f$”

• Minimum Time-bounded Kolmogorov complexity Problem (MINKT)  [Ko ’91]
  ≈ “the problem of computing the time-bounded Kolmogorov complexity of a given string $x$”
Recent Progress on Meta-Complexity

➢ Many papers have been published recently. For example:

[H. (FOCS’20)], [Liu & Pass (FOCS’20)], [Ilango (FOCS’20)]
[H. (CCC’20)], [Ilango (CCC’20)], [Saks & Santhanam (CCC’20)],
[Ilango, Loff, Oliveira (CCC’20)], [Kabanets-Koroth-Lu-Myrisiotis-Oliveira (CCC’20)]
[H. (STOC’20)], [Chen-Jin-Williams (STOC’20)]
[H. (ITCS’20)], [Santhaman (ITCS’20)], [Ilango (ITCS’20)],
[Chen-H.-Oliveira-Pich-Rajgopal-Santhanam (ITCS’20)]
...

Today’s Plan

➢ Focus on average-case complexity, meta-complexity, and Impagliazzo’s five worlds.
➢ Try to convey high-level ideas and might ignore technical details.

(E.g., BPP vs. P; quasi-poly-time vs. poly-time)
Impagliazzo’s five worlds and Minimum Circuit Size Problem
Impagliazzo’s five worlds

- Cryptomania
- Minicrypt
- Pessiland
- Heuristica

\[ \text{P} \neq \text{NP} \]

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

\[ \text{P} = \text{NP} \]
Impagliazzo’s five worlds

- Cryptomania
- Minicrypt
- Pessiland
- Heuristica
- Algorithmica

$P \neq NP$

[Impagliazzo ’95]

Classified five possible worlds consistent with our current knowledge.

- Easy to solve $NP$ problems
- No secure cryptography

$P = NP$

The icons are from https://commons.wikimedia.org/wiki/Category:Oxygen_icons_emotes
<table>
<thead>
<tr>
<th>Impagliazzo’s five worlds</th>
<th>[Impagliazzo ’95]</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cryptomania</td>
<td>Classified five possible worlds consistent with our current knowledge.</td>
</tr>
<tr>
<td>∃ public-key crypto.</td>
<td></td>
</tr>
<tr>
<td>Minicrypt</td>
<td></td>
</tr>
<tr>
<td>∃ one-way function</td>
<td>&amp;</td>
</tr>
<tr>
<td>Pessiland</td>
<td></td>
</tr>
<tr>
<td>DistNP ⊄ AvgP</td>
<td>&amp;</td>
</tr>
<tr>
<td>Heuristica</td>
<td></td>
</tr>
<tr>
<td>P ≠ NP</td>
<td>&amp;</td>
</tr>
<tr>
<td>Algorithmica</td>
<td></td>
</tr>
<tr>
<td>P = NP</td>
<td></td>
</tr>
</tbody>
</table>
Impagliazzo’s five worlds

[Impagliazzo ‘95]

Classified five possible worlds consistent with our current knowledge.

- **Cryptomania**
  \[ \exists \text{ public-key crypto.} \]

- **Minicrypt**
  \[ \exists \text{ one-way function} \quad \& \quad \nexists \text{ public-key crypto.} \]

- **Pessiland**
  \[ \text{DistNP} \not\subseteq \text{AvgP} \quad \& \quad \nexists \text{ one-way function} \]

- **Heuristica**
  \[ \text{Easy to solve NP on average} \quad \& \quad \text{Hard to solve NP in the worst-case} \]
  \[ P \neq NP \quad \& \quad \text{DistNP} \subseteq \text{AvgP} \]

- **Algorithmica**
  \[ P = NP \]

The icons are from https://commons.wikimedia.org/wiki/Category:Oxygen_icons_emotes
### Impagliazzo’s five worlds

<table>
<thead>
<tr>
<th>Cryptomania</th>
<th>Classification</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\exists$ public-key crypto.</td>
<td>Secure public-key crypto exists</td>
</tr>
<tr>
<td>$\exists$ one-way function &amp; $\nexists$ public-key crypto.</td>
<td>Cannot solve some NP problem</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Minicrypt</th>
<th>Classification</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\exists$ one-way function &amp; $\nexists$ public-key crypto.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Pessiland</th>
<th>Classification</th>
</tr>
</thead>
<tbody>
<tr>
<td>DistNP $\not\in$ AvgP &amp; $\nexists$ one-way function</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Heuristica</th>
<th>Classification</th>
</tr>
</thead>
<tbody>
<tr>
<td>$P \neq NP$ &amp; DistNP $\subseteq$ AvgP</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Algorithmica</th>
<th>Classification</th>
</tr>
</thead>
<tbody>
<tr>
<td>$P = NP$</td>
<td></td>
</tr>
</tbody>
</table>

[Impagliazzo '95]

Classified five possible worlds consistent with our current knowledge.

The icons are from https://commons.wikimedia.org/wiki/Category:Oxygen_icons_emotes
Impagliazzo’s five worlds

Cryptomania

∃ public-key crypto.

Minicrypt

The Ultimate Goal of Complexity Theory

To determine which world corresponds to ours!
(in particular, to resolve the conjecture that our world is Cryptomania.)

P ≠ NP  &  DistNP ⊆ AvgP

Heuristica

Algorithmica

P = NP
Known Facts and Open Questions

Cryptomania

\[ \exists \text{ public-key crypto.} \]

Minicrypt

\[ \exists \text{ one-way function} \]

Pessiland

DistNP \( \not\in \) AvgP

Heuristica

P \( \neq \) NP

Algorithmica
Towards Cryptomania

- **Cryptomania**
  - ∃ public-key crypto.
  - ∃ one-way function
  - DistNP $\not\in$ AvgP

- **Minicrypt**
  - Open Question: Can we exclude Minicrypto from possible worlds?

- **Pessiland**
  - Open Question: Can we exclude Pessiland from possible worlds?

- **Heuristica**
  - Open Question: Can we exclude Heuristica from possible worlds?

- **Algorithmica**
  - Open Question: P $\neq$ NP ($\iff$ Can we exclude Algorithmica?)

**Known facts**

- Proving all the implications $\iff$ Our world is Cryptomania

**Open questions**

- Proving a implication $\iff$ Excluding a world
Limits of Current Proof Techniques

- **Cryptomania**:
  - \( \exists \) public-key crypto.
  - Certain proof techniques are not sufficient to resolve the question.

- **Minicrypt**
  - \( \exists \) one-way function

- **Pessiland**
  - \( \text{DistNP} \not\subseteq \text{AvgP} \)

- **Heuristica**
  - \( P \neq NP \)
  - **Relativization barrier** [Baker-Gill-Solovey ‘75]
  - **Algebrization barrier** [Aaronson & Wigderson ‘09]

- **Algorithmica**
  - **Natural proof barrier** [Razborov & Rudich ‘97]

Known facts:
- Proving a implication
- Excluding a world

Open questions:
- Proving all the implications
  - Our world is Cryptomania
Limits of Current Proof Techniques

- **Cryptomania**: ∃ public-key crypto.
- **Minicrypt**: ∃ one-way function
- **Pessiland**: DistNP $\not\subseteq$ AvgP
- **Heuristica**: P $\neq$ NP
- **Algorithmica**:

**Known facts**
- Proving all the implications $\iff$ Our world is Cryptomania
- Proving a implication $\iff$ Excluding a world

**Open questions**
- Certain proof techniques are not sufficient to resolve the question.

**Relativization barrier** [Impagliazzo ‘11]

**Limits of black-box reductions**
- [Feigenbaum & Fortnow ‘93]
- [Bogdanov & Trevisan ‘06]
**Approach:** Meta-Complexity

- **Cryptomania**
  - $\exists$ public-key crypto.
- **Minicrypt**
  - $\exists$ one-way function
- **Pessiland**
  - $\text{DistNP} \not\in \text{AvgP}$
- **Heuristica**
  - $P \neq NP$
- **Algorithmica**

$\text{MCSP} \not\in P$

- **Known facts**
  - Excluding a world
- **Open questions**
  - Proving all the implications
  - Our world is Cryptomania
  - Proving a implication
  - Excluding a world
Minimum Circuit Size Problem (MCSP)

**Input**
- The truth table of a Boolean function $f : \{0,1\}^n \rightarrow \{0,1\}$

**Example**
```
truthtable($\oplus_2$) = 0110
```

**Output**
The minimum size of a circuit computing $f$
```
size($\oplus_2$) = 3
```

MCSP = “the problem of computing the circuit complexity of $f$”

- A representative example of meta-complexity-theoretic problems

(informal) [Kabanets & Cai ’00]
Minimum Circuit Size Problem (MCSP)

**Input**
- The truth table of a Boolean function \( f: \{0,1\}^n \rightarrow \{0,1\} \)
- A size parameter \( s \in \mathbb{N} \)

**Output**
Is the minimum size of a circuit computing \( f \) \( \leq s \)?

**Example**
- truthtable(⊕₂) = 0110
- size(⊕₂) = 3

\( \text{MCSP} = \text{“the problem of computing the circuit complexity of } f\text{”} \)

➢ A representative example of meta-complexity-theoretic problems

**Fact:** MCSP ∈ NP

**Open:** NP-hardness of MCSP

[Kabanets & Cai ‘00]
Relationships between the five worlds

- **Algorithmica**
- **Heuristica**
- **Pessiland**
- **Minicrypt**
- **Cryptomania**

**Known facts**

- \( \exists \) public-key crypto.
- \( \exists \) one-way function
- \( \text{DistNP} \not\subset \text{AvgP} \)
- \( P \neq NP \)
- \( \text{MCSP} \not\in P \)

**Theorem** [RR97, HILL99, ABKvMR06]

\[ \exists \text{OWF} \implies \text{MCSP} \not\in \text{BPP}. \]

**Fact**

\( \text{MCSP} \in \text{NP} \)

**Open questions**
Relationships between the five worlds

**Cryptomania**
- \( \exists \) public-key crypto.

**Minicrypt**
- \( \exists \) one-way function

**Pessiland**
- \( \text{DistNP} \not\in \text{AvgP} \)

**Heuristica**
- \( P \neq NP \)

**Algorithmica**

**Theorem** [RR97, HILL99, ABKvMR06]: \( \exists \text{OWF} \) implies \( \text{GapMCSP} \not\in \text{BPP} \).

**Fact**: \( \text{MCSP} \in \text{NP} \)

**Gap**: An approximation version

**Known facts**

**Open questions**
Worst- and average-case equivalence

**Cryptomania**

\[ \exists \text{ public-key crypto.} \]

**Minicrypt**

\[ \exists \text{ one-way function} \]

**Pessiland**

\[ \text{DistNP} \not\in \text{AvgP} \]

**Heuristica**

\[ P \neq NP \]

**Algorithmica**

\[ \not\exists \text{ public-key crypto.} \]

---

**Theorem** [H. (FOCS'18)]

Worst- and average-case complexities of GapMCSP are equivalent.

**Gap**

An approximation version
Worst- and average-case equivalence

Cryptomania

∃ public-key crypto.

Minicrypt

∃ one-way function

Pessiland

\text{DistNP} \not\in \text{AvgP}

Heuristica

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

Algorithmica

\text{Theorem} [H. (FOCS'18)]

Worst- and average-case complexities of \text{GapMCSP} are equivalent.

\text{MCSP} \not\in \text{AvgP} \iff \text{GapMCSP} \not\in \text{prBPP}

\text{AvgP: Average-case polynomial-time}

\text{P: (Worst-case) polynomial-time}

\text{Gap: An approximation version}

* More precisely, (MCSP[2^{en}],\mathcal{U}) \not\in \text{AvgBPP} (\exists \epsilon > 0) \iff \text{GapMCSP} \not\in \text{prBPP}.
Overcoming limits of black-box reductions

Cryptomania

\[ \exists \text{ public-key crypto.} \]

Minicrypt

\[ \exists \]

Pessiland

\[ \text{DistNP} \not\subset \text{AvgP} \]

Heuristica

\[ \text{P} \neq \text{NP} \]

Algorithmica

\[ \text{MCSP} \not\subset \text{AvgP} \]

\[ \text{GapMCSP} \not\subset \text{P} \]

\[ \Rightarrow \text{ Known facts} \]

\[ \not\Rightarrow \text{ Open questions} \]

\[ \textbf{Theorem} \ [\text{H. (FOCS'18)}] \]

\[ \text{Worst- and average-case complexities of GapMCSP are equivalent.} \]

AvgP: Average-case polynomial-time

P: (Worst-case) polynomial-time

Gap: An approximation version
Overcoming limits of black-box reductions

\[ \exists \text{ public-key crypto.} \]

\[ \exists \text{ one-way function} \]

\[ \text{DistNP} \not\subseteq \text{AvgP} \]

\[ \text{P} \neq \text{NP} \]

\[ \text{MINICRYPT} \}

\[ \text{PESSILAND} \]

\[ \text{HEURISTIC} \]

\[ \text{ALGORITHMICA} \]

\[ \text{CRYPTOMANIA} \]

\[ \text{THEOREM} \] [H. (FOCS’18)]

\[ \text{WORST- and average-case} \]

\[ \text{complexities of} \]

\[ \text{GapMCSP} \text{ are equivalent.} \]

\[ \text{MCSP} \not\subseteq \text{AvgP} \]

\[ \text{gapMCSP} \not\subseteq \text{P} \]

\[ \text{DISTNP} \not\subseteq \text{AvgP} \]

\[ \text{OBSVIOUS} \]

\[ \text{THEOREM} \] [Bogdanov & Trevisan ’06]

\[ \text{If there is a (black-box)} \text{ randomized nonadaptive reduction} \]

\[ \text{from GapMCSP to DistNP, then GapMCSP} \in \text{coNP/poly.} \]

(unlikely!)
**AvgP = Average-Case Poly-time = Errorless Heuristics**

\[(L, \mathcal{D}) \in \text{AvgP} \iff \exists \text{ alg. } A \text{ such that}\]

1. \(A(x) = L(x)\) for every \(x\), and
2. \(\mathbb{E}_{x \sim \mathcal{D}} [t_A(x)^\epsilon] = O(n)\) for some \(\epsilon > 0\),

where \(t_A(x)\) denotes the running time of \(A\) on input \(x\).

Equivalently:

\[(L, \mathcal{D}) \in \text{AvgP} \iff \exists \text{ alg. } A \text{ such that}\]

1. \(A(x, \delta) \in \{L(x), \perp\}\) for every \(x\),
2. \(\mathbb{P}_{x \sim \mathcal{D}} [A(x, \delta) = \perp] \leq \delta\), and
3. \(t_A(x, \delta) \leq \text{poly}(n/\delta)\).
A New Approach Towards Excluding Heuristica

- Known facts
- Public-key cryptography is possible.
- One-way functions exist.
- \( \text{DistNP} \not\in \text{AvgP} \)

- Open questions
- Can we exclude Heuristica?
- Is \( \text{GapMCSP} \) NP-hard?

Corollary of “\( \iff \)”

If \( \text{GapMCSP} \) is NP-hard, then Heuristica is excluded.

- \( \text{P} \neq \text{NP} \)
- \( \text{AvgP}: \) Average-case polynomial-time
- \( \text{P}: \) (Worst-case) polynomial-time

Gap: An approximation version
Impagliazzo’s Five Worlds

Cryptomania

∃ public-key crypto.

Minicrypt

∃ one-way function

Pessiland

DistNP \not\subseteq AvgP

Heuristica

P \neq NP

Algorithmica

NP-complete problems

Meta-Complexity Worlds

MINKT \not\in HeurP

MCSP \not\in AvgP

GapMCSP \not\in P

MultiMCSP \not\in P

AC^0-MCSP \not\in P

DNF \circ XOR-MCSP \not\in P

Known facts

Open questions

Recent results

[Impagliazzo (FOCS’18, CCC’20)]

[H. (FOCS’18, CCC’20)]

[Liu & Pass (FOCS’20)]

[Ilango, Loff, Oliveira (CCC’20)]

[Ilango (FOCS’20)]

[L. Oliveira-Santhanam (CCC’18)]
Recent Progress on NP-hardness of MCSP

Towards excluding Heuristica
\( \mathcal{C} \)-MCSP for a restricted circuit class \( \mathcal{C} \)

- A natural approach to make progress toward NP-hardness of MCSP:
  
  To restrict ourselves to a circuit class \( \mathcal{C} \) such as \( \mathcal{C} \in \{ \text{DNF}, \text{AC}^0, \ldots \} \).

**Definition** (\( \mathcal{C} \)-MCSP)

Given \( f: \{0,1\}^n \to \{0,1\} \) and \( s \in \mathbb{N} \), is there a \( \mathcal{C} \)-circuit of size at most \( s \) computing \( f \)?
NP-hardness of DNF-MCSP

Nearly 40 years ago, Masek proved NP-hardness of DNF-MCSP.

Theorem [Masek (1978 or 1979, unpublished)]

DNF-MCSP is NP-hard.

Examples of DNF formula
\[ \varphi = (\neg x_1 \land x_2) \lor (x_2 \land \neg x_3) \lor \neg x_2 \]
NP-hardness of (DNF $\circ$ XOR)-MCSP

We were able to extend DNF formulas to DNF $\circ$ XOR formulas.

**Theorem [H., Oliveira & Santhanam (CCC’18)]**

(DNF $\circ$ XOR)-MCSP is NP-hard.

A DNF $\circ$ XOR formula
Recent Progress: NP-hardness of AC$^0$-MCSP

- [Rahul Ilango] extended the frontier to depth-$d$ AC$^0$ formulas for any constant $d \geq 2$.

(cf. talk on June 18 in Oxford-Warwick complexity meeting.)

**Theorem** [Ilango (FOCS’20)]

For any constant $d \geq 2$, Depth-$d$-AC$^0$-MCSP is NP-hard (under randomized quasi-polynomial-time reductions).

An AC$^0$ formula
Recent Progress: NP-hardness of Multi-MCSP

**Theorem** [Ilango-Loff-Oliveira (CCC’20)]

Multi-MCSP is NP-hard
(under randomized reductions).

**Definition** (Multi-MCSP)

Given a function $f : \{0,1\}^n \rightarrow \{0,1\}^m$ and a size parameter $s$, is there a multi-output circuit of size $s$ computing $f$?

**Key Idea**: Instead of restricting a circuit class, try to restrict the structure of a circuit by specifying the $m$-bit output!
Impagliazzo’s Five Worlds

- **Cryptomania**: ∃ public-key crypto.
- **Minicrypt**: ∃ one-way function
- **Pessiland**: DistNP ⊈ AvgP
- **Heuristica**: P ≠ NP
- **Algorithmica**: AC⁰-MCSP ≠ P
- **MultiMCSP ≠ P**
- **DNF ∘ XOR-MCSP ≠ P**
- **MINKT ∉ HeurP**
- **MCSP ∉ AvgP**
- **GapMCSP ∉ P**

Meta-Complexity Worlds

- **Known facts**
- **Open questions**
- **Recent results**

**Known facts**

- MinkT ⊈ HeurP
- MCSP ⊈ AvgP
- GapMCSP ⊈ P

**Open questions**

- What’s the difference between Multi-MCSP and MCSP?
- Non-relativizing proof techniques?

**Relativization barrier**

- Impagliazzo ‘11
- Ko ‘91

**NP-complete problems**

- MultiMCSP ⇄ P
- AC⁰-MCSP ⇄ P
- DNF ∘ XOR-MCSP ⇄ P

**Recent results**

- [Liu & Pass (FOCS’20)]
- [Ilango (FOCS’20)]
- [H. Oliveira-Santhanam (CCC’18)]
Impagliazzo’s Five Worlds

- **Cryptomania**: $\exists$ public-key crypto.
- **Minicrypt**: $\exists$ one-way function
- **Pessiland**: $\text{DistNP} \not\subset \text{AvgP}$
- **Heuristica**: $P \neq \text{NP}$
- **Algorithmica**: $\text{MultiMCSP} \not\subset P$

Meta-Complexity Worlds

- **MINKT** $\not\subset \text{HeurP}$
- **GapMINKT** $\not\subset P$
- **MultiMCSP** $\not\subset P$
- **AC^0-MCSP** $\not\subset P$
- **DNF \circ XOR-MCSP** $\not\subset P$

Known facts

- $\text{DistNP} \not\subset \text{AvgP}$
- $\text{DistPH} \not\subset \text{AvgP}$
- $P \neq \text{NP}$

Open questions

- $\exists$ one-way function
- **GapMINKT** $\not\subset P$
- **GapMINKT^PH** $\not\subset P$

Recent results

- [H. (FOCS’18, CCC’20)]
- [Ilango (FOCS’20)]
- [Liu & Pass (FOCS’20)]
Average-Case Complexity

versus

Meta-Complexity

Towards better understanding of average-case complexity
Can we prove the converse?

**Theorem** [H. (FOCS’18)]

Worst- and average-case complexities of GapMCSP are equivalent.

- \( \exists \text{public-key crypto.} \)
- \( \exists \text{one-way function} \)
- \( \text{DistNP} \not\subseteq \text{AvgP} \)
- \( \text{MCSP} \not\subseteq \text{AvgP} \)
- \( \text{GapMCSP} \not\subseteq \text{P} \)

**AvgP:** Average-case polynomial-time

**P:** (Worst-case) polynomial-time

**Gap:** An approximation version
**MINKT**

(Minimum Time-bounded Kolmogorov Complexity Problem)  

**Input**
- A binary string $x \in \{0,1\}^*$
- A time bound $1^t$ (in unary)

**Output**

$K^t(x)$ (t-time-bounded Kolmogorov complexity)

$K^t(x) := \text{the minimum size of a program } M \text{ that outputs } x \text{ in time } t.$

**Example**

- $x = 1^n$
- $x = 1010111010101101$

$K^t(x) = \log n + O(1)$  
← print "1" × n

$K^t(x) \geq n - 1$ with probability $\geq \frac{1}{2}$.

**MINKT** = “the problem of computing the time-bounded Kolmogorov complexity of $x$”

Cf. **MCSP** = “the problem of computing the circuit complexity of $f$”

⇒ meta-complexity theoretic problems.

**Fact:** MINKT ∈ NP  
**Open:** NP-hardness of MINKT
MINKT versus MCSP

Cryptomania

∃ public-key crypto.

Minicrypt

∃ one-way function

Pessiland

DistNP ⊈ AvgP

Heuristica

P ≠ NP

Algorithmica

|GapMINKT: a $O(\log t|x|)$-additive approximation of $K^t(x)$|

|GapMCSP: a $|f|^{1-\epsilon}$-factor approximation of size($f$)|

Theorem [H. (FOCS’18, CCC’20)]

Worst- and average-case complexities of GapMINKT are equivalent.

Known facts

Open questions

*Assuming the existence of complexity-theoretic PRG (for derandomization).
Impagliazzo’s Five Worlds

- **Cryptomania**: ∃ public-key crypto.
- **Minicrypt**: ∃ one-way function
  - **Pessiland**: DistNP ⊈ AvgP
  - **Heuristica**: P ≠ NP
  - **Algorithmica**: [Liu & Pass (FOCS’20)]

Meta-Complexity Worlds

- **MINKT**: □ HeurP
  - **MCSP**: □ AvgP
  - **MultiMCSP**: □ P
  - **AC^0-MCSP**: □ P
  - **DNF ∘ XOR-MCSP**: □ P

Known facts: ▶
Open questions: ▲
Recent results: △

- [H. (FOCS’18, CCC’20)]
- [Ilango (FOCS’20)]
- [Ilango, Loff, Oliveira (CCC’20)]
- [H., Oliveira-Santhanam (CCC’18)]
Impagliazzo’s Five Worlds

- **Cryptomania**: \( \exists \) public-key crypto.
- **Minicrypt**: \( \exists \) one-way function
- **Pessiland**: \( \text{DistNP} \not\subseteq \text{AvgP} \)
- **Heuristica**: \( P \neq \text{NP} \)
- **Algorithmica**: \( \text{AC}^0 - \text{MCSP} \not\subseteq \text{P} \), \( \text{DNF} \circ \text{XOR-MCSP} \not\subseteq \text{P} \)

Meta-Complexity Worlds

- **MINKT \not\in \text{HeurP}**
- **MINKT \not\in \text{AvgP}**
- **GapMINKT \not\in \text{P}**

Known facts

- \( \rightarrow \)

Open questions

- \( \rightarrow \)

Recent results

- \( \leftrightarrow \)

Recent results

- \( \leftrightarrow \)

Known facts

- \( \rightarrow \)
Impagliazzo’s Five Worlds

- Cryptomania: \exists \text{ public-key crypto.}
- Minicrypt: \exists \text{ one-way function}
- Pessiland: \text{DistNP} \not\subseteq \text{AvgP}
- Algorithmic: \text{P} \neq \text{NP}

Meta-Complexity Worlds

- MINKT \not\subseteq \text{HeurP}
- MINKT \not\subseteq \text{AvgP}
- GapMINKT \not\in \text{P}
- MultiMCSP \not\in \text{P}
- \text{AC}^0\text{-MCSP} \not\in \text{P}
- \text{DNF} \circ \text{XOR-MCSP} \not\in \text{P}

PH: polynomial-time hierarchy

\text{P} = \text{NP} \iff \text{P} = \text{PH}
Impagliazzo's Five Worlds

<table>
<thead>
<tr>
<th>Cryptomania</th>
<th>Minicrypt</th>
<th>Pessiland</th>
<th>Heuristica</th>
<th>Algorithmica</th>
</tr>
</thead>
<tbody>
<tr>
<td>( \exists ) public-key crypto.</td>
<td>( \exists ) one-way function</td>
<td>DistNP ( \not\in ) AvgP</td>
<td>DistPH ( \not\in ) AvgP</td>
<td>P ( \neq ) NP</td>
</tr>
</tbody>
</table>

Meta-Complexity Worlds

| MINKT \( \not\in \) HeurP | MINKT \( \not\in \) AvgP | GapMINKT \( \not\in \) P |

Known facts

Open questions

Recent results

Theorem \[H. (FOCS'20)]

\[\text{DistPH} \subseteq \text{AvgP} \iff \text{GapMINKT}^{PH} \in P\]
**Average-Case Complexity**

\[ \text{DistPH} \subseteq \text{AvgP} \]

**Meta-Complexity Worlds**

\[ \Sigma_k \text{SAT}: \text{A } \Sigma_k^P \text{-complete problem} \]

\[ \text{GapMINKT}^{\Sigma_k \text{SAT}} \in P \ (\forall k \in \mathbb{N}) \]

\[ \text{GapMINKT}^A \in P \text{ for any } A \in \text{PH}. \]

**Worst-Case Meta-Complexity**

\[ \text{MINKT}^\text{PH} \in \text{AvgP} \]

\[ \text{GapMINKT}^\text{PH} \in P \]

**Theorem** [H. (FOCS’20)]

\[ \text{DistPH} \subseteq \text{AvgP} \iff \text{GapMINKT}^\text{PH} \in P \]
The diagram illustrates the relationships between the complexity classes and theorems related to average-case complexity and meta-complexity.

### Average-Case Complexity

- \( \text{DistPH} \subseteq \text{Avg}_{1-1/poly(n)} P \)
- \( \text{DistPH} \subseteq \text{Avg}_{1/poly(n)} P \)
- \( \text{DistPH} \subseteq \text{AvgP} \)
- \( \text{DistPH} \subseteq \text{Avg}_{1-1/poly(n)} P \)

### Meta-Complexity Worlds

- \( \text{coMINKT}^\text{PH} \in \text{Avg}_{1-1/poly(n)} P \)
- \( \text{MINK}^\text{PH} \in \text{Avg}_{1/poly(n)} P \)
- \( \text{MINK}^\text{PH} \in \text{AvgP} \)

### Worst-Case Meta-Complexity

- \( \text{GapMINKT}^\text{PH} \in P \)

### Theorem [H. (FOCS’20)]

\[
\text{DistPH} \subseteq \text{AvgP} \iff \text{GapMINKT}^\text{PH} \in P
\]

*Under the assumption that \( P = \text{ZPP} \)
**Average-Case Complexity**

- PH is easy on a $1/poly(n)$-fraction of inputs
- $\text{DistPH} \subseteq \text{Avg}_{1 - 1/poly(n)}^P$

**Meta-Complexity Worlds**

**Corollary [H. (FOCS’20)]**

Errorless hardness amplification for PH (for deterministic algorithms)

**Worst-Case Meta-Complexity**

- $\text{GapMINKT}^\text{PH} \in P$

- PH is easy on most inputs
- $\text{DistPH} \subseteq \text{AvgP}$
**Average-Case Complexity**

**Corollary** [H. (FOCS’20)]

Errorless hardness amplification for PH (for deterministic algorithms)

\[
\text{DistPH} \subseteq \text{Avg}_{1 - 1/\text{poly}(n)} P
\]

\[
\text{MINKT}^{PH} \in \text{NP}^{PH} = \text{PH}
\]

\[
\text{MINKT}^{PH} \in \text{Avg}_{1 - 1/\text{poly}(n)} P
\]

\[
\text{Goal} \Rightarrow \text{obvious}
\]

\[
\text{DistPH} \subseteq \text{AvgP}
\]

**Meta-Complexity Worlds**

Based on unexpected hardness results for Kolmogorov complexity and build on [H. (ITCS’20, STOC’20)]

Based on non-black-box worst-to-average-case reductions and build on [H. (FOCS’18, CCC’20)]

\[
\text{GapMINKT}^{PH} \in \text{P}
\]

➢ The proof goes through meta-complexity worlds (despite that the theorem is purely average-case complexity-theoretic).

➢ Meta-complexity appears essential!
Impagliazzo’s Five Worlds

Cryptomania

∃ public-key crypto.

Minicrypt

∃ one-way function

Pessiland

DistNP ⊈ AvgP

Heuristica

P ≠ NP

Algorithmica

Recent results

Theorem [Liu & Pass (FOCS’20)]

∃ one-way function if and only if MINKT is hard for two-sided-error average-case algorithms.

Open Question

• Is there a difference between errorless and two-sided-error average-case notions for MINKT?
Impagliazzo’s Five Worlds

Cryptomania

- $\exists$ public-key crypto.

Minicrypt

- $\exists$ one-way function

Pessiland

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

Heuristica

- $P \not= NP$

Algorithmica

- $P \not= NP$

Meta-Complexity Worlds

- $\text{MINKT} \not\in \text{HeurP}$
- $\text{MINKT} \not\in \text{AvgP}$
- $\text{MINKT}^{PH} \not\in \text{AvgP}$
- $\text{GapMINKT} \not\in P$
- $\text{GapMINKT}^{PH} \not\in P$

Recent results

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

Open questions

- $P \not= NP$[Liu & Pass (FOCS’20)]
- $\text{MINKT} \not\in \text{AvgP}$[H. (FOCS’18, CCC’20)]
- $\text{MINKT}^{PH} \not\in \text{AvgP}$[H. (FOCS’20)]
- $\text{GapMINKT} \not\in P$
- $\text{GapMINKT}^{PH} \not\in P$

Known facts

- $\text{MultiMCSP} \not\in P$
- $\text{AC}^0\text{-MCSP} \not\in P$
- $\text{DNF} \circ \text{XOR-MCSP} \not\in P$

Conclusions

Meta-complexity theoretic characterizations of central open questions
Summary

➢ Recent results provide meta-complexity-theoretic characterizations of central open questions in complexity theory.

➢ A meta-complexity view is useful (and appears promising):
   E.g., A hardness amplification theorem for PH via meta-complexity [H. (FOCS’20)]

➢ Open: Does GapMINKT ∈ P imply DistNP ⊆ AvgP?
   This implies a hardness amplification theorem for NP [H. (FOCS’20)]

➢ Questions or comments?