# Metacomplexity and Related Problems

Jacob Gray[1] Pengxiang Wang[2]

[1]University of Massachusetts Amherst

[2]University of Michigan

June 6, 2022

# Outline

# Background

- Computational Complexity Theory studies the resources required to solve computational problems on abstract machines
- Complexity theory's most well-known problem: $\mathsf{P} \stackrel{?}{=} \mathsf{NP}$

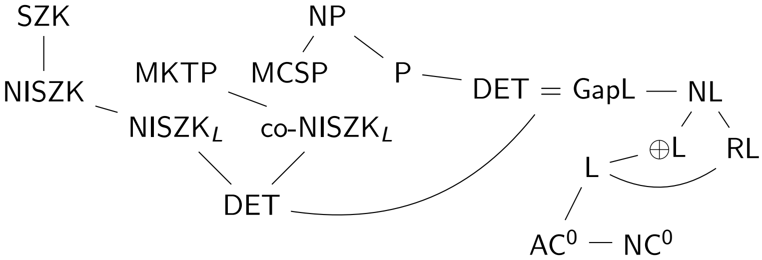


Figure 1: Some relations between complexity classes

# Metacomplexity

- Metacomplexity is the "complexity of computational problems about Complexity Theory" [1]
- Various metacomplexity problems connect to ordinary complexity classes
  - eg. Kolmogorov (Time) Complexity, Minimum Circuit Size Problem

# Kolmogorov (Time) Complexity

Consider the following two binary strings:

$$010101010101010101010101010101$$

$$111011001100111110110001000110$$

Short description for first string: $(01)^{15}$

The description for the second string is likely longer

Kolmogorov (Time) Complexity is formally defined using Turing Machines.

# What is a Zero Knowledge Proof System?

- Proof system: interactive process between powerful prover and weaker verifier
- Zero Knowledge: Not revealing additional information besides something being true/false
  - In SZK, "zero knowledge" is defined in terms of statistical difference

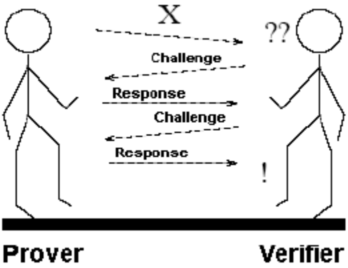


Figure 2: Interactive proof system, from [2]

# An example: Graph Non-isomorphism

Given two graphs $G_0$, $G_1$ claimed to be non-isomorphic:

1. Verifier randomly chooses to send a permutation of either $G_0$ or $G_1$ to the prover
2. Prover tries to guess whether the permuted graph was $G_0$ or $G_1$
3. If the prover is lying about graphs being non-isomorphic, is caught with probability $1/2$ every round
4. Repeat as many times as needed

# One-way Functions

A one-way function is a function that is easy to compute, but hard to invert (even when a program for the function is given). More formally, for any one-way function $f : \{0,1\}^* \to \{0,1\}^*$, polynomial $p(n)$, and efficient randomized algorithm $F$:

$$\Pr_{x \leftarrow \{0,1\}^n}[f(F(f(x))) = f(x)]p(n) \to 0$$

As $n \to \infty$

# Research Goals

- Proving NISZK subclass equivalences:

$$NISZK_{AC^0} \stackrel{?}{=} NISZK_L \stackrel{?}{=} NISZK_{NL}$$

- Improving one-way function results:

$$OWFs \in NC^0 \stackrel{?}{\leftrightarrow} OWFs \in DET$$

# Acknowledgements

We would like to thank our advisor, Eric Allender, his graduate student Harsha Tirumala, and the DIMACS REU 2022 program, which this research is being conducted as part of.

We would also like to thank the NSF, with this research being supported by NSF grant CCF-185221.

# bibliography

[1] Hanlin Ren and Rahul Santhanam. "A Relativization Perspective on Meta-Complexity". In: *39th International Symposium on Theoretical Aspects of Computer Science (STACS 2022)*. Ed. by Petra Berenbrink and Benjamin Monmege. Vol. 219. Leibniz International Proceedings in Informatics (LIPIcs). Dagstuhl, Germany: Schloss Dagstuhl – Leibniz-Zentrum für Informatik, 2022, 54:1–54:13. ISBN: 978-3-95977-222-8. DOI: 10.4230/LIPIcs.STACS.2022.54. URL: https://drops.dagstuhl.de/opus/volltexte/2022/15864.

[2] Stefan Weber. *A Coercion-Resistant Cryptographic Voting Protocol - Evaluation and Prototype Implementation*. July 2006.