How Hard Are Non-interactive Proof Systems?

John Gouwar Caleb Robelle

DIMACS REU Program

August 2, 2020

Talk Overview

1. Reductions, Hardness, and Circuit Complexity
2. Zero-Knowledge Proofs
3. Kolmogorov Complexity, MKTP, and MCSP
4. Our Results

Many-one reductions

Definition

Given problems A and B, and a complexity class $\mathcal{C}$, we say that a is $\mathcal{C}$ **many-one reducible** to B, $A \leq_m^{\mathcal{C}} B$, if there exists a $\mathcal{C}$-computable function f such that $f(x) \in B$ if and only if $x \in A$.

Example

Consider the following languages:

- $L_1 = \{x \in \{0,1\}^* | \, x$ is composed of alternating 1's and 0's$\}$
- $L_2 = \{x \in \{0,1\}^* | \, x$ is composed of alternating pairs of 1's and 0's$\}$
- $L_1 \leq_m^P L_2$

Hardness and Completeness

Definitions

A problem A is **hard** for a complexity class $\mathcal{C}$ if for every $B \in \mathcal{C}$, there exists a reduction from B to A. A problem A is **complete** for a class $\mathcal{C}$ if A is both hard for $\mathcal{C}$ and $A \in \mathcal{C}$.

Example

[Your favorite choice of NP-complete problem] is complete for NP under many-one polynomial time reductions.

Boolean Circuits

Any computable function $f : \{0,1\}^m \rightarrow \{0,1\}^n$ can be modeled by a sequence of boolean (AND, OR, and NOT) gates.

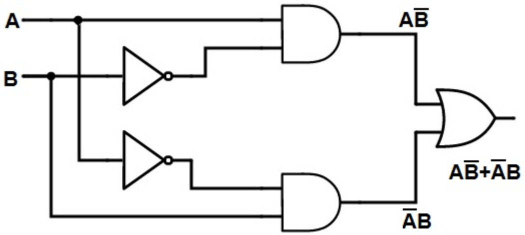

Figure: Example for XOR

We consider the **size** of a circuit c to be the number of gates in the circuit. We consider the **depth** of the circuit to be the number of gates that an input passes through before it is output.

The class NC^0

NC^0

NC^0 is the class of functions that can be computed by circuits where each output bit depends on a **constant** number of input bits. This class does not include $\mathrm{PARITY}, \mathrm{MAJORITY}$, or AND.

Projections

Let $C \in NC^0$. We say that C is a **projection** if each output bit depends on at most a **single** input bit.

Zero-Knowledge Proofs

Definition

SZK is the class of problems which have **interactive statistical zero knowledge proofs** as solutions. These are proofs in which a prover and a verifier interact in such a way that the verifier is certain that the prover knows the secret, but does not give the secret away directly.

Example

Proving knowledge of the difference between Coke and Pepsi:

- Prover claims to know the difference between Coke and Pepsi
- Verifier flips a coin fifty times and gives the prover Pepsi if heads and Coke if tails to check if the prover has the knowledge
- If the prover knows the difference, they should pick the right beverage every time.
- If the prover has no knowledge, they only have a $\frac{1}{2^{50}}$ of getting it right every time.

Non-Interactive Zero Knowledge

Definition

NISZK is the class of problems which have **non-interactive statistical zero knowledge proofs** as solutions. Here, the prover and a verifier have shared access to a random string and the verifier cannot send messages to the prover.

Importance of NISZK

SZK contains hard problems if and only if NISZK contains hard problems. SZK contains the following assumed hard problems:

- Graph isomorphism
- Discrete log
- Decisional Diffie-Hellman

Distinguishing Randomness

Question

Given the following 3 strings, can you tell which one was generated by the flipping of random coins:

- 1010101010101010
- 1101110011101111
- 0100111001110011

Answer

- print "01" * 8
- Calculate the digits of π modulo 2
- Actual coin flips.

Kolmogorov complexity

Definition

Suppose $x \in \{0,1\}^*$. Given a universal Turing machine, U, we define the *Kolmogorov Complexity*, $C(x)$, the length of the shortest description d, such that $U(d, \epsilon) = x$.

Problem

This metric is undecidable in the general case.

Time-Bounded Kolmogorov Complexity

KT Complexity

Let U be a universal Turing machine. For each string x, define $\mathrm{KT}_U(x)$ to be

$$\min\{|d| + T : (\forall\, \sigma \in \{0, 1, *\})(\forall\, i \leq |x| + 1) \\ U^d(i, \sigma) \text{ accepts in } T \text{ steps iff } x_i = \sigma\}$$

We define $x_i = *$ if $i > |x| + 1$; thus, for $i = |x| + 1$ the machine accepts iff $\sigma = *$. The notation U^d indicates that the machine U has random access to the description d.

The Minimum KT Problem

MKTP

Suppose $y \in \{0,1\}^*$ and $\theta \in \mathbb{N}$. We define the following language,

$$\mathsf{MKTP} = \{(y, \theta) \mid \mathrm{KT}(y) \leq \theta\}$$

Properties of MKTP

- MKTP $\in$ NP
- MKTP has not been proven to be an member of P or NP-complete. Therefore, it is a candidate NP-intermediate problem.
- If MKTP $\in$ P, then cryptography as we know it ceases to exist.
- If MKTP is NP-complete, then ZPP $\neq$ EXP.

The Minimum Circuit Size Problem

Circuit Complexity

Given a binary string y, we can interpret y as a truth table of size $2^{|y|}$. The circuit complexity of y, $C(y)$, is the size of the smallest circuit which computes the truth table which y represents.

MCSP

Suppose $y \in \{0,1\}^*$ and $\theta \in \mathbb{N}$. We define the following language,

$$\mathsf{MCSP} = \{(y, \theta) \mid C(y) \leq \theta\}$$

Properties of MCSP

- All of the previously stated properties for MKTP hold for MCSP as well.
- KT complexity is polynomially related to circuit complexity, but no known many-one reduction exists between the two problems.

Previous Results

- SZK $\subseteq$ BPP$^{\mathsf{MKTP}}$. This holds for MCSP as well. (Allender-Das, '18)
- MKTP is hard for DET under NC^0 many one reductions. It is not known whether this holds for MCSP as well. (Allender-Hirahara, '19)
- SZK$_\mathsf{L}$ contains most of the interesting problems in SZK. (Dvir et al., '10)

Entropy Approximation

Entropy

The *entropy* of a distribution is a metric of how “random” we consider the distribution to be. It is the expected value of the information carried by a given element of X. Formally, for a discrete distribution X:

$$H(X) = -\sum_{x \in X} \Pr(x) \cdot \log(\Pr(x))$$

EA

Suppose X is an arbitrary distribution represented by a circuit $C : \{0,1\}^m \to \{0,1\}^n$ and $k \in \mathbb{N} \setminus \{0\}$. We define Promise-EA as follows,

$$\begin{aligned} \mathrm{EA}_{YES} &= \{(X,k) \mid H(X) < k-1\} \\ \mathrm{EA}_{NO} &= \{(X,k) \mid H(X) > k+1\} \end{aligned}$$

- EA is complete for NISZK under $\leq_m^{\mathrm{P}}$ reductions.

Our Results

Primary Result

MKTP is hard for $\mathsf{NISZK_L}$ under projections.

- $\mathsf{EA_{NC^0}}$ is complete for the complexity class $\mathsf{NISZK_L}$ under projections.
- MKTP is hard for NISZK under P/poly many-one reductions by reduction from EA.
- $\mathsf{EA_{NC^0}}$ is reducible to MKTP via a projection.

Review

- $\mathsf{\textbf{NISZK}_L}$: The set of problems which have non-interactive proof systems where the verifier and simulator are in logspace.
- **MKTP**: The problem of deciding whether the "complexity" of a string is greater than or less than a given value.
- **Our Result**: MKTP is hard for $\mathsf{NISZK}_\mathsf{L}$ under very restrictive reductions.
- **Open Question**: Is MKTP NP-hard?

Acknowledgements

We would like to thank the DIMACS REU program for giving us the opportunity with funding through the through NSF grant CCF-1836666.

We would also like to thank our advisor, Dr. Eric Allender, for his support and mentorship.

Logic Gate Source:
https://www.electronicshub.org/exclusive-or-gatexor-gate/