MCSP and MKTP

Vishal Ramesh, Sasha Sami, and Noah Singer
Mentor: Eric Allender, DIMACS REU 2021

June 1, 2021

Outline

Guiding question

Is it hard to show that a particular function is difficult to compute?

Circuits and truth tables

- A *Boolean circuit* is a discrete object composed of logic gates and wires, which maps from Boolean inputs to Boolean outputs
- A *Boolean function* is of the form $f : \{0,1\}^k \to \{0,1\}$
- A Boolean function f can be represented by its *truth table*, listing the value f takes for every input

Example

Truth table for XOR:

z	XOR(z)
00	0
01	1
10	1
11	0

MCSP

MCSP *(minimum circuit size problem)*: Input is a string x of length 2^k, interpreted as a truth table of a k-bit function f. What is the size of the smallest circuit computing f?

The complexity of MCSP

- How difficult is MCSP?
- $\mathbf{NP}$: problems whose solutions can be efficiently verified
- MCSP $\in \mathbf{NP}$
- Unlike almost all other problems in $\mathbf{NP}$, don't have good theoretical understanding of how MCSP fits in

"Most problems in $\mathbf{NP}$"

Most problems $\mathcal{L} \in \mathbf{NP}$ are known to have one of two properties:

- $\mathcal{L}$ has an efficient algorithm (i.e., $\mathcal{L} \in \mathbf{P}$)
- $\mathcal{L}$ is *hard/universal* for $\mathbf{NP}$: For every other $\mathcal{L}' \in \mathbf{NP}$, there is an efficient *reduction* algorithm $\mathcal{A}$ converting instances of $\mathcal{L}'$ to instances of $\mathcal{L}$

The complexity of MCSP, revisited

- Have good reasons to believe MCSP $\notin \mathbf{P}$ [KC00]
- Known barriers to showing that MCSP is hard for $\mathbf{NP}$ via a "very simple" reduction (cf. [MW17])
  - "Simplicity" typically includes locality, efficiency, etc.
- This contrasts with other $\mathbf{NP}$-complete problems (e.g., SAT)

What is MKTP ?

MKTP *(minimum KT complexity problem)*: Given a string x of length 2^k, interpreted as a truth table of a k-bit function f. What is the smallest *description* of f?

Here "description length" is defined as *time-bounded Kolmogorov complexity*, based on Turing machines.

Relation to MCSP

- All theorems about MCSP are known to hold for MKTP
- Recently, hardness results were proven for MKTP that are not yet known to hold for MCSP
  - MKTP is hard for a certain class of problems that have non-interactive statistical zero-knowledge proofs [All+21a]
  - A "conditional" variant of MKTP is hard for $\mathbf{NP}$ under randomized reductions! [All+21b]

Zero-Knowledge Proofs

A *zero-knowledge proof* is a method by which a prover $\mathcal{P}$ can prove to the verifier $\mathcal{V}$ that he knows a secret, without conveying any information apart from the fact that he knows the secret.

Example

Alice is color-blind. Bob has two balls: red and blue. Bob wants to prove to Alice the balls have different colors. **Protocol:**

1. Alice shows Bob one of the balls.
2. Alice puts both balls behind her back, and then randomly picks one ball and shows it to Bob.
3. Alice then asks, "Are the two balls I showed the same color?"

$\mathbf{SZK}$ and $\mathbf{NISZK_L}$

Notion of zero-knowledge proofs is captured by having a simulator $\mathcal{S}$ for every verifier which can output a transcript that "looks like" an interaction between the verifier and the (honest) prover.

- $\mathbf{SZK}$: Class of problems with zero-knowledge proofs, where the transcript outputted by $\mathcal{S}$ is statistically close to interaction between $\mathcal{P}$ and $\mathcal{V}$. And, $\mathcal{V}$ and $\mathcal{S}$ run in probabilistic polynomial time.
- $\mathbf{NISZK}$: Subset of $\mathbf{SZK}$, where the interaction is unidirectional, from $\mathcal{P}$ to $\mathcal{V}$.
- $\mathbf{NISZK_L}$: Subset of $\mathbf{NISZK}$ where $\mathcal{V}$ and $\mathcal{S}$ are restricted to logspace.

Directions to be explored

- Can we show that $\overline{\text{MCSP}}$ is hard for $\mathbf{NISZK}$ under $\mathbf{P/poly}$ reductions and for $\mathbf{NISZK_L}$ under projections?
  - This is what [All+21a] does for $\overline{\text{MKTP}}$
- Can we understand fundamental barriers to establishing equivalence of MCSP and MKTP and their variants?

Acknowledgments

We would like to thank our adviser, Dr. Eric Allender.

This work was carried out while the authors were participants in the 2021 DIMACS REU program. V.R. and S.S. were supported by CoSP, a project funded by European Union's Horizon 2020 research and innovation programme, grant agreement No. 823748, while N.S. was supported by NSF grant CCF-1852215.

References

Eric Allender, Rahul Ilango, and Neekon Vafa. "The non-hardness of approximating circuit size". In: *Theory of Computing Systems* (2020), pp. 1–20.

Eric Allender et al. "Cryptographic Hardness under Projections for Time-Bounded Kolmogorov Complexity". In: *Electron. Colloquium Comput. Complex.* 28 (2021).

Eric Allender et al. *One-way Functions and a Conditional Variant of MKTP*. 2021.

Valentine Kabanets and Jin-Yi Cai. "Circuit Minimization Problem". In: *Proceedings of the Thirty-Second Annual ACM Symposium on Theory of Computing*. STOC '00. Portland, Oregon, USA: Association for Computing Machinery, 2000, pp. 73–79. ISBN: 1581131844. DOI: 10.1145/335305.335314.