Minimum Circuit Size Problem

Rahul Ilango and Neekon Vafa
Advisor: Eric Allender
What is a boolean function?

An n-bit boolean function takes as input n zeros or ones and outputs zero or one.

Majority(A,B,C) is the function which takes three 0/1 inputs and

- Outputs 1 if two or three of the bits are 1
- Outputs 0 otherwise (if two or three of the bits are 0)

Truth Table as a string: “00010111”
What is a circuit?

\[(A \text{ AND } B) \text{ OR } (A \text{ AND } C) \text{ OR } (B \text{ AND } C)\]

Can be computed with 5 gates!
Circuit Complexity of a String

For a circuit C:

- \(tt(C)\) is the truth table of C, and
- \(size(C)\) is the number of gates of C.

For a binary string \(s\) of length \(2^n\), the circuit complexity of \(s\), \(CC(s)\), is the size of the smallest circuit which has truth table \(s\).

- \(CC(s) = \min \{size(C): tt(C) = s\}\)
- \(CC(00010111) \leq 5\)
MCSP (Minimum Circuit Size Problem)

MCSP = given truth table s and threshold i, is CC(s) ≤ i?

- CC(00010111) ≤ 5
- Seems difficult without brute forcing
P, NP, and MCSP

P = problems whose answers are easy to compute (e.g. is a graph connected?)

NP = problems whose answers are easy to check given some “evidence string” (e.g. can you travel n cities with $x$ of gas?)

- All problems in P are in NP
- MCSP is in NP
- We think $P \neq NP$
Research Direction 1

Is MCSP NP-intermediate?

We already know that if MCSP is in P, then most cryptography breaks.

Goal

If MCSP is hard within NP, then something “bad” happens.
MKTP

- For a Python program $P$ that takes no input, let $\text{cost}(P)$ be the length of the program as a string plus the time it takes to run
- $\text{KT}(x) =$ smallest cost of any program $P$ that prints $x$
- $\text{KT}(x)$ and $\text{CC}(x)$ are polynomially related

$\text{MKTP} =$ given string $x$ and threshold $i$, is $\text{KT}(x) \leq i$?

- Just like MCSP, we have MKTP in NP. Is MKTP NP-intermediate?
Research Direction 2

MCSP vs MKTP

- Stronger results have been shown for MKTP than MCSP

Goal

- Investigate differences between the two problems
Sources

https://medium.com/@bryanjordan/monkey-thinking-7241e9db353e

https://www.circuitlab.com/circuit/5n8tu7/majority-3-bit-circuit/
Acknowledgement

We thank our advisor Eric Allender and NSF grant CCF-1559855.