Minimum Circuit Size Problem

Advisor: Eric Allender

Karel Král, Michael Rudow, Veronika Slívová, Martin Töpfer.

June 5, 2016

Introduction

1. Complexity is the study of the amount of resources necessary to solve a problem. Examples include time and space.

Introduction

1. Complexity is the study of the amount of resources necessary to solve a problem. Examples include time and space.
2. The Minimum Circuit Size Problem MCSP is an example of a problem of unknown complexity.

Background

P and NP

1. P is the set of problems for which can be solved in polynomial time.
2. NP is the class of problems which can be solved in polynomial time with a polynomially long advice string.

Background

P and NP

1. P is the set of problems for which can be solved in polynomial time.
2. NP is the class of problems which can be solved in polynomial time with a polynomially long advice string.

Reducibility

We say that a problem A is reducible to another problem B if we can solve the problem A using a program that solves instances of B.

Background

P and NP

1. P is the set of problems for which can be solved in polynomial time.
2. NP is the class of problems which can be solved in polynomial time with a polynomially long advice string.

Reducibility

We say that a problem A is reducible to another problem B if we can solve the problem A using a program that solves instances of B.

NP-completeness

A problem is NP-Complete if every problem in NP reduces to it.
If any NP-Complete problem is in P then $P = NP$

MCSP

Circuit

A circuit is a mathematical model representing real computer circuits or boolean formulas. It minimally includes and, or and not gates, but may be extended to include others. It takes an input of length n and outputs 0 or 1.

MCSP

Circuit

A circuit is a mathematical model representing real computer circuits or boolean formulas. It minimally includes and, or and not gates, but may be extended to include others. It takes an input of length n and outputs 0 or 1.

MCSP

"The Minimum Circuit Size Problem (MCSP): Given a number i and a Boolean function f on n variables, represented by its truth table of size 2^n, determine if f has a circuit of size i." [**?**]

MCSP

Circuit

A circuit is a mathematical model representing real computer circuits or boolean formulas. It minimally includes and, or and not gates, but may be extended to include others. It takes an input of length n and outputs 0 or 1.

MCSP

"The Minimum Circuit Size Problem (MCSP): Given a number i and a Boolean function f on n variables, represented by its truth table of size 2^n, determine if f has a circuit of size i." [**?**]

MCSP is suspected to be an NP-Intermediate problem. This means it is not solvable in polynomial time and it is in NP, but it is also not NP-Hard.

RP, co-RP, ZPP and Oracles

RP, co-RP, ZPP

1. RP is the class of algorithms that run in polynomial time with small probability of rejecting instead of accepting.
2. co-RP is the class of algorithms that run in polynomial time with small probability of accepting instead of rejecting.
3. ZPP is the class of algorithms that run with no error in expected polynomial time.

Oracle classes

Class C^A contains languages which can be solved with an algorithm using computational power C and a subroutine to decide the problem A.

Graph Automorphism

Graph Automorphism Problem: Given Graph G is there a permutation σ such that edge $(u, v) \in G$ if and only if $(\sigma(u), \sigma(v)) \in \sigma(G)$.
This is another problem in NP which is not known to be in P and not known to be NP-Complete

Open problem

Is $GA \in ZPP^{MCSP}$?
Approach: prove $GA \in RP^{MCSP}$ and $GA \in co - RP^{MCSP}$.
To prove $GA \in RP^{MCSP}$, attempt to follow the technique used by Allender to prove GI (Graph Isomorphism) $\in RP^{MCSP}$ [**?**]
Given $GA \in RP^{MCSP}$, if $GA \in ZPP^{MCSP}$ then $GnA \in ZPP^{MCSP}$. Thus it is likely difficult to prove $GA \in co - RP^{MCSP}$

SZK

Interactive Proofs

The prover wants to persuade the verifier that something holds (US beer vs water).

Statistical Zero Knowledge

Interactive proof where the verifier learns statistically nothing about the solution (will not learn how to tell the drinks apart).

Kolmogorov Complexity

Kolmogorov complexity of a string x is the length of the shortest program that outputs x.

A string is Kolmogorov random if its complexity is at least its length.

Open Question (Allender)

Is there a significant subclass of SZK that reduces to Kolmogorov random strings?

Conclusion

1. MCSP is a difficult problem. It is been studied for decades and still defies provable classification with relation to P and being $NP - Hard$.
2. Through determining it's relative complexity compared to other problems of unknown complexity, the difficulty of MCSP can be more accurately determined.
3. The goal of this summer is to examine several open problems focusing on various reductions between MCSP and other possibly NP-Intermediate problems to provide evidence for future classification of MCSP.

TODO bibliography

Q/A

Thank you for your attention.