Minimum Circuit Size Problem

Azucena Garvia-Bosshard and Amulya Musipatla
Advisor: Eric Allender

P vs NP

P: set of problems that are easy to solve

NP: set of problems whose solutions are easy to verify

We think P≠NP (but don’t know how to prove it)

A language is NP-complete if it is at least as hard to solve as every other problem in NP.

NP-intermediate problem

A problem is NP-intermediate if it is

- in NP
- not in P
- not NP-complete

Theorem: P = NP if and only if there are no NP-intermediate problems.

Some possible NP-intermediate problems are the Minimum Circuit Size Problem, Integer Factorization and Graph Isomorphism.

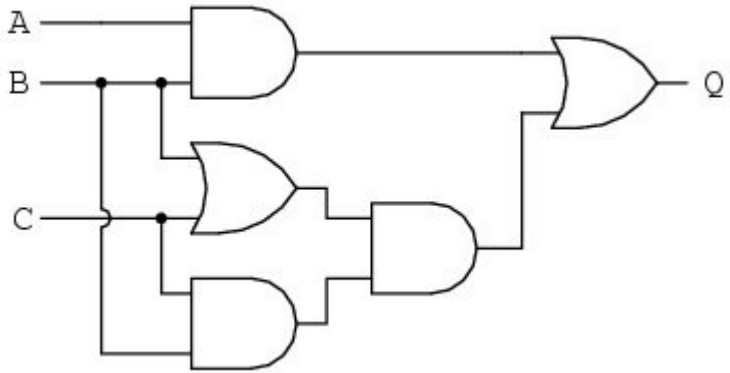
Boolean Functions

An n-bit boolean function takes in a string of 0s and 1s of length n and outputs a 0 or 1

Can be represented by a truth table

Input	Output
000	0
001	1
010	0
011	0
100	1
101	1
110	1
111	0

Boolean Circuits



Compute a boolean function. In the figure A, B, and C represent different bits of the input and Q is the output.

tt(C): truth table of the circuit C

size(C): measure of the size of the circuit C (# gates, # wires, etc)

Minimum Circuit Size Problem

The problem is to determine if a given Boolean function *f* on n variables has a circuit of size at most *i*, for some integer *i*.

MSCP = {(f, i) | f has a circuit of size at most i}

Our Research

Is MCSP NP-intermediate?

- We know MCSP is in NP
- If MCSP is in P, then cryptography breaks down.
- Want to show that if MCSP is NP-complete, something unexpected happens.

Thank you!

To our mentor Eric Allender and the NSF grant CCF-1852215

https://www.allaboutcircuits.com/textbook/digital/chpt-7/circuit-simplification-examples/