Lecture 1 - Circuit Minimization Problem

Lecture 1: Circuit Minimization Problem

Introduction

These notes abstract [@DBLP:conf/stoc/KabanetsC00], which sparked Western interest in the Minimum Circuit Size Problem (MCSP). This paper contributed a clear definition of MCSP, and formal evidence that resolving the complexity of MCSP will be *difficult.* Kabanets and Cai gave two kinds of evidence:

1. MCSP is Easy $\implies$ Circuit Lower Bounds & Derandomization
2. A "simple" proof that MCSP is NP-hard $\implies$ Circuit Lower Bounds

Roughly: "settling the complexity of MCSP is as hard as proving circuit lower bounds." Though theorists generally expect that circuit lower bounds are *true*, there is formal evidence that they will be hard to prove [@DBLP:journals/jcss/RazborovR97]. Thus, while we are free to conjecture that MCSP is NP-complete, we should expect that this will be difficult to prove.

Here we give: the basic definitions, a couple of results from each type of implication, and an updated discussion of the open problems from [@DBLP:conf/stoc/KabanetsC00].

Motivation

Valentine mentioned that he was interested in MCSP because of the problem's connection to pseudo-randomness. At the time, breakthrough hardness-to-randomness tradeoffs had just been completed [@DBLP:conf/stoc/ImpagliazzoW97]. The utility of access to hard truth tables was clear. Lacking circuit lower bounds, one motivation for studying MCSP is "can we at least recognize a hard truth-table when we see it?".

Definitions & Preliminaries

We begin by formally defining the problem.

Input: A Boolean function $f_n : \{0,1\}^n \to \{0,1\}$ given as a truth table (length 2^n) and a number $s_n \in \mathbb{N}$ (in binary).
Output: Is f_n computable by a Boolean circuit of size at most s_n?

MCSP is clearly in NP. The maximum circuit size for any function is $O(2^n/n)$, and we have 2^n bits of input. Therefore, an NP computation has time to guess and check every possible circuit of size less than or equal to s.

MCSP is linked pseudorandomness. But observe that it operates on the *truth tables* of functions. So, if we want MCSP to interact with a pseudorandom object, that object must be "local" in the following sense:

A function f is a local pseudorandom function against Λ if:

$$|\Pr_{g \sim G}[C^g = 1] - \Pr_{f \sim F_n}[C^f = 1]| < \epsilon$$

and the image of g is locally computable in Λ.

What if MCSP is Efficient?

If one could prove that MCSP is efficient, then

No Pseudorandomness

Maximum-Complexity Functions in E^{NP}

Derandomization

Conclusions & Discussion

This is a thing ss

References