Computational Complexity	October 1, 2018

Lecture 3 (Notes)

Lecturer: Ola Svensson *Scribes: Ola Svensson*

Disclaimer: These notes were written for the lecturer only and may contain inconsistent notation, typos, and they do not cite relevant works. They also contain extracts from the two main inspirations of this course:

1. The book *Computational Complexity: A Modern Approach* by Sanjeev Arora and Boaz Barak;
2. The course *http://theory.stanford.edu/ trevisan/cs254-14/index.html* by Luca Trevisan.

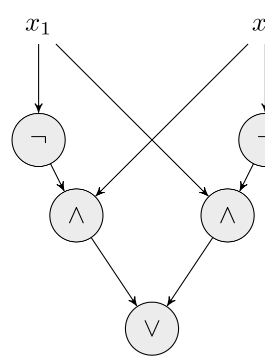
1 Introduction

- Recall last lecture: Non-determinism.
- Today: why diagonalization alone will not solve **P** vs **NP** question (see last lecture's notes) + beginning of circuits, non-uniform computation.

2 Circuits

A circuit C has n inputs and m outputs, and is constructed with AND, OR, and NOT gates. Each gate has fan-in 2 except the NOT gate which has fan-in 1. The out-degree can be any number. A circuit is *not* allowed to have any cycles.

Example 1 *A circuit C computing the XOR function, i.e., $C(x_1, x_2) = 1$ iff $x_1 \neq x_2$:*



Definition 1 (Size) *The size of a circuit C, denoted by $|C|$, is the number of its gates.*

- The size of the XOR circuit C above is 5.

Definition 2 (Circuit families and language recognition) *Let $T : \mathbb{N} \to \mathbb{N}$ be a function . A $T(n)$-*size circuit family *is a sequence of $\{C_n\}_{n\in\mathbb{N}}$ of Boolean circuits, where C_n has n inputs and a single output, and its size $|C_n| \leq T(n)$ for every n.*

We say that language L is in $\mathbf{SIZE}(T(n))$ *if there exists a $T(n)$-size circuit family $\{C_n\}_{n\in\mathbb{N}}$ such that for every $x \in \{0,1\}^n$, $x \in L \Leftrightarrow C_n(x) = 1$.*

Example 2 *For any $B \subseteq \{0,1\}^*$, the unary language $U_B = \{1^n :$ exists a string of length n in $B\}$ has a linear-sized circuit family. If $1^n \in U_B$ the circuit is simply a tree of AND gates and otherwise if $1^n \notin U_B$ then the circuit C_n is the trivial circuit that always outputs 0.*

Example 3 *The language* $\{\langle m, n, m+n\rangle : m, n \in \mathbb{Z}\}$ *also has linear-sized circuits that implement the grade-school algorithm for addition.*