Lesson 7: Boolean circuits part. I

Theme: Some classical results on boolean circuits.

Let $n \in \mathbb{N}$, where $n \geq 1$. An $n$-input Boolean circuit $C$ is a directed acyclic graph with $n$ source vertices (i.e., vertices with no incoming edges) and 1 sink vertex (i.e., vertex with no outgoing edge).

The source vertices are labelled with $x_1, \ldots, x_n$. The non-source vertices, called gates, are labelled with one of $\land, \lor, \neg$. The vertices labelled with $\land$ and $\lor$ have two incoming edges, whereas the vertices labelled with $\neg$ have one incoming edge. The size of $C$, denoted by $|C|$, is the number of vertices in $C$.

On input $w = x_1 \cdots x_n$, where each $x_i \in \{0, 1\}$, we write $C(w)$ to denote the output of $C$ on $w$, where $\land, \lor, \neg$ are interpreted in the natural way and 0 and 1 as false and true, respectively.

We refer to the in-degree and out-degree of vertices in a circuit as fan-in and fan-out, respectively. In our definition above, we require fan-in 2.

- A circuit family is a sequence $\{C_n\}_{n \in \mathbb{N}}$ such that every $C_n$ has input $n$ inputs and a single output.
  To avoid clutter, we write $\{C_n\}$ to denote a circuit family.
- We say that $\{C_n\}$ decides a language $L$, if for every $n \in \mathbb{N}$, for every $w \in \{0, 1\}^n$, $w \in L$ if and only if $C_n(w) = 1$.
- We say that $\{C_n\}$ is of size $T(n)$, where $T : \mathbb{N} \to \mathbb{N}$ is a function, if $|C_n| \leq T(n)$, for every $n \in \mathbb{N}$.

We define the following class.

$$P_{/poly} \overset{\text{def}}{=} \{L : L \text{ is decided by } \{C_n\} \text{ of size } q(n) \text{ for some polynomial } q(n)\}$$

That is, the class of languages decided by a circuit family of polynomial size.

Remark 7.1 It is not difficult to show that every unary language $L$ is in $P_{/poly}$. Thus, $P_{/poly}$ contains some undecidable language.

Definition 7.2 A circuit family $\{C_n\}$ is $P$-uniform, if there is a polynomial time DTM that on input $1^n$, outputs the description of the circuit $C_n$.

Theorem 7.3 A language $L$ is in $P$ if and only if it is decided by a $P$-uniform circuit family.

Theorem 7.4 (Karp and Lipton 1980) If $NP \subseteq P_{/poly}$, then $PH = \Sigma_2^p$.

Theorem 7.5 (Meyer 1980) If $EXP \subseteq P_{/poly}$, then $EXP = \Sigma_2^p$.

Theorem 7.6 (Shannon 1949) For every $n > 1$, there is a function $f : \{0, 1\}^n \to \{0, 1\}$ that cannot be computed by a circuit of size $2^n/(10n)$.
The classes $\textbf{NC}$ and $\textbf{AC}$. For a circuit $C$, the \textit{depth} of $C$ is the length of the longest directed path from an input vertex to the output vertex. For a function $T : \mathbb{N} \to \mathbb{N}$, we say that a circuit family \{${C_n}$\} has depth $T(n)$, if for every $n$, the depth of $C_n$ is $\leq T(n)$.

For every $i$, the classes $\textbf{NC}^i$ and $\textbf{AC}^i$ are defined as follows.

- A language $L$ is in $\textbf{NC}^i$, if there is $f(n) = \text{poly}(n)$ such that $L$ is decided by a circuit family of size $f(n)$ and depth $O(\log^i n)$.
- The class $\textbf{AC}^i$ is defined analogously, except that gates in the circuits are allowed to have unbounded fan-in.

The classes $\textbf{NC}$ and $\textbf{AC}$ are defined as follows.

$$\textbf{NC} \overset{\text{def}}{=} \bigcup_{i \geq 0} \textbf{NC}^i \quad \text{and} \quad \textbf{AC} \overset{\text{def}}{=} \bigcup_{i \geq 0} \textbf{AC}^i$$

Note that $\textbf{NC}^i \subseteq \textbf{AC}^i \subseteq \textbf{NC}^{i+1}$.

*Here we take the length of a path as the number of edges in it.*