# Lesson 6: Boolean circuits

**Theme:** Some classical results on boolean circuits.

Let $n \in \mathbb{N}$, where $n \geqslant 1$. 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 $\wedge, \vee, \neg$. The vertices labelled with $\wedge$ and $\vee$ 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 $\wedge, \vee, \neg$ are interpreted in the natural way and 0 and 1 as $\mathsf{false}$ and $\mathsf{true}$, 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 $|C_n| \leqslant T(n)$, for every $n \in \mathbb{N}$.

We define the following class.

$$\mathbf{P}_{/\mathsf{poly}} \stackrel{\mathsf{def}}{=} \big\{L : L \text{ is decided by } \{C_n\} \text{ of size } q(n) \text{ for some polynomial } q(n)\big\}$$

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

**Remark 6.1** It is not difficult to show that *every* unary language $L$ is in $\mathbf{P}_{/\mathsf{poly}}$. Thus, $\mathbf{P}_{/\mathsf{poly}}$ contains some undecidable language.

**Definition 6.2** A circuit family $\{C_n\}$ is $\mathbf{P}$*-uniform*, if there is a polynomial time DTM that on input $1^n$, output the description of the circuit $C_n$.

**Theorem 6.3** *A language $L$ is in $\mathbf{P}$ if and only if it is decided by a $\mathbf{P}$-uniform circuit family.*

**Theorem 6.4 (Karp and Lipton 1980)** *If $\mathbf{NP} \subseteq \mathbf{P}_{/\mathsf{poly}}$, then $\mathbf{PH} = \mathbf{\Sigma}_2^p$.*

**Theorem 6.5 (Meyer 1980)** *If $\mathbf{EXP} \subseteq \mathbf{P}_{/\mathsf{poly}}$, then $\mathbf{EXP} = \mathbf{\Sigma}_2^p$.*

**Theorem 6.6 (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 NC and AC.** For a circuit $C$, the *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 $\leqslant T(n)$.

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

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

The classes **NC** and **AC** are defined as follows.

$$\mathbf{NC} \stackrel{\mathsf{def}}{=} \bigcup_{i \geqslant 0} \mathbf{NC}^i \qquad \text{and} \qquad \mathbf{AC} \stackrel{\mathsf{def}}{=} \bigcup_{i \geqslant 0} \mathbf{AC}^i$$

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

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