# Lesson 7: Boolean circuits

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

## 1 Some basics

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 7.1** 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 7.2** 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 7.3** *A language $L$ is in $\mathbf{P}$ if and only if it is decided by a $\mathbf{P}$-uniform circuit family.*

**Theorem 7.4 (Karp and Lipton 1980)** *If $\mathbf{NP} \subseteq \mathbf{P}_{/\mathsf{poly}}$, then $\mathbf{PH} = \mathbf{\Sigma}_2^p$.*

**Theorem 7.5 (Meyer 1980)** *If $\mathbf{EXP} \subseteq \mathbf{P}_{/\mathsf{poly}}$, then $\mathbf{EXP} = \mathbf{\Sigma}_2^p$.*

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

# 2 The switching lemma – Decision tree version

This section is based on Sect. 13.1 in N. Immerman's textbook "Descriptive Complexity" (1998). See also P. Beame's note "A switching lemma primer" (1994).

## 2.1 Some useful notations and definitions

We will consider circuits with unbounded fan-in. We will often use the terms "boolean formula" and "boolean function" interchangeably. Recall that a literal is either a (boolean) variable or its negation.

A *term* is a conjunction of some literals. The *length* of a term is the number of literals in it. A *$k$-term* is a term of length $k$. A formula is a DNF formula if it is a disjunction of terms. It is $k$-DNF, if all its terms have length at most $k$.

**Decision tree.** Let $F$ be a boolean function with variables $x_1, \ldots, x_n$. A *decision tree* of $F$ is a tree constructed inductively as follows.

- If $F$ already evaluates to a constant 0 or 1, the decision tree has only one node labelled with 0 or 1, respectively.
- If $F$ is not a constant, its decision tree has a root with two children, where the left and right children are decision trees for $F[x_1 \mapsto 0]$ and $F[x_1 \mapsto 1]$, respectively.

  Here $F[x_1 \mapsto b]$ denotes the resulting formula obtained by assigning $x_1$ with $b$.

Note that a decision tree depends on the ordering of the variables $x_1, \ldots, x_n$.

**Canonical decision tree for DNF formulas.** Let $F = C_1 \vee C_2 \vee \cdots \vee C_m$ be a DNF formula, i.e., each $C_i$ is a term. The *canonical decision tree* of $F$, denoted by $\mathcal{T}(F)$, is the decision tree obtained with the variables being ordered as follows: All the variables in $C_1$ appear first, followed by all the variables in $C_2$ (which haven't appeared yet), and so on. Let $\mathsf{depth}(\mathcal{T}(F))$ denote the depth of the canonical decision tree of $F$.

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

**Restriction.** Let $F$ be a formula with variables $x_1, \ldots, x_n$. A *restriction* (on $x_1, \ldots, x_n$) is a function $\rho : \{x_1, \ldots, x_n\} \to \{0, 1, *\}$. Intuitively, $\rho(x_i) = *$ means variable $x_i$ is not assigned. We denote by $F|_\rho$ the resulting formula where we assign the variables in $F$ according to $\rho$. Note that if the formula $F$ is DNF, the formula $F|_\rho$ is also DNF. For $\ell \leqslant n$, $\mathcal{R}_n^\ell$ denotes the set of restrictions (on $n$ variables) where exactly $\ell$ variables are unassigned.

For two restrictions $\rho_1$ and $\rho_2$ whose sets of assigned variables are disjoint, we denote by $\rho_1\rho_2$ the restriction obtained by combining both restrictions. That is, for every variable $x$, if $x$ is assigned according to $\rho_1$ (or $\rho_2$), then $\rho_1\rho_2$ assigns $x$ according to $\rho_1$ (or $\rho_2$).

## 2.2 The switching lemma

**Lemma 7.7 (Switching lemma – Håstad 1986)** *Let $F$ be a $k$-DNF formula with $n$ variables. For every $s \geqslant 0$ and every $p \leqslant 1/7$, the following holds.*

$$\frac{|\{\rho \in \mathcal{R}_n^{pn} \ : \ \mathsf{depth}(\mathcal{T}(F|_\rho)) \geqslant s\}|}{|\mathcal{R}_n^{pn}|} \quad < \quad (7pk)^s \tag{1}$$

One can also write Eq. (1) as $\mathbf{Pr}_{\rho \in \mathcal{R}_n^{pn}}[\mathsf{depth}(\mathcal{T}(F|_\rho)) \geqslant s] < (7pk)^s$. Here $\mathbf{Pr}_{\rho \in \mathcal{R}_n^{pn}}[\mathcal{E}]$ denotes the probability of event $\mathcal{E}$ where $\rho$ is randomly chosen from $\mathcal{R}_n^{pn}$.

Let $\mathsf{stars}(k, s)$ be the set that contains a sequence $\bar{Z} \stackrel{\mathsf{def}}{=} (Z_1, \ldots, Z_t)$ where $\sum_{i=1}^t |Z_i| = s$ and each $Z_i$ is a non-empty subset of $\{1, \ldots, k\}$. When $s = 0$, we define $\mathsf{stars}(k, s)$ to be $\{\varepsilon\}$, where $\varepsilon$ denotes the "empty sequence". That is, $|\mathsf{stars}(k, 0)| = 1$.

**Lemma 7.8** *For every $k, s \geqslant 1$, $|\mathsf{stars}(k, s)| \leqslant \gamma^s$, where $\gamma$ is such that $(1 + \frac{1}{\gamma})^k = 2$. Hence, $|\mathsf{stars}(k, s)| < (k/\ln 2)^s$.*

**Proof.** The proof is by induction on $s$. Base case $s = 0$ is trivial.

For the induction hypothesis, we assume that the lemma holds for every $s' < s$. The induction step is as follows. Observe that if $Z_0$ is a non-empty subset of $\{1, \ldots, k\}$ and $\bar{Z} \in \mathsf{stars}(k, s - |Z_0|)$, then $(Z_0, \bar{Z}) \in \mathsf{stars}(k, s)$. From here, we have:

$$\begin{aligned}
|\mathsf{stars}(k, s)| \ = \ \sum_{i=1}^{\min(k,s)} \binom{k}{i} |\mathsf{stars}(k, s - i)| \ & \leqslant \ \sum_{i=1}^{k} \binom{k}{i} |\mathsf{stars}(k, s - i)| \\
& \leqslant \ \sum_{i=1}^{k} \binom{k}{i} \gamma^{s-i} \\
& = \ \gamma^s \sum_{i=1}^{k} \binom{k}{i} (1/\gamma)^i \\
& = \ \gamma^s \big((1 + 1/\gamma)^k - 1\big) \\
& = \ \gamma^s
\end{aligned}$$

∎

**Proof of Switching lemma:** Let $F$ be a $k$-DNF formula with $n$ variables. Let $s \geqslant 0$ and $p \leqslant 1/7$. Let $\ell = pn$. Let $X$ be the set of restrictions $\rho$ such that $\mathsf{depth}(\mathcal{T}(F|_\rho)) \geqslant s$. We will show that there is an injective function $\xi$:

$$\xi \ : X \ \to \ \mathcal{R}^{\ell - s} \times \mathsf{stars}(k, s) \times \{0, 1\}^s$$

The existence of $\xi$ implies $|X| \leqslant |\mathcal{R}^{\ell-s}| \cdot |\mathsf{stars}(k,s)| \cdot 2^s$ and Switching lemma follows immediately from Lemma 7.8 and the fact that $|\mathcal{R}_n^\ell| = \binom{n}{\ell} 2^{n-\ell}$.

Let $F \stackrel{\mathsf{def}}{=} C_1 \vee C_2 \vee \cdots$, where each $C_i$ is a term of length at most $k$. Let $\rho \in X$, i.e., $\mathsf{depth}(\mathcal{T}(F|_\rho)) \geqslant s$. Consider the lexicographically first branch in $\mathcal{T}(F|_\rho)$ with length $\geqslant s$ and let $b$ be the first $s$ steps in this branch. To define $\xi(\rho)$, we do the following.

- Let $C_{i_1}$ be the first term that is not set to 0 in $F|_\rho$.

  Let $V_1$ be the set of variables in $C_{i_1}|_\rho$. (Note that by the definition of the canonical decision tree, this means the variables in $V_1$ are assigned at the beginning of $\mathcal{T}(F|_\rho)$.)

  Let $a_1$ be the (unique) assignment that makes $C_{i_1}|_\rho$ true.

  Let $b_1$ be the "initial" assignment of $b$ that assigns variables in $V_1$.
  (If $b$ ends before all the variables in $V_1$ is used, let $b_1 = b$ and "shorten" $a_1$ so that both $a_1$ and $b_1$ assign the same set of variables.)

  Let $S_1 \subseteq \{1, \ldots, k\}$ be the set of index $j$ where the $j^{\text{th}}$ variable in $C_{i_1}$ is assigned by $a_1$. (Note that from the term $C_{i_1}$ and the set $S_1$, we can reconstruct $a_1$.)

- Repeat the above process but with $b \setminus b_1$, and we obtain $a_2$, $b_2$ and the set $S_2$,

Performing the process above, we obtain $a_1 \cdots a_t$, $b_1 \cdots b_t$ and $(S_1, \ldots, S_t)$. Note that $b = b_1 \cdots b_t$. Let $a$ denote $a_1 \cdots a_t$. Note also that the number of variables assigned by both $a$ and $b$ is exactly $s$. Thus, the sum $|S_1| + \cdots + |S_t| = s$, and hence, $(S_1, \ldots, S_t) \in \mathsf{stars}(k,s)$.

Let $\delta : \{1, \ldots, s\} \to \{0,1\}$ be a function defined as follows.

$$\delta(j) \stackrel{\mathsf{def}}{=} \begin{cases} 1, & \text{if } a \text{ and } b \text{ assign the same value to the variable in the } j^{\text{th}} \text{ step} \\ 0, & \text{otherwise} \end{cases}$$

Note that $\delta$ can be viewed as a 0-1 string of length $s$.

Now we define the mapping $\xi$ as follows.

$$\xi(\rho) \stackrel{\mathsf{def}}{=} (\rho a, (S_1, \ldots, S_t), \delta)$$

where $a$, $(S_1, \ldots, S_t)$ and $\delta$ are defined as above.

We need to show that $\xi$ is injective. We will show that if $(\rho', (S_1, \ldots, S_t), \delta)$ is in the range of $\xi$, we can construct a unique $\rho$ such that $\xi(\rho) = \rho'$. Note that if $(\rho', (S_1, \ldots, S_t), \delta)$ is in the range of $\xi$, there is $a_1 \cdots a_t$ such that $\rho' = \rho a$ and $(S_1, \ldots, S_t)$ and $\delta$ satisfy the property imposed by the definition of $\xi$ above. Thus, to reconstruct $\rho$, it suffices to reconstruct $a_1 \cdots a_t$.

We denote $\rho'$ by $\rho a_1 \cdots a_t$ for some $a_1 \cdots a_t$ (which at this point is not known yet). We will construct $a_1, \ldots, a_t$ by doing the following.

- Find out the term $C_{i_1}$ which is the first term in $F$ that evaluates to 1 under $\rho'$.

  From $C_{i_1}$ and $S_1$, we reconstruct $a_1$.

  From $a_1$ and $\delta$, we reconstruct $b_1$.

- Repeat the same process but replacing $\rho'$ with $(\rho' \setminus a_1) b_1$. (Here note that $(\rho' \setminus a_1) b_1$ is the same as $\rho b_1 a_2 \cdots a_t$)

  From this step, we figure out $a_2$ and $b_2$.

We repeat the same process until we figure out all $a_1, \cdots, a_t$ and hence the restriction $\rho$. This completes the proof of Lemma 7.7. ∎

# 3 Applications of the switching lemma

By the equivalence $p_1 \wedge \cdots \wedge p_m \equiv \neg(\neg p_1 \vee \cdots \vee \neg p_m)$, we can transform a circuit $C$ into another circuit $C'$ that uses only $\neg$ and $\vee$ gates. Moreover, $\mathsf{depth}(C') \leqslant 3 \cdot \mathsf{depth}(C)$. In this section we always assume that circuits only use $\neg$ and $\vee$ gates.

Note that every gate $g$ in a circuit defines a boolean formula. Abusing the notation, we will often treat every gate as a formula too. For every vertex $u$ in a circuit $C$, we define the height of $u$, denoted by $\mathsf{height}(u)$, as follows.

- The height of a source vertex (i.e., the input vertex) is 0.
- The height of a gate vertex $u$ is the maximum of $\mathsf{height}(v) + 1$, where $v$ ranges over all edges $(u, v)$ in $C$.

So, a circuit of depth $d$ has vertices of height from 0 to $d$.

In the following, log has base 2.

**Lemma 7.9** *Let $C$ be a circuit with $n$ variables, size $m$ and depth $d$. For every $1 \leqslant j \leqslant d$, let $n_j \stackrel{\mathsf{def}}{=} \frac{n}{14(14\log m)^{j-1}}$. Assume that $\log m > 1$. Then, the following holds.*

*For every $1 \leqslant j \leqslant d$, there is a restriction $\rho_j \in \mathcal{R}_n^{n_j}$ such that for every gate $f$ of height $j$ in $C$, the formula $f|_{\rho_j}$ has a decision tree with height $< \log m$.*

**Proof.** The proof is by induction on $j$. The base case is $j = 1$, where $n_1 \stackrel{\mathsf{def}}{=} n/14$. We randomly choose (with equal probability) a restriction $\rho$ from $\mathcal{R}_n^{n_1}$. For a gate $f$ of height 1, let $\mathcal{E}_f$ denote the event that "$\mathsf{depth}(\mathcal{T}(f|_\rho)) \geqslant \log m$." Let $\mathcal{E}$ denote the event that "there is a gate $f$ of height 1 such that $\mathsf{depth}(\mathcal{T}(f|_\rho)) \geqslant \log m$."

We will first show that $\mathbf{Pr}_{\rho\in\mathcal{R}_n^{n_1}}[\mathcal{E}_f] < 1/m$, for every gate $f$ of height 1. Let $f$ be a gate of height 1. If $f$ is a $\neg$-gate, then the depth of its decision tree is 1. Since $\log m > 1$, we have:

$$\mathbf{Pr}_{\rho\in\mathcal{R}_n^{n_1}}[\mathcal{E}_f] \;=\; 0 \;<\; 1/m$$

If $f$ is an $\vee$-gate, we can view $f$ as 1-DNF, i.e., every term has length 1. By Lemma 7.7 where $p = 1/14$, $k = 1$ and $s = \log m$, we have:

$$\mathbf{Pr}_{\rho\in\mathcal{R}_n^{n_1}}[\mathcal{E}_f] \;<\; (7 \cdot (1/14) \cdot 1)^{\log m} \;=\; (1/2)^{\log m} \;=\; 1/m$$

Then,

$$\mathbf{Pr}_{\rho\in\mathcal{R}_n^{n_1}}[\mathcal{E}] \;=\; \mathbf{Pr}_{\rho\in\mathcal{R}_n^{n_1}}\Big[\bigcup_{f \text{ has height } 1} \mathcal{E}_f\Big] \;\leqslant\; \sum_{f \text{ has height } 1} \mathbf{Pr}_{\rho\in\mathcal{R}_n^{n_1}}[\mathcal{E}_f] \;<\; m \cdot (1/m) \;=\; 1$$

This means $\mathbf{Pr}_{\rho\in\mathcal{R}_n^{n_1}}[\overline{\mathcal{E}}] > 0$, which means there is a restriction $\rho \in \mathcal{R}_n^{n_1}$ such that for all gate $f$ of height 1, $\mathsf{depth}(\mathcal{T}(f|_\rho)) < \log m$, i.e., $f|_\rho$ has a decision tree with depth $< \log m$.

For the induction hypothesis, we assume Lemma 7.9 holds for $j-1$. Let $\rho_0 \in \mathcal{R}_n^{n_{j-1}}$ be a restriction such that every gate $g$ of height $j-1$ has decision tree with depth $< \log m$. Applying $\rho_0$ on all gates of height $j-1$, we can view each gate of height $j-1$ as DNF where each term has length $< \log m$.

Similar to above, we randomly choose a restriction $\rho$ from $\mathcal{R}_{n_{j-1}}^{n_j}$. For a gate $f$ of height $j$, let $\mathcal{E}'_f$ denote the event that "every decision tree of $f|_{\rho_0\rho}$ has depth $\geqslant \log m$." Let $\mathcal{E}'$ denote the event that "there is a gate $f$ of height $j$ such that every decision tree of $f|_{\rho_0\rho}$ has depth $\geqslant \log m$."

We will show that $\mathbf{Pr}_{\rho\in\mathcal{R}^{n_j}_{n_{j-1}}}[\mathcal{E}'_f] < 1/m$, for every gate $f$ of height $j$. Let $f$ be a gate of height $j$. If $f$ is a $\neg$-gate, let $f = \neg g$, where $g$ is of height $j-1$. Since $g|_{\rho_0}$ has decision tree with depth $< \log m$, so does $f|_{\rho_0}$. Thus,

$$\mathbf{Pr}_{\rho\in\mathcal{R}^{n_j}_{n_{j-1}}}[\mathcal{E}'_f] \;=\; 0 \;<\; 1/m$$

If $f$ is an $\vee$-gate, we can view $f$ as $k$-DNF, where $k = \log m$. By Lemma 7.7 with $p = 1/(14\log m)$, $k = \log m$ and $s = \log m$, we have:

$$\mathbf{Pr}_{\rho\in\mathcal{R}^{n_j}_{n_{j-1}}}[\mathsf{depth}(\mathcal{T}(f|_{\rho_0\rho})) \geqslant \log m] \;<\; (7\cdot\frac{1}{14\log m}\cdot\log m)^{\log m} \;=\; (1/2)^{\log m} \;=\; 1/m$$

Now, note that:

$$\mathbf{Pr}_{\rho\in\mathcal{R}^{n_j}_{n_{j-1}}}[\mathcal{E}'_f] \;\leqslant\; \mathbf{Pr}_{\rho\in\mathcal{R}^{n_j}_{n_{j-1}}}[\mathsf{depth}(\mathcal{T}(f|_{\rho_0\rho})) \geqslant \log m]$$

Thus,

$$\mathbf{Pr}_{\rho\in\mathcal{R}^{n_j}_{n_{j-1}}}[\mathcal{E}'_f] \;<\; 1/m$$

Applying similar argument as above, we obtain:

$$\mathbf{Pr}_{\rho\in\mathcal{R}^{n_j}_{n_{j-1}}}[\mathcal{E}'] \;<\; 1$$

Hence, there is a restriction $\rho \in \mathcal{R}^{n_j}_{n_{j-1}}$ such that for every gate $f$ of height $j$, $f|_{\rho_0\rho}$ has a decision tree with depth $< \log m$. Now, $\rho_0\rho \in \mathcal{R}^{n_j}_{n}$. This completes the proof of Lemma 7.9. ∎

Consider the following language $\mathsf{PARITY} \subseteq \{0,1\}^*$.

$$\mathsf{PARITY} \;\stackrel{\mathsf{def}}{=}\; \{w : \text{the number of 1's in } w \text{ is odd}\}$$

Obviously, it can be viewed as a family of boolean functions $\{f_n\}_{n\in\mathbb{N}}$, where each $f_n$ has $n$ variables $x_1,\ldots,x_n$ and $f_n(x_1,\ldots,x_n) \stackrel{\mathsf{def}}{=} \sum_{i=1}^n x_i \pmod 2$.

Applying Lemma 7.9, we immediately obtain that PARITY is not in $\mathbf{AC}^0$.

**Theorem 7.10 (Furst, Saxe and Sipser 1981, Ajtai 1983, Yao 1985)** $\mathsf{PARITY} \notin \mathbf{AC}^0$.