1 Introduction

H˚astad’s Switching Lemma is one of the main tools for dealing with constant-depth circuit, consisting of AND, OR and NOT gates with unbounded fan-in are allowed (no XOR gates). Roughly speaking, the lemma says, under a random restriction, an AND of (arbitrarily many) small ORs can be written as an OR of small ANDs. To see how this lemma works, let us first arrange the circuit in standard form satisfying the followings.

- Push all the NOT gates to the bottom layer, which contains literals \( x_1, \overline{x_1}, \ldots, x_n, \overline{x_n} \). This is possible because of the De Morgan’s laws: \( \neg(\neg A \lor B) = \neg A \land \neg B \) and \( \neg(\neg A \land B) = \neg A \lor \neg B \).

- Same layer contains the same type of gates, and two adjacent layers have different types of gates. In other words, AND, OR gates are alternating between layers. This can be done by merging the same type of gates in adjacent layers.

- The inputs of any gate at the \( i \)th layer are outputs of gates in the \( (i + 1) \)th layer. This can be done by adding some dummy gates, either AND or OR, with fan-in 1. The first two transformations will not increase the size (= number of gates) of the circuit, and this one will increase the size of the circuit by at most a multiplicative factor \( d \), where \( d \) is the depth of the circuit.

Without loss of generality, assume the circuit is in standard form. A lot of lower bound argument by directly applying switching lemma works as follows. Suppose we want to prove circuit lower bound for some explicit function \( f \).
Assume for contradiction that $f$ can be computed by depth $d$ size $S$ circuit, which can be artificially viewed as a depth $d+1$ size $S$ circuit with bottom fan-in 1. We will apply switching lemma $d-1$ times, and each time the second bottom layer will switch from AND of ORs to OR of ANDs or the other way so that we can reduce the depth by 1 by merging the second bottom layer with the third bottom layer. Finally, we will end up with a depth 2 circuit computing $f|_{\rho}$ with specific bottom fan-in $t$, where

$$\rho = \rho_1 \circ \rho_2 \circ \ldots \circ \rho_{d-2},$$

where $\rho$ is the random restriction we have applied. However, $f|_{\rho}$ is supposed to be uncomputable by depth 2 circuit with bottom fan-in $t$, which is a contradiction! A lot of constant depth circuit lower bounds fall into this argument, which is sometimes called depth reduction argument.

Håstad comes up with this lemma and uses it to prove an almost tight (up to a multiplicative constant in the exponent) lower bound on the size of constant depth circuit computing parity function. Besides that, there are many other nice applications of Håstad’s Switching Lemma.

It is worth mentioning that there are other forms of the switching lemma, and some cover different range of parameters. However, Håstad’s Switching Lemma is usually considered as the most powerful one, and for the author, it is still mysterious why many (almost) tight results can be deduced from it.

## 2 The Lemma

Before stating the lemma, we need a few definitions.

**Definition 2.1 (Conjunctive Normal Form).** $t$-CNF (Conjunctive Normal Form) is an AND of clauses of width at most $t$. A clause of width $t$ is an OR of $t$ literals. For example, $x_1 \lor x_2 \lor x_4$ is a clause of width 3, and $(x_1 \lor x_2) \land (\overline{x_1} \lor \overline{x_2})$ is 2-CNF.

**Definition 2.2 (Disjunctive Normal Form).** $s$-DNF (Disjunctive Normal Form) is an OR of disjuncts of width at most $s$, where a disjunct of width $s$ is an AND of $s$ literals.

Now we define random restriction, which is a key concept in circuit complexity.
**Definition 2.3.** A restriction $\rho$ is a mapping from \( \{x_1, \ldots, x_n\} \) to \( \{0, 1, *\} \). A random restriction \( \rho \in R(p, q) \), \( 0 \leq p, q \leq 1 \), is a random restriction such that
\[
\Pr_{\rho}[\rho(x_i) = *] = p,
\Pr_{\rho}[\rho(x_i) = 0] = (1 - p)q,
\Pr_{\rho}[\rho(x_i) = 1] = (1 - p)(1 - q),
\]
independently, for each \( i \).

Now, we are ready to state Håstad’s Switching Lemma.

**Lemma 2.4** (Håstad’s Switching Lemma). Let \( f \) be some Boolean function which can be written as some \( t \)-CNF. Then, for any integer \( s \geq 1 \), any \( p \in [0, 1] \),
\[
\Pr_{\rho \in R(p,1/2)}[f|_\rho \text{ is not } s\text{-DNF}] \leq (5pt)^s.
\]
Here, \( f|_\rho \) is not \( s\text{-DNF} \) means \( f|_\rho \) can not be written as \( s\text{-DNF} \).

**Exercise 2.5.** Prove that you can “switch” CNF and DNF in the above lemma; that is, assuming Håstad’s Switching Lemma, prove for any \( t\)-DNF \( f \), \( \Pr_{\rho \in R(p,1/2)}[f|_\rho \text{ is not } s\text{-CNF}] \leq (5pt)^s \), or vice versa.

**Remark 2.6.** Note that the probability \( (5pt)^s \) does not depends on the number of variables!

**Remark 2.7.** There are variants of Håstad’s Switching Lemma for different kinds of random restrictions, which are tailored for some specific function we are interested in. Roughly speaking, switching lemma works as long as a random restriction is likely to kill a clause (For some CNF containing clause \( C \), if \( C|_\rho = 0 \), then the whole CNF will be 0; if \( C|_\rho = 1 \), then \( C \) will simply disappear).

On the other hand, the concept of (random) restriction is necessary. Consider the threshold function \( \text{Th}_k^n(x) \), which is 1 if and only if \( x_1 + x_2 + \ldots + x_n \geq k \). It is easily seen that \( \text{Th}_k^n(x) \) can be written as \( k\text{-DNF} \), and \( (n - k)\text{-CNF} \), but not \( (n - k - 1)\text{-CNF} \). If \( k \) is fixed and \( n \) goes to infinity, this example shows, in general, \( t\text{-CNF} \) can not be written as \( s\text{-DNF} \), where \( s = s(t) \) only depends on \( t \).
3 Upper Bound of Parity

Definition 3.1. Let $\text{PAR}_n(x_1, \ldots, x_n)$ denote the parity function in $n$ variables, that is, $\text{PAR}_n(x_1, \ldots, x_n) = 1$ if and only if $\sum_i x_i \equiv 1 \pmod{2}$.

For depth 2 circuit,

$$\text{PAR}_n(x) = \bigvee_{y \in \{0,1\}^n : \text{PAR}_n(y) = 1} \left( \bigwedge_{i: y_i = 1} x_i \wedge \bigwedge_{i: y_i = 0} \overline{x_i} \right),$$

or

$$\text{PAR}_n(x) = \bigwedge_{y \in \{0,1\}^n : \text{PAR}_n(y) = 0} \left( \bigvee_{i: y_i = 0} x_i \vee \bigvee_{i: y_i = 1} \overline{x_i} \right),$$

where both have size $2^{n-1} + 1$, which in fact are the optimal.

For depth 3, observe that

$$\text{PAR}_n(x_1, \ldots, x_n) = \text{PAR}_m(\text{PAR}_m(y_1), \ldots, \text{PAR}_m(y_m)),$$

where $m = \sqrt{n}$, and $y_1 = (x_1, \ldots, x_m)$, $y_2 = (x_{m+1}, \ldots, x_{2m})$, etc. For the $\text{PAR}_m$ outside, write it as $m$-CNF of size $2^{m-1} + 1$; and for the $\text{PAR}_m$ inside, write it as $m$-DNF of size $2^{m-1} + 1$, which is a depth 4 circuit of size $(1 + m)(2^{m-1} + 1) \leq n2^{\sqrt{n}}$. To make it depth 3, simply merge two layers in the middle, which are both OR gates, and the size will not increase.

Using the same argument, it is not difficult to prove (we leave it as an exercise):

Theorem 3.2. For any $d \geq 2$, $\text{PAR}_n$ can be computed by depth $d$ circuit of size at most $n2^{n/(d-1)}$.

If the depth $d \geq \log n$, it turns out there exists linear size circuit computing $\text{PAR}_n$.

Theorem 3.3. $\text{PAR}_n$ can be computed by depth $\lceil \log n \rceil$ circuit of size $2n - 1$.

Proof. Build a complete binary tree with $n$ leaves, corresponding to variables $x_1, x_2, \ldots, x_n$; all the non-leaf nodes are $\text{XOR} = \text{PAR}_2$ gates. Since the depth of the binary tree is $d = \lceil \log n \rceil$, the number of non-leaf nodes is

$$(n - 2^{d-1}) + 2^{d-2} + 2^{d-3} + \ldots + 1 = n - 1$$

4
For each XOR gate, we need 2 gates to implement (recall that XOR can be either written as 2-CNF or 2-DNF, and apply the gates merging technique again) except for the top gate (3 gates are needed). The total number of gates is $2(n - 1) + 1 = 2n - 1$.

In the next section, we will prove a $n2^{\Omega(n^{1/(d-1)})}$ lower bound for $\text{PAR}_n$, which matches the upper bound up to a multiplicative constant in the exponent assuming Håstad’s Switching Lemma. After proving the upper bound, hopefully, the readers will appreciate the lower bound better.

## 4 Lower Bound of Parity

In this section, we will prove the following theorem using switching lemma.

**Theorem 4.1.** For any $d \geq 2$, $\text{PAR}_n$ cannot be computed by depth-$d$ size-$2^{cn^{1/(d-1)}}$ circuit (when $n$ is sufficiently large), where $c$ is a reasonable constant, say $1/11$.

**Proof.** Assume for contradiction that $\text{PAR}_n$ can be computed by some depth-$d$ size-$S$ circuit $C(x)$, where $S < 2^{cn^{1/(d-1)}}$, and the constant $c$ will be determined later. Without loss of generality, assume our circuit $C(x)$ is already in standard form (depth $d$ size $S$ circuit can be transformed to standard form of depth $d$ size $dS$, for which we only need to make the constant $c$ slightly larger, that is, $c + \epsilon$ for any $\epsilon > 0$).

**First step.** View $C(x)$ as a depth-$(d + 1)$ circuit by adding a dummy layer consisting of AND or OR gates of fan-in 1 to the bottom (whether AND or OR depends on the original bottom layer so that it is alternating). The motivation is to apply switching lemma for $t = 1$. Apply switching lemma to this circuit with parameter $t = 1$, $s = (1 + \delta)c_H \log S$ and $p = 1/(2c_H)$, where $\delta > 0$ is an arbitrarily small constant, and $c_H$ denotes the constant 5 in Håstad’s Switching Lemma, that is, apply random restriction $\rho_0 \in \mathcal{R}(1/(2c_H), 1/2)$. For each gate in the second bottom layer, which is 1-CNF or 1-DNF, w. p. (= with probability) at least

$$1 - (c_H pt)^s = 1 - \left(\frac{1}{2}\right)^{(1+\delta)c_H \log S} \geq 1 - S^{-1-\delta},$$
(note that $c_H > 1$) that gate can be written as $s$-DNF (or $s$-CNF respectively). If all the bottom gates can be switched, we get a depth-$d$ circuit of bottom fan-in $s = (1 + \delta)c_H \log S$.

Second step. Apply random restriction $\rho_i \in \mathcal{R}(p, 1/2)$, where

$$p = 1/(2c_H s) = 1/(2(1 + \delta)c_H \log S),$$

for $i = 1, 2, \ldots, d - 2$. For $\rho_1$, for each gate in the second bottom layer, by switching lemma, w. p. at least $1 - (c_H pt)^s \geq 1 - S^{-1 - \delta}$, this $t$-CNF can be converted to $s$-DNF (or $t$-DNF to $s$-CNF), where $t = s = (1 + \delta) \log S$. For each $\rho_i$, the depth of the circuit is supposed to be reduced by 1. Finally, it remains to count the number of times we have applied switching lemma, which is at most $S$, the total number of gates in the original circuit. Apply a union bound, with probability $\geq 1 - S^{-\delta} \rightarrow 1$, circuit $C(x)_{|\rho}$ can be converted to a depth 2 size $S$ circuit, where

$$\rho = \rho_{d-2} \circ \ldots \circ \rho_0 \in \mathcal{R}(1/(2c_H (2(1 + \delta) \log S)^{d-2}), 1/2).$$

Final step. We have proved $C(x)_{|\rho}$ can be written as a depth-2 size-$S$ circuit with high probability. Observe parity is still a parity function or its negation after applying any restriction in possibly less number of variables. Let us count the number of free variables after applying $p$. The expected number of free variables is

$$\frac{n}{2c_H (2c_H (1 + \delta) \log S)^{d-2}}.$$  

By Chernoff bound, we claim

$$m := |\rho^{-1}(\ast)| > \frac{n}{2c_H (2c_H (1 + 2\delta) \log S)^{d-2}},$$

w.h.p. It is not difficult to prove that any depth-2 circuit computing $\text{PAR}_m$ should have bottom fan-in $m$ (we leave it as an exercise for readers), which implies

$$(1 + \delta) \log S \geq m \geq n/(2c_H (2c_H (1 + 3\delta) \log S)^{d-2})$$

which implies $S \geq 2^{n^{d-1}/(2(2+3\delta)c_H)}$. Therefore, as long as constant $c < 1/(2c_H)$ (since $\delta > 0$ can be arbitrarily small), our theorem holds. For example, take $c = 1/11$.\qed
Using the same argument, the following result can be proved, which is left as an exercise for readers.

**Exercise 4.2.** If Boolean function \( f \) can be computed by depth-\( d \) circuit of size \( S \), then \( f \) can become a constant after setting at most

\[
n - \frac{n}{\Omega_d((\log S)^{d-2})} + \log S
\]

inputs, where the constant in \( \Omega_d \) only depends on \( d \).

**References**