Boolean function complexity

Lecturer: *Nitin Saurabh* Meeting: 3
Scribe: *Nitin Saurabh* 08.05.2019

1 Depth reduction

Consider a De Morgan F of depth d. Since the underlying graph in F is a binary tree, we have a bound on the number of leaves $\mathsf{L}(F) \leq 2^d$. That is, $\mathsf{D}(F) \geq \log \mathsf{L}(F)$, where $\mathsf{D}(F)$ denotes the depth of the formula F. This implies,

$$\mathsf{D}(f) \geq \log \mathsf{L}(f),$$

where $\mathsf{L}(f)$ (resp. $\mathsf{D}(f)$) denotes the minimal size (resp. depth) of a formula computing f. We now show that formulas can be balanced. That is, $\mathsf{D}(f) = \Theta(\log \mathsf{L}(f))$.

Theorem 1 (Spira 1971)**.** *Let F be a De Morgan formula of size ℓ. Then, there exists an equivalent formula F' such that $\mathsf{D}(F') \leq 3 \log \ell$.*

Proof. We prove it by induction on the size ℓ. When ℓ equals 1 or 2, the inequality trivially holds.

For the induction step, assume that the inequality holds for all formulas of size strictly less than ℓ. Given a formula F of size ℓ, we find a node g in the formula such that the number of leaves in the subformula below g is at least $\ell/2$ but individually the left and right subformula below g have strictly less than $\ell/2$ leaves. Such a node can easily be found by starting at the root and checking if the current node satisfies the properties required. If so we have found g, else there exists a child of g such that number of leaves below it is at least $\ell/2$. We move to this child and check if this node satisfies the properties needed. Continuing in this way we find the node g. We use the following equivalence

$$F \equiv (g \wedge F|_{g=1}) \vee (\neg g \wedge F|_{g=0}),$$

to modify the formula F to F' as shown in Fig. 1 where $g = g_L \odot g_R$ for some $\odot \in \{\vee, \wedge\}$. By $F|_{g=b}$, for $b \in \{0,1\}$, we mean the formula obtained by removing the subformula at g in F and substituting b at its place. By the choice of g, we have that the size of each subformula g_L, g_R, $F|_{g=0}$, and $F|_{g=1}$ is at most $\ell/2$. Inductively we balance these subformulas to obtain the formula F'. The depth of the formula thus constructed is given by the following recurrence

$$D(\ell) \leq D(\ell/2) + 3.$$

Therefore, $\mathsf{D}(F') \leq 3 \log \ell$. □

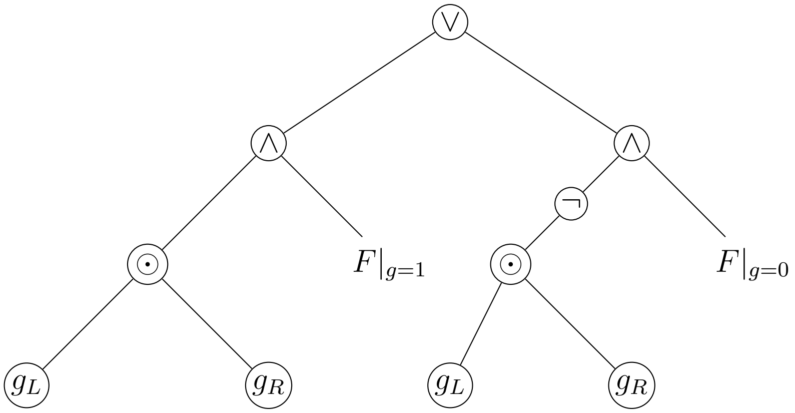

Figure 1: Depth reduction: transformation of F to F'

Remark 1.1. *In the process of reducing the depth, the size of the new formula has increased polynomially. The size of F', in the construction above, is at most $\ell^{\log 6}$.*

We will now see lower bounds for formulas. Unlike the case of general circuits where no super-linear lower bounds are known, the situation for formulas is somewhat better. We have almost cubic lower bounds against them.

2 Lower bounds: Khrapchenko's method

Definition 2. *Let $\mathcal{B}_n$ denote the set of all Boolean function over n variables. A formal complexity measure μ is a function $\mu\colon \mathcal{B}_n \to \mathbb{N}$ such that*

1. $\mu(x_i) = 1$, $\forall\ i \in [n]$,
2. $\mu(f) = \mu(\neg f)$, *for all* $f \in \mathcal{B}_n$, *and*
3. $\mu(f \vee g) \leq \mu(f) + \mu(g)$, *for all* $f, g \in \mathcal{B}_n$.

It easily follows from the definition that $\mu(f \wedge g) \leq \mu(f) + \mu(g)$. An example of a formal complexity measure is the De Morgan formula complexity of a function $\mathsf{L}(f)$. In fact, $\mathsf{L}(f)$ is the largest complexity measure.

Lemma 3. *Let μ be a formal complexity measure. Then, $\mathsf{L}(f) \geq \mu(f)$ for all Boolean function f.*

Proof. We prove it by induction on $\mathsf{L}(f)$. Base case: $\mathsf{L}(f) = 1$. Then, $f = x_i$ or $\neg x_i$ and, hence, the lemma follows from the definition.

For the induction step consider an optimal formula F for the Boolean function f. Wlog, assume that the output gate is $\vee$. Then, $F = G \vee H$ where G and H compute functions

g and h, respectively. Since F is optimal for f, G and H are also optimal for g and h, respectively. Therefore,

$$\begin{aligned}\mathsf{L}(f) &= \mathsf{L}(g) + \mathsf{L}(h)\\ &\geq \mu(g) + \mu(h)\\ &\geq \mu(g \vee h) = \mu(f).\end{aligned}$$

The second inequality follows from the induction hypothesis, while the third from the definition of μ. □

Definition 4 (Khrapchenko's measure)**.** *For $A, B \subseteq \{0,1\}^n$, let $H(A,B)$ be the set of pairs in $A \times B$ that are neighbors in the Boolean hypercube graph (or, Hamming graph). That is,*

$$H(A,B) = \{(a,b) \in A \times B \mid a \text{ and } b \text{ differ in exactly one position}\}.$$

Define,

$$K_{A,B} := \frac{|H(A,B)|^2}{|A| \cdot |B|}.$$

Then, Khrapchenko's measure associated with a Boolean function f is defined as follows

$$K(f) := \max\{K_{A,B} \mid A \subseteq f^{-1}(1) \text{ and } B \subseteq f^{-1}(0)\}.$$

We now show that Khrapchenko's measure $K(f)$ is a formal complexity measure and thus lower bounds the formula complexity $\mathsf{L}(f)$.

Theorem 5 (Khrapchenko 1971)**.** *For all Boolean function f, $\mathsf{L}(f) \geq K(f)$.*

Proof. It suffices to show that $K(f)$ is a formal complexity measure. The theorem then follows from Lemma 3. We verify each of the three properties required of a formal complexity measure.

Claim 2.1. *$K(x_i) = 1$.*

Proof. Lower bound: consider $A = \{x \in \{0,1\}^n \mid x_i = 1\}$ and $B = \{x \in \{0,1\}^n \mid x_i = 0\}$. Then, $K(x_i) \geq K_{A,B} = 1$.

Upper bound: Note that for any point $a \in x_i^{-1}(1)$ there is exactly one point $b \in x_i^{-1}(0)$ such that a and b are neighbours, and vice versa. □

Claim 2.2. *$K(f) = K(\neg f)$.*

Proof. This follows since K is symmetric with respect to $f^{-1}(1)$ and $f^{-1}(0)$. □

Claim 2.3. *$K(f \vee g) \leq K(f) + K(g)$.*

Proof. Let $K(f \vee g) = K_{A,B}$ for some $A \subseteq (f \vee g)^{-1}(1)$ and $B \subseteq (f \vee g)^{-1}(0)$. Clearly then $B \subseteq f^{-1}(0)$ and $B \subseteq g^{-1}(0)$. Arbitrarily partition A into two parts A_f and A_g such that $A_f \subseteq f^{-1}(1)$ and $A_g \subseteq g^{-1}(1)$. Thus, we have

$$\begin{aligned} K(f) \geq K_{A_f,B} &= \frac{|H(A_f, B)|^2}{|A_f| \cdot |B|}, \text{ and} \\ K(g) \geq K_{A_g,B} &= \frac{|H(A_g, B)|^2}{|A_g| \cdot |B|}. \end{aligned}$$

Therefore,

$$\begin{aligned} K(f) + K(g) &\geq \frac{|H(A_f, B)|^2}{|A_f| \cdot |B|} + \frac{|H(A_g, B)|^2}{|A_g| \cdot |B|}, \\ &\geq \frac{(|H(A_f, B)| + |H(A_g, B)|)^2}{|A_f| \cdot |B| + |A_g| \cdot |B|}, \\ &\geq \frac{|H(A, B)|^2}{|A| \cdot |B|} = K_{A,B} = K(f \vee g), \end{aligned}$$

where the second inequality follows from the following inequality: for all α_1, α_2, β_1, $\beta_2 > 0$,

$$\frac{\alpha_1^2}{\beta_1} + \frac{\alpha_2^2}{\beta_2} \geq \frac{(\alpha_1 + \alpha_2)^2}{\beta_1 + \beta_2}.$$

□

□

Observe that $H(f^{-1}(1), f^{-1}(0))$ is the number of edges in the following bipartite graph obtained from the hypercube graph given a function f: vertex set $\{0,1\}^n$ is partitioned into two sets $f^{-1}(1)$ and $f^{-1}(0)$. An edge in the hypercube graph is retained in the bipartite graph if and only if the edge crosses this partition, i.e., the two end-points of the edge lies in separate parts. Thus, intuitively, larger the number of edges crossing the partition larger the lower bound on formula size. To this end we study parity functions using Khrapchenko's measure.

Theorem 6. $\mathsf{L}(\mathsf{Parity}_n) \geq n^2$.

Proof. From Theorem 5, we know that $\mathsf{L}(\mathsf{Parity}_n) \geq K(\mathsf{Parity}_n)$. To obtain the lower bound we compute Khrapchenko's measure $K_{A,B}$ when $A = \mathsf{Parity}^{-1}(1)$ and $B = \mathsf{Parity}^{-1}(0)$. Therefore,

$$\mathsf{L}(\mathsf{Parity}_n) \geq K(\mathsf{Parity}_n) \geq K_{A,B} = \frac{(n2^{n-1})^2}{2^{n-1}2^{n-1}} = n^2.$$

□

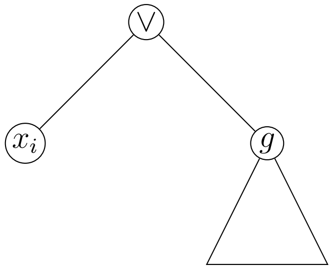

Figure 2: Structure on the sibling of a leaf in an optimal formula

Observe that recursively using $x_1 \oplus x_2 \equiv (\neg x_1 \wedge x_2) \vee (x_1 \wedge \neg x_2)$ we can construct a formula of size $O(n^2)$ computing Parity_n, and if $n = 2^k$, then in fact $\mathsf{L}(\mathsf{Parity}_n) = n^2$. Thus, for the parity function Khrapchenko's measure gives tight lower bound. However, we can not prove better than quadratic lower bound using Khrapchenko's measure.

Lemma 7. *For any Boolean function f on n variables, $K(f) \leq n^2$.*

Proof. Recall, $K(f) = \max\{K_{A,B} \mid A \subseteq f^{-1}(1) \text{ and } B \subseteq f^{-1}(0)\}$. Since every point in A can have at most n neighbours in B and vice versa, we have for any A and B,

$$H(A,B) \leq \min\{n \cdot |A|, n \cdot |B|\}.$$

Therefore, $K_{A,B} = \frac{|H(A,B)|^2}{|A| \cdot |B|} \leq n^2$. □

3 Subbotovskaya's method of random restrictions

We will now see a lower bound method due to Subbotovskaya, now known as "method of random restrictions". It has turned out to be one of the most powerful tools in circuit complexity.

Her idea was to set some of the variables randomly and show that the restriction reduces the formula size non-trivially whereas the resulting subfunction is not much easier.

We start with an observation on the structure of an optimal formula. We call a node v in a tree T a *sibling* of another node w if both have the same parent in T.

Lemma 8. *Let F be an optimal De Morgan formula for a Boolean function f. Further, let l be a leaf and g be its sibling in F. Then, the subformula rooted at g has no leaf labelled by the same variable as the leaf l.*

Proof. The proof is by contradiction. Suppose not; then there exists a sibling g of a leaf l such that the subformula rooted at g has a leaf labelled by the same variable as the leaf l. Wlog, we assume that l is labelled by x_i and the parent of g and l is an $\vee$ gate. See Fig. 2. Using the equivalence

$$x_i \vee g \equiv x_i \vee (g|_{x_i=0}),$$

we can reduce the size of the formula F by evaluating the subformula given by g at $x_i = 0$. Thus we obtain a contradiction to the optimality of F. □

Lemma 9 (Subbotovskaya 1961)**.** *Let f be a function on n variables. Then, there exists a variable x_i, $i \in [n]$, and a setting to it $b \in \{0,1\}$ such that the subfunction f' obtained by restricting x_i to b in f satisfies*

$$\mathsf{L}(f') \leq \left(1 - \frac{1}{n}\right)^{3/2} \cdot \mathsf{L}(f).$$

Proof. Let F be an optimal formula for f, and x_i be the variable that labels the most number of leaves in F. Say this number is t. Clearly, then $t \geq \mathsf{L}(f)/n$. Let $\ell_1, \ldots, \ell_t$ be the leaves labelled by x_i and $g_1, \ldots, g_t$ be their siblings in F, respectively. Since the gates are labelled by $\vee$ and $\wedge$, for each sibling g_j there is a setting to $x_i \in \{0,1\}$ such that the parent of g_j and ℓ_j evaluates to a constant. Therfore, one of the settings to x_i must make at least half of the parents evaluate to constants. Say this setting is given by $x_i = b$. We restrict x_i to b to obtain f' from f.

On simplifying F under the restriction $x_i = b$, we obtain a new formula F' that computes f'. Thus, $\mathsf{L}(f') \leq \mathsf{L}(F')$. Let us now compute the size of F'. By Lemma 8 we know that none of g_j, $1 \leq j \leq t$, contains x_i. Upon setting x_i to b, the siblings whose parent evaluates to a constant are removed from F. Therefore, at least $t/2$ siblings are removed. Hence, at least $t/2$ additional leaves are removed. Thus, using $t \geq \mathsf{L}(f)/n$, we obtain the bound

$$\mathsf{L}(f') \leq \mathsf{L}(F') \leq \mathsf{L}(f) - t - \frac{t}{2} \leq \mathsf{L}(f) - \frac{3}{2n}\mathsf{L}(f) = \left(1 - \frac{3}{2n}\right)\mathsf{L}(f) \leq \left(1 - \frac{1}{n}\right)^{3/2}\mathsf{L}(f).$$

□

Definition 10. *A map $\rho : [n] \to \{0,1,*\}$ is called a* restriction*. We say that ρ is a* restriction on k variables *if $|\rho^{-1}(\{0,1\})| = k$. By restricting a function $f\colon \{0,1\}^n \to \{0,1\}$ with ρ we obtain the subfunction $f_\rho\colon \{0,1\}^{|\rho^{-1}(*)|} \to \{0,1\}$ by setting the variables in $\rho^{-1}(\{0,1\})$ according to ρ and leaving the variables in $\rho^{-1}(*)$ unset.*

Recursively applying the above lemma we obtain the following generalization.

Theorem 11 (Subbotovskaya 1961)**.** *Let f be a function on n variables and $k \in [n]$. Then, there exists a restriction ρ on $n-k$ variables such that the subfunction f_ρ on k variables satisfies the following:*

$$\mathsf{L}(f_\rho) \leq \left(\frac{k}{n}\right)^{3/2} \cdot \mathsf{L}(f).$$

Proof. Using Lemma 9 recursively $n-k$ times, we obtain a subfunction f_ρ on k variables such that

$$\begin{aligned}
\mathsf{L}(f_\rho) &\leq \left(1 - \frac{1}{n}\right)^{3/2}\left(1 - \frac{1}{n-1}\right)^{3/2} \cdots \left(1 - \frac{1}{k+1}\right)^{3/2} \cdot \mathsf{L}(f) \\
&= \left(\frac{n-1}{n} \cdot \frac{n-2}{n-1} \cdots \frac{k}{k+1}\right)^{3/2} \cdot \mathsf{L}(f) \\
&= \left(\frac{k}{n}\right)^{3/2} \cdot \mathsf{L}(f).
\end{aligned}$$

□

To being with, using Subbotovskaya's theorem we can prove the following suboptimal lower bound of $n^{3/2}$ for Parity_n. Note that even after setting $n-1$ variables, Parity_n depends on the last variable. Therefore using Theorem 11 with $k = 1$, we obtain the following inequality

$$1 \le \mathsf{L}((\mathsf{Parity}_n)_\rho) \le \frac{1}{n^{3/2}} \cdot \mathsf{L}(\mathsf{Parity}_n).$$

In the next class we will see larger lower bounds using this method of random restrictions.