Monotone Circuits

- A boolean circuit is <u>monotone</u> if it contains only AND/OR gates (<u>no</u> NOT).

- A monotone circuit can compute only <u>monotone functions</u> :

<u>Definition</u>: • For $x, y \in \{0,1\}^n$ we define $x \leq y$ if $\forall i \in [n]$, $x_i \leq y_i$.

• A function $f: \{0,1\}^n \to \{0,1\}$ is <u>monotone</u> if $\forall x \leq y$, $f(x) \leq f(y)$.

- Consider a <u>hard</u> monotone function, $\underline{\text{Clique}}_{k,n}: \{0,1\}^{\binom{n}{2}} \to \{0,1\}$ that on a graph G is 1 iff G has a <u>k-clique</u> (a complete graph on k vertices).

<u>Qn:</u> Clearly, $\text{Clique}_{k,n}$ is monotone. Is there a poly-sized monotone circuit ?

Theorem (Razborov 1985): $\forall k \leq n^{1/4}$, $\nexists$ monotone circuit of size $\leq n^{\sqrt{k}/20}$ solving $\text{Clique}_{k,n}$.

- **Idea**: Using the probabilistic method, we will show that any monotone circuit, computing Clique, can be approximated by an OR of too few **clique indicators**.

Definition: $\forall S \subseteq [n]$, let $C_S : \{0,1\}^{\binom{n}{2}} \to \{0,1\}$ be defined 1 on G iff vertices S form a clique in G.

- C_S is a **clique indicator** of S.
- $C_\phi := 1$.

▷ $$\text{Clique}_{k,n} \equiv \bigvee_{S \in \binom{[n]}{k}} C_S \; .$$

- Let us first show a **lower bound** on the number of clique indicators for $\text{Clique}_{k,n}$:

- Define two distributions on n-vertex graphs:

$\underline{Y}$:= on random $K \in \binom{[n]}{k}$ output a clique on k & no other edges

$\underline{\mathcal{N}}$:= on random $c : [n] \to [k-1]$ output the graph: (u,v) is an edge iff $c(u) \neq c(v)$.

▷ $\text{Clique}_{k,n}$ is 1 on Y & 0 on $\mathcal{N}$.

(Clique is hard)

Lemma 1: If $k \leq n^{1/4}$ & $S \in \binom{[n]}{k}$ then,

either $\Pr_{G \in \mathcal{N}}[C_S(G) = 1] > 0.99$

or $\Pr_{G \in Y}[C_S(G) = 1] < n^{-\sqrt{k}/20}$.

Pf: . Denote $\ell := \sqrt{k-1}/10$.

Case-I: If $|S| \leq \ell$ then a random $c : S \to [k-1]$ is 1-1 with probability $\geq 1 \cdot (1 - \frac{1}{k-1}) \cdots (1 - \frac{\ell-1}{k-1})$

$\geq 1 - \frac{1+2+\ldots+(\ell-1)}{k-1} > 1 - \frac{\ell^2}{k-1} = 0.99$.

$\Rightarrow$ vertices S in $G \in \mathcal{N}$ will form a clique

with high probability.

$$\Rightarrow \Pr_{G \in \mathcal{N}} [C_S(G) = 1] > 0.99 .$$

Case-II: Let $|S| > \ell$. Consider the probability of S being a clique in $G \in \mathcal{Y}$:

$$\Pr_{G \in \mathcal{Y}} [C_S(G) = 1] = \Pr_{K \in \binom{[n]}{k}} [S \subseteq K]$$

$$\leq \binom{n-\ell}{k-\ell} / \binom{n}{k} \leq \binom{n}{k-\ell} / \binom{n}{k} = \frac{(k-\ell+1)\cdots k}{(n-k+1)\cdots(n-k+\ell)}$$

$$< \frac{k^\ell}{(n/2)^\ell} = \left(\frac{2k}{n}\right)^\ell \leq n^{-0.7\ell} < n^{-\sqrt{k}/20} .$$

□

△ This means that an OR of $m \leq n^{\sqrt{k}/20}$ clique indicators cannot be $\text{clique}_{k,n}$.

Pf:

- Presence of just one C_S ($|S| \leq \ell$) will make the OR true with probability ≥ 0.99 on $\mathcal{N}$ instances.
- If all the m C_S satisfy $|S| > \ell$, then the OR is false on $\mathcal{Y}$ instances with

$$\text{prob.} \geq \left(1 - n^{-\sqrt{k}/20}\right)^m \geq \left(1 - \frac{1}{r}\right)^{r-1} \geq e^{-1},$$

where $r := n^{-\sqrt{k}/20}$. □

- Next, we show that a <u>small</u> monotone circuit can be approximated by an OR of <u>few</u> clique indicators.

<u>Lemma 2</u>: Let $k \leq n^{1/4}$ & C be a monotone circuit of size $s \leq n^{\sqrt{k}/20}$. Then, $\exists m \leq n^{\sqrt{k}/20}$, $\exists S_1, \ldots, S_m \subseteq [n]$ s.t.

$$\Pr_{G \in Y}\left[\bigvee_{i \in [m]} C_{S_i}(G) \geq C(G)\right] > 0.9,$$

$$\Pr_{G \in N}\left[\quad " \quad \leq C(G)\right] > 0.9.$$

(Monotone circuit is easy)

<u>Pf. of the theorem</u>:

- If $\exists$ monotone circuit C of size $\leq n^{\sqrt{k}/20}$ computing $\text{Clique}_{k,n}$, then (by Lemma 2) we get $S_1, \ldots, S_m \subseteq [n]$ s.t.

$\bigvee_{i\in[m]} C_{S_i}(G)$ "mostly" agrees with $\text{clique}_{k,n}(G)$ for $G \in Y \cup N$.

- This contradicts Lemma 1.

$\Rightarrow$ monotone C of size $\leq n^{\sqrt{k}/20}$ cannot exist. $\square$

Pf. of Lemma 2:

- Define $\ell := \sqrt{k}/10$, $p := 100\ell \cdot \lg n$, $m := (p-1)^{\ell} \cdot \ell!$.
- Note that $m \ll n^{\sqrt{k}/20}$.
- Think of C as a sequence of monotone functions $f_1, \dots, f_s : \{0,1\}^{\binom{n}{2}} \to \{0,1\}$, where each f_i is an AND/OR of $\{f_{i'}, f_{i''}\}$ for $i', i'' < i$, or is an input variable $x_{u,v}$ for $u, v \in [n]$.

  Finally, $C = f_s$.
- Then we define functions $\tilde{f}_1, \dots, \tilde{f}_s$ approximating $f_1, \dots, f_s$ (resp.) s.t.

  Each $\tilde{f}_i$ is an OR of $\leq m$ clique indicators $C_{S_1}, \dots, C_{S_m}$, $|S_i| \leq \ell$.