Monotone Circuits

- A boolean circuit is monotone if it contains only AND/OR gates (no NOT gate!)

- A monotone circuit can compute only monotone functions.

Defn: • For $x, y \in \{0,1\}^n$ we define $x \le y$ if $\forall i \in [n]$, $x_i \le y_i$.

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

▷ Monotone function $f \Longleftrightarrow \exists$ monotone circuit.

- Consider a <u>hard</u> monotone function:

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

▷ $\text{Clique}_{k,n}$ is a monotone function.

<u>Qn:</u> $\exists$? poly(n)-size monotone circuit for $\text{Clique}_{k,n}$?

[<u>OPEN</u>: for circuits & algorithms.]

<u>Theorem</u> (Razborov '85): $\forall k \leq n^{1/4}$ $\nexists$ monotone circuits of size $\leq n^{\sqrt{k}/20}$ computing $\text{Clique}_{k,n}$.

(exp. lower bound)

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

Defn: • For $\emptyset \neq S \subseteq [n]$, let $C_S : \{0,1\}^{\binom{n}{2}} \to \{0,1\}$ be defined 1 on G iff S is a clique in G.

• C_S is a clique-indicator of S.

• $C_\emptyset := 1$.

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

- First, we show a lower bound on number of S needed.

- Define two simple input distributions on n-vertex graphs.

Yes-instances with unique k-clique $\rightarrow$ $\mathcal{Y}$:= on random $K \in \binom{[n]}{k}$ output a clique on K & no other edges.

No-instances $(k-1)$-partite graph $\rightarrow$ $\mathcal{N}$:= on random $c: [n] \rightarrow [k-1]$ output the graph: (u,v) is edge iff $c(u) \neq c(v)$.

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

(But, $\text{Clique}_{k-1,n} = 1$ on $\mathcal{N}$!)

Lemma 1 (Clique hard): If $k \le n^{1/4}$ & $S \in \binom{[n]}{k}$ then,

either $\Pr_{G \in N}[C_S(G) = 0] < 0.01$

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

$\Rightarrow$ Success $< 1\%$

Pf: • Denote $\ell := \sqrt{k-1}/10$.

Case-1: $[\,|S| \le \ell\,]$ A random $c : S \to [k-1]$ is one-one with probability $\geq 1 \cdot \left(1 - \frac{1}{k-1}\right) \cdot \left(1 - \frac{2}{k-1}\right) \cdots \left(1 - \frac{\ell-1}{k-1}\right)$

$$\geq 1 - \frac{1+2+\dots+\ell-1}{k-1} > 1 - \frac{\ell^2}{k-1} = 0.99\,.$$

$\Rightarrow$ vertices S in $G \in N$ form a clique $\Rightarrow C_S(G) = 1$ on N whp.

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

Case-2 $[\,|S|>\ell\,]$: The prob. of S being a clique in $G \in \mathcal{Y}$:

$$\Pr_{G\in\mathcal{Y}}[C_S(G)=1] = \Pr_{K\in\binom{[n]}{k}}[S\subseteq K] = \frac{\binom{n-|S|}{k-|S|}}{\binom{n}{k}} \leq \binom{n-\ell}{k-\ell}\Big/\binom{n}{k}$$

$$\leq \binom{n}{k-\ell}\Big/\binom{n}{k} = \frac{(k-\ell+1)\cdots k}{(n-k+1)\cdots(n-k+\ell)} < \frac{k^\ell}{(n/2)^\ell} = \left(\frac{2k}{n}\right)^\ell$$

$$< n^{-0.7\ell} < n^{-\sqrt{k}/20}. \qquad \square$$

$\triangleright$ Thus, OR of $m \leq n^{\sqrt{k}/20}$ clique-indicators cannot be $\text{Clique}_{k,n}$.

Pf: • Suppose $\mathrm{Clique}_{k,n} = \bigvee_{i\in[m]} C_{S_i}$.

• If $\exists i,\ |S_i| \le \ell \overset{\text{(Case 1)}}{\Longrightarrow} C_{S_i}(\alpha) = 1$ whp

$\Longrightarrow \mathrm{Clique}_{k,n}(\alpha) = 1$ whp, ↯.

• So, $\forall i,\ |S_i| > \ell. \overset{\text{(Case 2)}}{\Longrightarrow} \Pr_{G\in\mathcal{Y}}[C_{S_i}(G) = 0] > (1-n^{-\sqrt{k}/20})$.

$$\Longrightarrow \Pr_{G\in\mathcal{Y}}[\mathrm{Clique}_{k,n}(G) = 0] > (1-n^{-\sqrt{k}/20})^m \geq \left(1-\frac{1}{r}\right)^r \geq 1/e.$$

where $r := n^{\sqrt{k}/20}$

$\Longrightarrow$ ↯

$\Longrightarrow \mathrm{Clique}_{k,n} \neq \bigvee_{i\in[m]} C_{S_i}$. □

— Next, we show that a small monotone circuit can be approximated by OR of few clique-indicators. [on $\mathcal{Y}$ & $\mathcal{N}$ distributions.]

[easy wrt. clique problem & $\mathcal{Y}, \mathcal{N}$]

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

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

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

Pf of Razborov's Thm: • If $\exists$ monotone circuit C of size $\leq n^{\sqrt{k}/20}$ computing $\text{Clique}_{k,n}$, then by Lemma-2, $\exists$ $S_1, \ldots, S_m \subseteq [n]$ s.t. $\bigvee_i C_{S_i}(G)$ "mostly" agrees with $\text{Clique}_{k,n}(G)$ on $G \in \mathcal{Y} \cup \mathcal{N}$.

• But, by Lemma 1, the error has to be ≥ 0.99.

$$\Rightarrow \lightning.$$

$\Rightarrow$ monotone C of size $\leq n^{\sqrt{k}/20}$ can't exist.

$\square$

<u>Pf. of Lemma 2:</u> • Define $\ell := \sqrt{k}/10$; $m := (p-1)^{\ell} \cdot \ell!$;
$p := 100\ell \cdot \log n$. $\triangleright$ $m \approx p^{\ell} \approx (\sqrt{k} \cdot \log n)^{\sqrt{k}} \ll n^{\sqrt{k}/20}$.

• Think of the monotone circuit 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 $u, v \in [n]$.

At the root: $C = f_s$.

• <u>Goal:</u> define functions $\tilde{f}_1, \dots, \tilde{f}_s$ approximating $f_1, \dots, f_s$ resp. s.t. $\tilde{f}_i$ is OR of $\leq m$ clique-indicators $C_{S_1}, \dots, C_{S_m}$; $|S_i| \leq \ell$.

(We call $\tilde{f}_i$: an <u>(m,ℓ)-function</u>).

- We construction $\tilde{f}_i$'s by induction on depth/size.
  For $f_i = f_{i'} \vee f_{i''}$ we'll construct
  $\tilde{f}_i =: \tilde{f}_{i'} \sqcup \tilde{f}_{i''}$ (resp. $\tilde{f}_{i'} \sqcap \tilde{f}_{i''}$ for $f_{i'} \wedge f_{i''}$).

- Operation $f \sqcup g$ (for (m,ℓ)-fns f, g):
  - Let $f = \bigvee_{i \in [m]} C_{S_i}$ & $g = \bigvee_{j \in [m]} C_{T_j}$.
  - Consider $h := \bigvee_{i \in [2m]} C_{Z_i}$, where $Z_i := S_i$; $Z_{j+m} := T_j$ for $i, j \in [m]$.

▷ h is a $(2m, \ell)$-fn., not (m,ℓ)-fn. !

▷ $h = f \vee g$.

- We need to <u>approximate</u> h by an (m,ℓ)-fn., using the following iterative process:

(1) As long as there are $>m$ distinct sets, find p subsets $Z_{i_1},\ldots,Z_{i_p}$ the form a <u>Sunflower</u>, i.e. same mutual intersection, i.e. $\exists Z \subseteq [n]$, $\forall j<j' \in [p]$, $Z_{i_j} \cap Z_{i_{j'}} = Z$.

(2) Replace the functions $C_{Z_{i_1}},\ldots,C_{Z_{i_p}}$ in h by C_Z.

(3) Repeat this till we get an (m,ℓ)-function h'.

Define $f \sqcup g := h'$.

<u>Qn</u>: Does a sunflower exist? What's the error?

Sunflower Lemma (Erdös & Rado '60): Let $\mathcal{Z}$ be a collection of distinct sets of size $\leq \ell$. If $|\mathcal{Z}| > (p-1)^{\ell} \cdot \ell!$ then $\exists\, \underbrace{Z_1, \dots, Z_p}$ $\in \mathcal{Z}$ & set Z s.t. $\forall\, i<j \in [p]$, $Z_i \cap Z_j = Z$. ← sunflower

($Z_i \subseteq \mathcal{U}$ arbitrary & $p > 2$.)

$\triangleright$ $\Pr_{G \in \mathcal{Y}} [\,(f \sqcup g)(G) < f(G) \vee g(G)\,] = 0.$ ← no error on $\mathcal{Y}$

Pf: • for any $Z \subseteq Z_i$, $C_{Z_i}(G) = 1 \Rightarrow C_Z(G) = 1$

$\Rightarrow$ If $f(G) \vee g(G) = 1$ then $(f \sqcup g)(G) = 1$. $\square$

$\triangleright \Pr_{G \in \mathcal{N}} [(f \sqcup g)(G) > f(G) \vee g(G)] < 1/108$. ← small error on $\mathcal{N}$

Pf: • We may make an $\mathcal{N}$-instance true, if $C_Z(G) = 1$ but $C_{Z_i}(G) = 0$, $\forall i \in [p]$.

• Recall that $G \in \mathcal{N}$ is generated by a random $c : [n] \to [k-1]$ (add edge (u,v) iff $c(u) \neq c(v)$).

▷ c is one-one on Z, but <u>not</u> on Z_i, $\forall i$.

• $\Pr_c [c \text{ one-one on } Z_i \mid c \text{ is one-one on } Z]$

$$= \left(1 - \frac{|Z|}{k-1}\right) \cdot \left(1 - \frac{|Z|+1}{k-1}\right) \cdots \left(1 - \frac{\ell-1}{k-1}\right) > 1 - \frac{\ell^2}{k-1} > \frac{1}{2}.$$

- As $Z_1 \setminus Z, \ldots, Z_p \setminus Z$ are mutually disjoint, so:

$$\Pr_c[\forall i \in [p],\ c \text{ is } \underline{\text{not}} \text{ one-one on } Z_i \mid c \text{ one-one on } Z] < (1/2)^p = n^{-10\sqrt{k}} < 1/10ms.$$ $(m, s < n^{\sqrt{k}/20})$

- $\because$ Sunflower-lemma is applied $< m$ times.

$$\Rightarrow \Pr_{G \in \mathcal{N}}[(f \sqcup g)(G) \text{ is wrong}] < m \cdot \frac{1}{10ms} = \frac{1}{10s}. \qquad \square$$

<u>Operation $f \sqcap g$</u> (f, g are (m,ℓ)-fns.):

- AND corresponds to $\underline{h} := (\vee C_{S_i}) \wedge (\vee C_{T_j}) = \bigvee_{i,j \in [m]} C_{S_i \cup T_j}$ on $G \in \mathcal{Y}$. (Exercise) $\quad C_{S_i \cup T_j} = C_{S_i} \wedge C_{T_j}$

- Approximate h by (m,ℓ)-function as:

(1) Drop those C_Z from h s.t. $|Z| > \ell$.

(2) On the rest use repeatedly Sunflower-lemma.

(3) Remaining function h' is $(f \sqcap g)$.

Qn: What's the error introduced?

$\triangleright \Pr_{G \in \mathcal{Y}} [(f \sqcap g)(G) < f(G) \wedge g(G)] < 1/10s$ ← small error on $\mathcal{Y}$

Pf: • $f = \bigvee C_{S_i}$; $g = \bigvee C_{T_j}$ $\Rightarrow$ $f \wedge g |_{\mathcal{Y}} = \bigvee C_{S_i \cup T_j} =: h$

• Recall $G \in \mathcal{Y}$ corresponds to a $K \in \binom{[n]}{k}$.

• $(f \sqcap g)(G) = 0$, while $f(G) \wedge g(G) = 1$ $\Longrightarrow$

$\exists i, j, Z := S_i \cup T_j \subseteq K$ but $C_{S_i \cup T_j}$ was dropped & $|S_i \cup T_j| > \ell$.

- By Lemma-1, $\Pr_K[Z \le K] < n^{-0.7\ell} < 1/10sm^2$.

- We could drop $< m^2$ many such Z's from h.

$\Rightarrow \Pr_{G \in \mathcal{Y}}[(f \sqcap g)(G) \text{ is wrong}] < 1/10s$. $\square$

▷ $h|_N < f \wedge g|_N$.

▷ $\Pr_{G \in N}[(f \sqcap g)(G) > f(G) \wedge g(G)] < 1/10s$.

Pf: • $(f \sqcap g)(G) = 1$, while $f(G) \wedge g(G) = 0 \Rightarrow$

We replaced $C_{Z_1}, \ldots, C_{Z_p}$ by C_Z s.t. c is one-one on Z, but not one-one on Z_i , $\forall i$. $\Rightarrow \Pr$ same as in $f \sqcup g$. $\square$

▷ We compute $\sqcup, \sqcap$ $(<s)$-many times in C,

$\Rightarrow \Pr_{G \in Y}[\tilde{f}_s(G) < c(G)] < 1/10$,

& $\Pr_{G \in N}[$ " $>$ " $] < 1/10$.

$\Rightarrow$ This finishes Lemma-2. $\square$

Sunflower Lemma: $\mathcal{Z}$ is a collection of (sets of size $\le \ell$). $|\mathcal{Z}| > (p-1)^{\ell} \cdot \ell!$ $\Rightarrow \exists Z_1, \ldots, Z_p \in \mathcal{Z}$ forming a sunflower, i.e. $\exists Z, \forall i < j \in [p]$, $Z_i \cap Z_j = Z$.

— Idea: Induct on ℓ.

Proof: • For $\ell = 1$: $\mathcal{Z}$ has only singletons.

$\Rightarrow$ distinct subsets $Z_1, \ldots, Z_p \in \mathcal{Z}$ form a sunflower.

• Let $\ell > 1$: Let $\mathcal{M}$ be a maximal collection of mutually disjoint sets in $\mathcal{Z}$. If $|\mathcal{M}| \geq p$ then done!

• $|\mathcal{M}| < p$: $\Rightarrow$ $|\bigcup \mathcal{M}| \leq (p-1) \cdot \ell$. ——— (1)

• Also, $\forall Z \in \mathcal{Z}$, $Z \cap (\bigcup \mathcal{M}) \neq \phi$. ——— (2)

$\Rightarrow$ $\exists\, x \in \bigcup \mathcal{M}$ appearing in s-many sets in $\mathcal{Z}$, say, $Z_1, \ldots, Z_s \in \mathcal{Z}$, s.t. $s \geq |\mathcal{Z}| / (p-1)\ell$ [Eqns. 1 & 2]

▷ $s \geq (p-1)^{\ell} \cdot \ell! \,/\, (p-1)\ell = (p-1)^{\ell-1} \cdot (\ell-1)!$.

• Apply induction hypothesis on $\{Z_1 \setminus \{x\}, \ldots, Z_s \setminus \{x\}\} =: \mathcal{Z}'$

$\Rightarrow$ $\exists$ a sunflower in $\mathcal{Z}'$. $\Rightarrow$ $\exists$ sunflower in $\mathcal{Z}$. $\square$

OPEN: (Sunflower Conjecture) The $(\ell!)$ can be reduced to c^{ℓ}, for some constant c.

Relates to fast matrix multiplication algorithms.