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 $\text{Clique}_{k,n}$.

↳ n^k upper bd. is easy

- **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.
- $C_\phi := 1$.

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

- 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:

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

has many (k-1)-cliques → $\underline{\mathcal{N}}$:= 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 $\mathcal{Y}$ & 0 on $\mathcal{N}$.

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

(Clique is hard)

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

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

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.

(Monotone circuit is easy) (wrt clique)

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

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

<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.

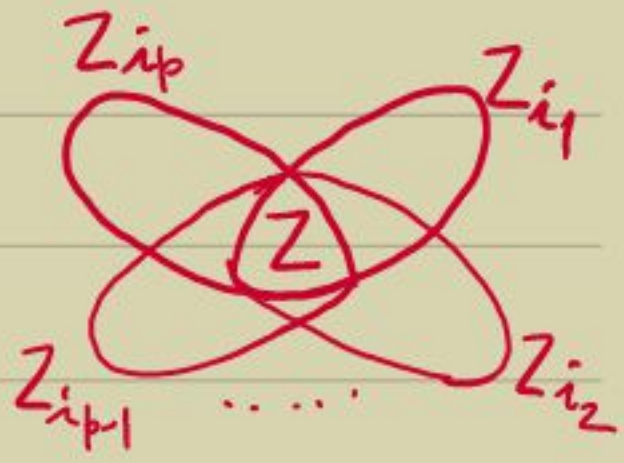
  Each $\tilde{f}_i$ is an OR of $\leq m$ clique indicators $C_{S_1}, \dots, C_{S_m}$, $|S_i| \leq \ell$.

(We call such a function: an (m,ℓ)-function.)

- We construct $\tilde{f}_i$'s by induction.
  For $f_i = f_{i'} \vee f_{i''}$ we construct $\tilde{f}_i := \tilde{f}_{i'} \sqcup \tilde{f}_{i''}$ as follows:
  (respectively, $f_{i'} \wedge f_{i''} \mapsto \tilde{f}_{i'} \sqcap \tilde{f}_{i''}$.)

- Operation $f \sqcup g$:
  Let f, g be two (m,ℓ)-functions:
  $f = \bigvee_{i \in [m]} C_{S_i}$ & $g = \bigvee_{j \in [m]} C_{T_j}$.

- Consider the function $h := \bigvee_{i \in [2m]} C_{Z_i}$, where $Z_i := S_i$ & $Z_{m+j} := T_j$, $\forall i,j \in [m]$.
  Clearly, h is not an (m,ℓ)-function.
- We approximate h by an (m,ℓ)-function as follows:
  i) As long as $\exists > m$ distinct sets, find p subsets $Z_{i_1}, \dots, Z_{i_p}$ that form a sunflower (i.e. $\exists Z \subseteq [n], \forall j < j' \in [p]$, $Z_{i_j} \cap Z_{i_{j'}} = Z$).



ii) Replace the functions $C_{Z_{i_1}}, \ldots, C_{Z_{i_p}}$ in h with C_Z.

iii) Repeat this till we get an (m,ℓ)-function h'. Define $f \sqcup g := h'$.

▷ We do not get stuck because a sunflower exists in each of the above steps.

"Sunflower" Lemma (Erdös & Rado, 1960): Let $\mathcal{Z}$ be a collection of distinct sets of size $\leq \ell$. If $|\mathcal{Z}| > (p-1)^\ell \cdot \ell!$ then $\exists\, Z_1, \ldots, Z_p \in \mathcal{Z}$ (each of size $\leq \ell$) & a set Z s.t. $\forall i<j \in [p]$, $Z_i \cap Z_j = Z$.

- $Z_i \subseteq \mathcal{U}$ (arbitrary) & $p > 2$.
- How well does $f \sqcup g$ approximate $f \vee g$?

▷ $\Pr_{G \in \mathcal{Y}} [(f \sqcup g)(G) < f(G) \vee g(G)] = 0$.

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

$\Rightarrow$ If $f(G)\,V_g(G) = 1$ then $(f \sqcup g)(G) = 1$. □

▷ $\Pr_{G \in \mathcal{N}}[(f \sqcup g)(G) > f(G)\,V_g(G)] < 1/10p$.

Pf: • During an application of the Sunflower's lemma, we may make an $\mathcal{N}$ instance true, by replacing $C_{Z_1}, \ldots, C_{Z_p}$ by C_Z s.t. $C_Z(G) = 1$ while $\forall i \in [p]$, $C_{Z_i}(G) = 0$.

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

$\Rightarrow$ c is 1-1 on Z but <u>not</u> on Z_i's.

• $\Pr_c[c \text{ is 1-1 on } Z_i \mid c \text{ is 1-1 on } Z]$

$$\geq \left(1 - \frac{|Z|}{k-1}\right)\left(1 - \frac{|Z|+1}{k-1}\right) \cdots \left(1 - \frac{\ell}{k-1}\right)$$

$$> 1 - \frac{|Z| + \cdots + \ell}{k-1} > 1 - \frac{\ell^2}{k-1} > 1/2$$

- As $Z_1 \setminus 2, \ldots, Z_p \setminus 2$ are mutually disjoint we also get:

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

- Sunflower lemma might be applied $< m$ times

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

□

Operation $f \sqcap g$:

- Let h be the function $\bigvee_{i,j \in [m]} C_{S_i \cup T_j}$.

- We approximate it by an (m,ℓ)-function as:
  - i) Drop those C_Z from h s.t. $|Z| > \ell$.
  - ii) Reduce the number of clique indicators by repeated applications of the Sunflower lemma.
  - iii) Remaining function h' is $(f \sqcap g)$.

- How well does $f \sqcap g$ approximate $f \wedge g$?

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

Pf: • $f = \bigvee_{i \in [m]} C_{S_i}$ & $g = \bigvee_{j \in [m]} C_{T_j}$.

* $\Rightarrow f \wedge g = \bigvee_{i,j \in [m]} C_{S_i \cup T_j} = h$.

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

• The only way $(f \sqcap g)(G) = 0$, while $f(G) \wedge g(G) = 1$ for a $G \in \mathcal{Y}$, is if we drop a C_Z, $Z \subseteq k$ & $|Z| > \ell$. ($\ell = \sqrt{k}/10$)

• By Lemma 1, $\Pr_{k \in \binom{[n]}{k}} [Z \subseteq k] < n^{-0.7\ell} < \frac{1}{10sm^2}$.

• We could drop at most m^2 Z's from h.

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

* Prove that $C_{S_i} \wedge C_{T_j} = C_{S_i \cup T_j}$ on $G \in \mathcal{Y}$.

▷ $h|_N = f \wedge g$.

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

Pf: • A $G \in N$ corresponds to a $c : [n] \to [k-1]$.

• The only way $(f \sqcap g)(G) = 1$, while $f(G) \wedge g(G) = 0$ for $G \in N$, is when we replace $G_{Z_1}, \dots, G_{Z_b}$ by G_Z s.t. c is 1-1 on Z but c is not 1-1 on Z_i, $\forall i \in [b]$.

$\Rightarrow$ an analysis like that of $f \sqcup g$ gives us error probability $< 1/10s$. □

▷ As we compute $\sqcup$ & $\sqcap$ at most s times in C, we get:

$$\Pr_{G \in Y}[\tilde{f}_b(G) < C(G)] < 1/10 \quad \&$$

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

$\Rightarrow$ This finishes Lemma 2. □

– Finally, we prove the Sunflower lemma:

Sunflower lemma

Pf: • We induct on ℓ (set size-bound).

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

$\Rightarrow$ any distinct $Z_1, \dots, Z_p \in \mathcal{Z}$ is 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 we are done.

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

• Also, $\mathcal{M}$'s maximality $\Rightarrow \forall Z \in \mathcal{Z}$, $Z \cap (\cup \mathcal{M}) \neq \emptyset$.

$\Rightarrow \exists\, x \in \cup \mathcal{M}$ appearing in $\geq |\mathcal{Z}| / \ell(p-1)$ many sets in $\mathcal{Z}$, say $Z_1, \dots, Z_p \in \mathcal{Z}$.

• Since $s > (\ell-1)! \cdot (p-1)^{\ell-1}$, by induction $\exists$ a sunflower in $\{Z_1 \setminus \{x\}, \dots, Z_p \setminus \{x\}\}$

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

Relates to matrix multiplication tool! [ASU'11]

- Sunflower conjecture: The $(\ell!)$ can be improved to c^ℓ for some constant c.