# A NEW SEPARATION BETWEEN MONOTONE & NON-MONOTONE CIRCUTIS


Bruno Cavalar (Oxford)

Théo Borém Fabris (U.CPH)

Partha Mukhopadhyay (CMI)

Srikanth Srinivasan (U.CPH)

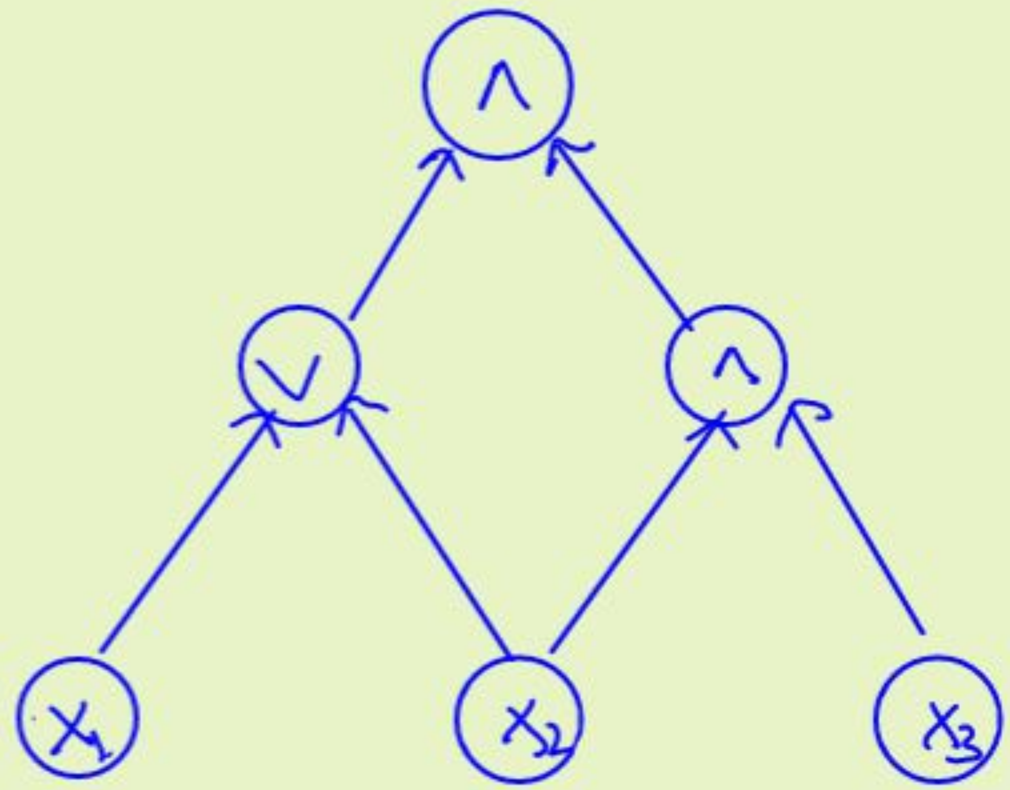
Amir Yehudayoff (U.CPH)

# Monotone Boolean Circuits

→ Boolean circuit

De Morgan basis

AND / OR



# Monotone Boolean Circuits

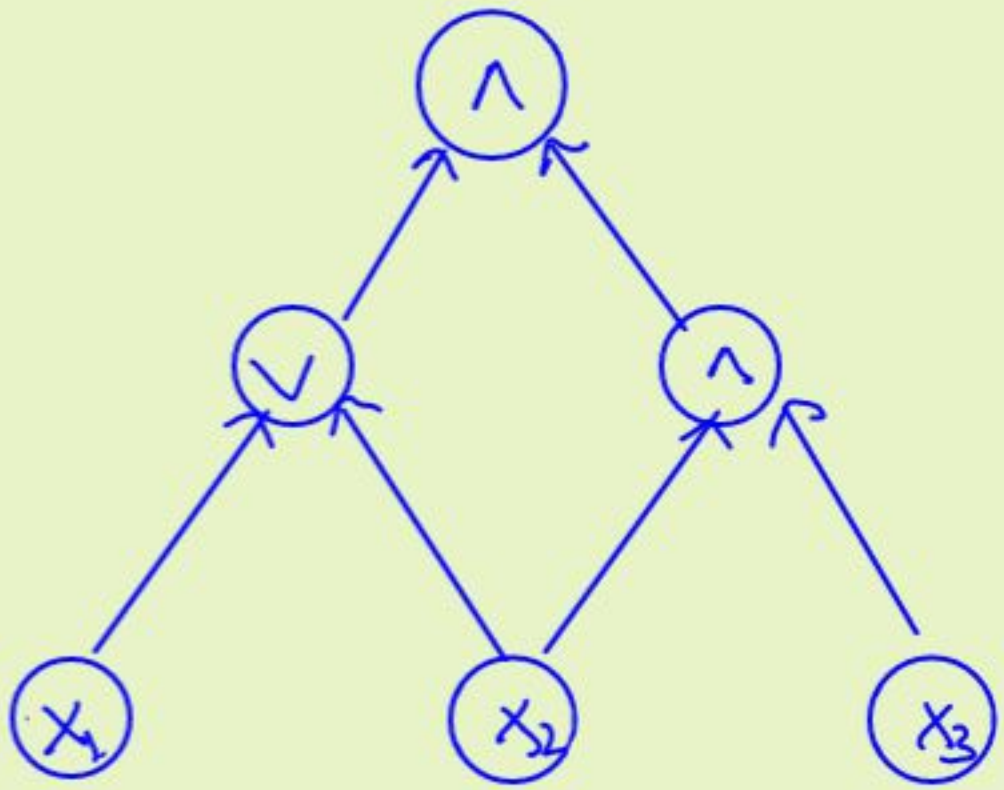
→ Boolean circuit

De Morgan basis

AND / OR

→ Computes monotone

$f:\{0,1\}^n \to \{0,1\}$ → $x \le y \Rightarrow f(x) \le f(y)$



# Monotone Boolean Circuits

→ Boolean circuit

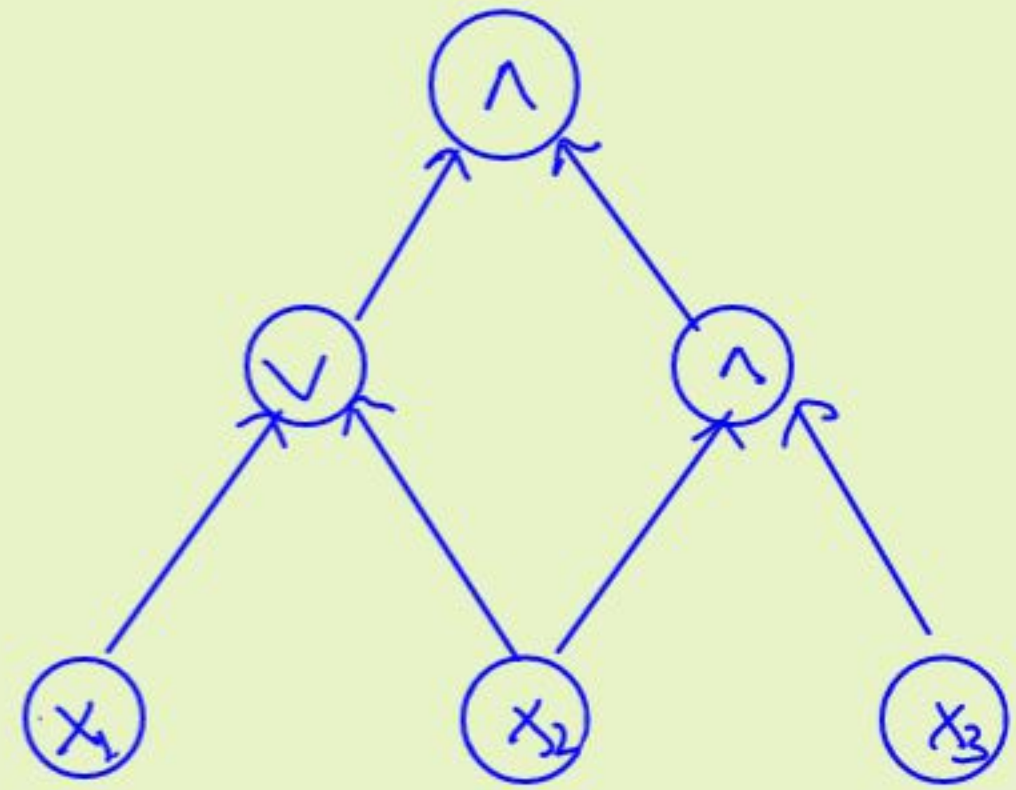
De Morgan basis

AND / OR

→ Computes monotone

$f : \{0,1\}^n \to \{0,1\}$

→ Any monotone $f$ has a monotone ckt. of size $O(2^n)$



## Monotone Boolean Circuits

→ Boolean circuit

De Morgan basis

AND / OR

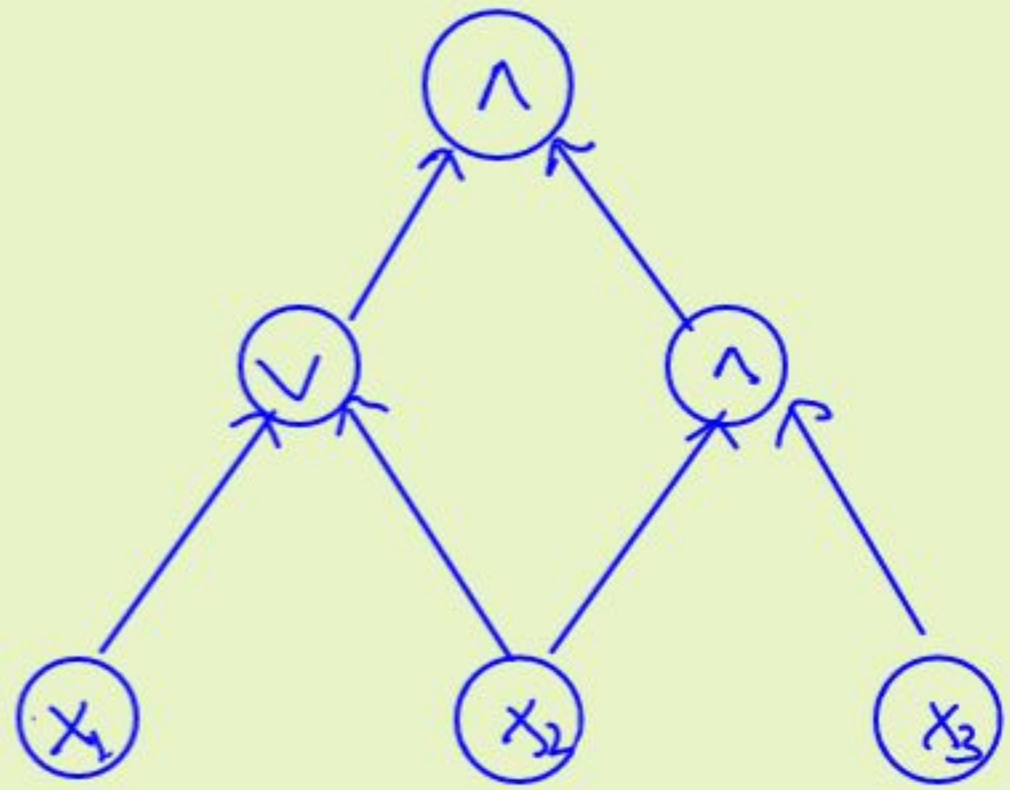
→ Computes monotone

$f : \{0,1\}^n \to \{0,1\}$

→ Any monotone $f$ has a monotone ckt. of size $O(2^n)$

→ Most $f$ need size $2^{\Omega(n)}$

→ Explicit $f$ ?



Razborov '85

**Thm**: $n^{\Omega(\log n)}$ lower bounds for

→ Clique

→ Perfect Matching

Razborov '85

Thm: $n^{\Omega(\log n)}$ lower bounds for

→ Clique ----> Should be exponential!

→ Perfect Matching ---> Monotone vs. non-monotone separation!

## Further developments

LB $n^{\Omega((\log n)^c)}$ $\exp(n^{\varepsilon})$

UB

NP Razborov '85

P Razborov '85

# Further developments

| | | |
|---|---|---|
| LB | $n^{\Omega((\log n)^c)}$ | $\exp(n^{\varepsilon})$ |
| UB | | |
| NP | Razborov'85 | AB'87 $\varepsilon = 1/6$ |
| | | Andreev'85, HR'01 $\varepsilon = 1/3$ |
| | | CKR'20 $\varepsilon = 1/2$ |
| P | Razborov'85 | |

# Further developments

| | | | |
|---|---|---|---|
| LB | $n^{\Omega((\log n)^c)}$ | $\exp(n^{\varepsilon})$ | |
| UB | | | |
| NP | Razborov'85 | AB'87 | $\varepsilon = 1/6$ |
| | | Andreev'85, HR'01 | $\varepsilon = 1/3$ |
| | | CKR'20 | $\varepsilon = 1/2$ |
| P | Razborov'85 | Tardos'87 | $\varepsilon = 1/6$ |
| | | dRV'25 | $\varepsilon = 1/3$ |

# Further developments

| | | | |
|---|---|---|---|
| LB | $n^{\Omega((\log n)^c)}$ | $\exp(n^{\varepsilon})$ | |
| UB | | | |
| NP | Razborov'85 | AB'87 | $\varepsilon = 1/6$ |
| | | Andreev'85, HR'01 | $\varepsilon = 1/3$ |
| | | CKR'20 | $\varepsilon = 1/2$ |
| P | Razborov'85 | Tardos'87 | $\varepsilon = 1/6$ |
| | | dRV'25 | $\varepsilon = 1/3$ |
| NC | BGW'99 | | |
| L | BGW'99 | | |

# Further developments

| | | | |
|---|---|---|---|
| LB | $n^{\Omega((\log n)^c)}$ | $\exp(n^{\varepsilon})$ | |
| UB | | | |
| NP | Razborov'85 | AB'87 | $\varepsilon = 1/6$ |
| | | Andreev'85, HR'01 | $\varepsilon = 1/3$ |
| | | CKR'20 | $\varepsilon = 1/2$ |
| P | Razborov'85 | Tardos'87 | $\varepsilon = 1/6$ |
| | | dRV'25 | $\varepsilon = 1/3$ |
| NC | BGW'99 | GKRS'19 + LMMPZ'22 | $\varepsilon = 1/4$ |
| | | This result | $\varepsilon = 1/3$ |
| L | BGW'99 | | |

# Further developments

| | | | |
|---|---|---|---|
| LB | $n^{\Omega((\log n)^c)}$ | $\exp(n^{\varepsilon})$ | |
| UB | | | |
| NP | Razborov'85 | AB'87 | $\varepsilon = 1/6$ |
| | | Andreev'85, HR'01 | $\varepsilon = 1/3$ |
| | | CKR'20 | $\varepsilon = 1/2$ |
| P | Razborov'85 | Tardos'87 | $\varepsilon = 1/6$ |
| | | dRV'25 | $\varepsilon = 1/3$ |
| NC | BGW'99 | GKRS'19 + LMMPZ'22 | $\varepsilon = 1/4$ |
| | | This result | $\varepsilon = 1/3$ |
| | | CGRSS'25 | $\varepsilon = 1/6$ |
| L | BGW'99 | | |
| $AC^0$ | CGRSS'25 | | |

## Main Result

$$M = \begin{array}{c} \begin{array}{cccc} x_1 & \cdots & \cdots & x_n \end{array} \\ \begin{pmatrix} | & & & | \\ v_1 & \cdots & \cdots & v_n \\ | & & & | \end{pmatrix}_{m \times n} \end{array}$$

$$f_M(x_1, \ldots, x_n) = 1 \iff rk\{v_i \mid x_i = 1\} = \text{full} = m$$

## Main Result

$$M = \begin{array}{c} \begin{array}{ccc} x_1 & \cdots & x_n \end{array} \\ \begin{pmatrix} | & & | \\ v_1 & \cdots & v_n \\ | & & | \end{pmatrix}_{m \times n} \end{array}$$

$f_M(x_1, .., x_n) = 1 \iff rk\{v_i \mid x_i = 1\} = \text{full} = m$

Thm: $\exists n = \tilde{O}(m^{3/2})$, $M$ s.t. any monotone Bool. $C$ for $f_M$ has size $\exp(\tilde{\Omega}(\sqrt{m}))$.

# Qualitative differences

$$M = \begin{array}{c} \begin{array}{ccc} x_1 & \cdots & x_n \end{array} \\ \begin{pmatrix} | & & | \\ v_1 & \cdots & v_n \\ | & & | \end{pmatrix}_{m\times n} \end{array}$$

$f_M(x_1,..,x_n)=1 \iff rk\{v_i \mid x_i=1\} = \text{full} = m$

# Qualitative differences

$$M = \begin{array}{c} \begin{array}{ccc} x_1 & \cdots & x_n \end{array} \\ \begin{pmatrix} | & & | \\ v_1 & \cdots & v_n \\ | & & | \end{pmatrix}_{m \times n} \end{array}$$

$f_M(x_1,..,x_n) = 1 \iff rk\{v_i \mid x_i = 1\} = \text{full} = m$

→ Computed by monotone rank program

$$M = \begin{array}{c} \begin{array}{ccc} x_{j_1} & \cdots & x_{j_s} \end{array} \\ \begin{pmatrix} | & & | \\ v_1 & \cdots & v_s \\ | & & | \end{pmatrix} \end{array} \quad f_M(x) = 1 \iff rk\{v_i \mid x_{j_i} = 1\} = \text{full}$$

[GKRS'19]: separation from monotone span programs

# Qualitative differences

$$M = \begin{array}{c} \begin{array}{ccc} x_1 & \cdots & x_n \end{array} \\ \begin{pmatrix} | & & | \\ v_1 & \cdots & v_n \\ | & & | \end{pmatrix}_{m \times n} \end{array}$$

$f_M(x_1,..,x_n) = 1 \iff rk\{v_i \mid x_i = 1\} = \text{full} = m$

→ Computed by monotone rank program

$$M = \begin{array}{c} \begin{array}{ccc} x_{j_1} & \cdots & x_{j_s} \end{array} \\ \begin{pmatrix} | & & | \\ v_1 & \cdots & v_s \\ | & & | \end{pmatrix} \end{array}$$

$f_M(x) = 1 \iff$
$rk\{v_i \mid x_{j_i} = 1\} = \text{full}$

[GKRS'19]: separation from monotone span programs

Thm: [Bolzano AI] Rank exponentially weaker than Span.

# Qualitative differences

$$M = \begin{array}{c} \begin{array}{ccc} x_1 & \cdots & x_n \end{array} \\ \begin{pmatrix} | & & | \\ v_1 & \cdots & v_n \\ | & & | \end{pmatrix}_{m \times n} \end{array}$$

$f_M(x_1, .., x_n) = 1 \iff rk\{v_i \mid x_i = 1\} = \text{full} = m$

→ Computed by monotone rank program

$$M = \begin{array}{c} \begin{array}{ccc} x_{j_1} & \cdots & x_{j_s} \end{array} \\ \begin{pmatrix} | & & | \\ v_1 & \cdots & v_s \\ | & & | \end{pmatrix} \end{array}$$

$f_M(x) = 1 \iff rk\{v_i \mid x_{j_i} = 1\} = \text{full}$

[GKRS'19]: separation from monotone span programs

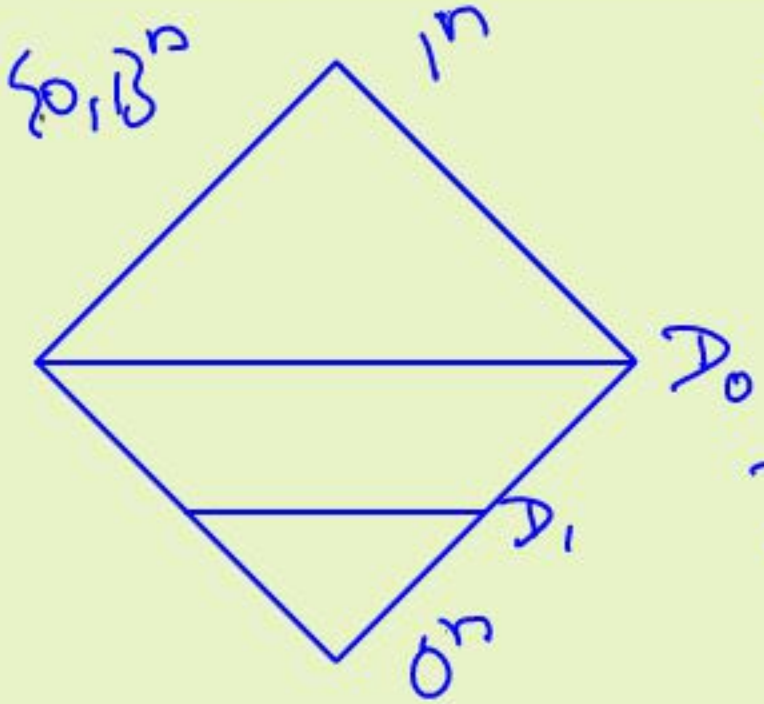
Thm: [Bolzano AI] Rank exponentially weaker than Span.

→ Min terms $\iff$ max. ind. sets of a matroid.

Solves an open problem of JS'20.

# Proof Method

$f : \{0,1\}^n \to \{0,1\}$




$D_1$ : hard dist. on 1 inputs

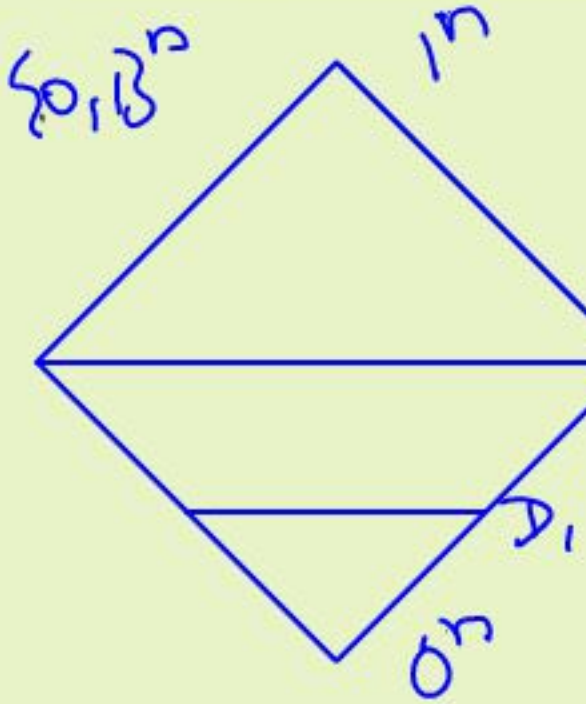
$D_0$ : " " " 0 "

$D_1$ : supp. on wt. $w \ll n$

$D_0$ : sunflower lemma

# Proof Method

$f:\{0,1\}^n \to \{0,1\}$




$D_1$: hard dist. on 1 inputs

$D_0$: " " " 0 "

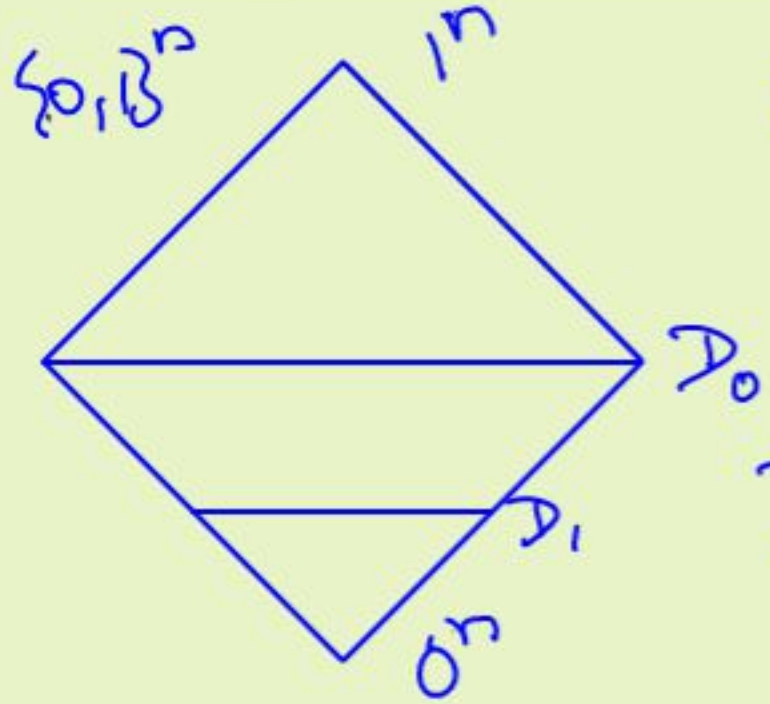
$D_1$: supp. on wt. $w \ll n$

$D_0$: sunflower lemma

$D_1$ is $k$-spread: $\Pr_{x \sim D_1}\left[\bigwedge_{i \in I} x_i = 1\right] \leq O\left(\frac{w}{n}\right)^{|I|} \ \forall\, |I| \leq k$

# Proof Method

$f:\{0,1\}^n \to \{0,1\}$




$D_1$ : hard dist. on 1 inputs

$D_0$ : " " " 0 "

$D_1$ : supp. on wt. $w \ll n$ $\quad D_0$ : sunflower lemma

$D_1$ is $k$-spread : $\Pr_{x \sim D_1}\left[\bigwedge_{i \in I} x_i = 1\right] \leq O\left(\frac{w}{n}\right)^{|I|} \ \forall\, |I| \leq k$

$D_0$ has an $(r, 2k)$- : $\quad F = \bigvee_{i=1}^{N} T_i \quad |T_i| = \ell \leq 2k$, $\ N \geq r^{\ell}$

sunflower lemma

$\Rightarrow \exists F' = \bigvee_{i=1}^{p} T_i$ : $\Pr_{x \sim D_0}\left[F'(x) \neq \bigcap_{i=1}^{p} T_i(x)\right] \leq \frac{1}{n^{10k}}$.

# Proof Method

$D_1$ is $k$-spread: $\Pr_{x\sim D_1}\left[\bigwedge_{i\in I} x_i = 1\right] \le O\left(\frac{w}{n}\right)^{|I|} \;\forall\, |I| \le k$

$D_0$ has an $(r,2k)$-sunflower lemma: $F = \bigvee_{i=1}^{N} T_i$ $\quad |T_i| = \ell \le 2k$, $\quad N \ge r^{\ell}$

$\Rightarrow \exists F' = \bigvee_{i=1}^{p} T_i : \Pr_{x\sim D_0}\left[F'(x) \ne \bigcap_{i=1}^{p} T_i(x)\right] \le \frac{1}{n^{10k}}.$

Thm [this work based on CKR'20, CGRSS'25]:

Any monotone Boolean ckt. for $f$ has size

$$\left(\frac{c \cdot n}{w r}\right)^{k}$$

# Sunflower lemmas

$D_0$ has an $(r,2k)$-sunflower lemma: $\quad F = \bigvee_{i=1}^{N} T_i \quad |T_i| = \ell \le 2k$, $N \ge r^\ell$

$$\Rightarrow \exists F' = \bigvee_{i=1}^{p} T_i : \Pr_{x\sim D_0}\left[F'(x) \neq \bigcap_{i=1}^{p} T_i(x)\right] \le \frac{1}{n^{10k}}.$$

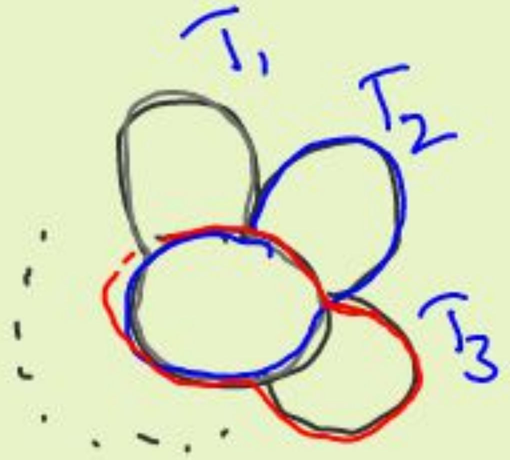
# Sunflower lemmas

$D_0$ has an $(r, 2k)$-sunflower lemma: $\quad F = \bigvee_{i=1}^{N} T_i \quad |T_i| = \ell \leq 2k$, $N \geq r^{\ell}$

$\Rightarrow \exists F' = \bigvee_{i=1}^{p} T_i : \Pr_{x \sim D_0}\left[F'(x) \neq \bigcap_{i=1}^{p} T_i(x)\right] \leq \frac{1}{n^{10k}}$.

$D_0 = \mathcal{U}_n$ (uniform on $\{0,1\}^n$)

**Obs**: Sufficient to find a combinatorial sunflower with $c2^{\ell} k \log n$ petals.



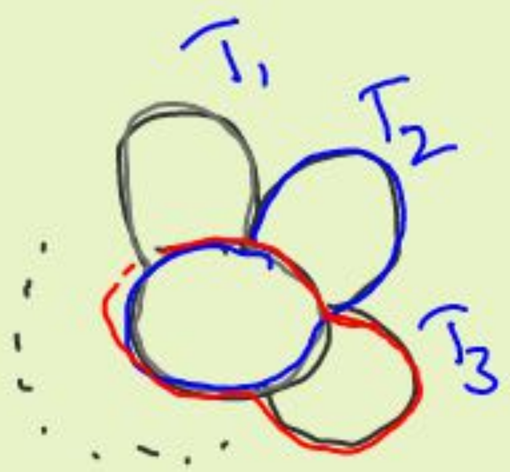
## Sunflower lemmas

$\mathcal{D}_0$ has an $(r,2k)$-sunflower lemma: $F = \bigvee_{i=1}^{N} T_i$, $|T_i| = \ell \le 2k$, $N \geq r^\ell$

$\Rightarrow \exists F' = \bigvee_{i=1}^{p} T_i : \Pr_{x \sim \mathcal{D}_0}\left[F'(x) \neq \bigcap_{i=1}^{p} T_i(x)\right] \le \frac{1}{n^{10k}}$.

$\mathcal{D}_0 = \mathcal{U}_n$ (uniform on $\{0,1\}^n$)

Obs: Sufficient to find a combinatorial sunflower with $c2^\ell k \log n$ petals.




ER'61: Need $r \geq 2^\ell k \log n$

# Sunflower lemmas

$D_0$ has an $(r,2k)$-sunflower lemma: $F = \bigvee_{i=1}^{N} T_i$ $\quad |T_i| = \ell \leq 2k$, $N \geq r^{\ell}$

$\Rightarrow \exists F' = \bigvee_{i=1}^{p} T_i : \Pr_{x \sim D_0}\left[F'(x) \neq \bigcap_{i=1}^{p} T_i(x)\right] \leq \frac{1}{n^{10k}}$.

$D_0 = \mathcal{U}_n$ (uniform on $\{0,1\}^n$)

Rossman'11: Sufficient to find "nearly disjoint" subfamilies.

ALWZ'19: "Spread" subfamilies $\Rightarrow$ sunflower lemma

ALWZ'19, BCW'21, Rao'25: $r \geq c \cdot k \log n$ sufficient.

# Proving lower bounds for $f_M$

$$M = \begin{pmatrix} | & & | \\ v_1 & \cdots & v_n \\ | & & | \end{pmatrix}_{m \times n}$$

$f_M(x_1, \ldots, x_n) = 1 \iff \{v_i \mid x_i = 1\}$ full rank.

$D_1$ is $k$-spread: $\Pr_{x \sim D_1}\left[\bigwedge_{i \in I} x_i = 1\right] \le O\left(\frac{w}{n}\right)^{|I|} \ \forall |I| \le k$

$D_0$ has an $(r, 2k)$-sunflower lemma: $F = \bigvee_{i=1}^{N} T_i$ $\quad |T_i| = \ell \le 2k$ $\quad N \ge r^\ell$

$\Rightarrow \exists F' = \bigvee_{i=1}^{p} T_i : \Pr_{x \sim D_0}\left[F'(x) \ne \bigcap_{i=1}^{p} T_i(x)\right] \le \frac{1}{n^{10k}}$.

# Proving lower bounds for $f_M$

$$M = \begin{pmatrix} | & & | \\ v_1 & \cdots & v_n \\ | & & | \end{pmatrix}_{m \times n}$$

$f_M(x_1, \ldots, x_n) = 1 \iff \{v_i \mid x_i = 1\}$ full rank.

Random $M \in \mathbb{F}_2^{m \times n}$ $(n = m^{O(1)})$

$D_1$ is $k$-spread: $\Pr_{x \sim D_1}\left[\bigwedge_{i \in I} x_i = 1\right] \leq O\left(\frac{\omega}{n}\right)^{|I|} \;\forall\, |I| \leq k$

$D_0$ has an $(r, 2k)$-sunflower lemma: $F = \bigvee_{i=1}^{N} T_i \quad |T_i| = \ell \leq 2k \quad N \geq r^{\ell}$

$\Rightarrow \exists F' = \bigvee_{i=1}^{p} T_i : \Pr_{x \sim D_0}\left[F'(x) \neq \bigcap_{i=1}^{p} T_i(x)\right] \leq \frac{1}{n^{10k}}$

# Proving lower bounds for $f_M$

$$M = \begin{pmatrix} | & & | \\ v_1 & \cdots & v_n \\ | & & | \end{pmatrix}_{m \times n} \qquad f_M(x_1, \ldots, x_n) = 1 \iff \{v_i \mid x_i = 1\} \text{ full rank.}$$

Random $M \in \mathbb{F}_2^{m \times n}$ $(n = m^{O(1)})$

$\Rightarrow$ $\Omega(1)$-fraction of $m \times m$ sub-matrices full-rk.

$D_1$ is $k$-spread: $\Pr_{x \sim D_1}\left[\bigwedge_{i \in I} x_i = 1\right] \leq O\left(\frac{m}{n}\right)^{|I|}$ $\forall\, |I| \leq k$

$D_0$ has an $(r, 2k)$-sunflower lemma: $F = \bigvee_{i=1}^{N} T_i$ $\quad |T_i| = \ell \leq 2k$, $N \geq r^{\ell}$

$\Rightarrow \exists F' = \bigvee_{i=1}^{p} T_i$ : $\Pr_{x \sim D_0}\left[F'(x) \neq \bigcap_{i=1}^{p} T_i(x)\right] \leq \frac{1}{n^{10k}}$.

# Proving lower bounds for $f_M$

$$M = \begin{pmatrix} | & & | \\ v_1 & \cdots & v_n \\ | & & | \end{pmatrix}_{m \times n}$$

$f_M(x_1, \dots, x_n) = 1 \iff \{v_i \mid x_i = 1\}$ full rank.

Random $M \in \mathbb{F}_2^{m \times n}$ $(n = m^{O(1)})$

$\Rightarrow$ $\Omega(1)$-fraction of $m \times m$ sub-matrices full-rk.

$D_1$: $S \in_R \binom{[n]}{m}$ $x = \mathbb{1}_S$

$$\Pr_{x \sim D_1}\left[\bigwedge_{i \in I} x_i = 1\right] \leq \left(\frac{m}{n}\right)^{|I|}$$

$D_1$ is $k$-spread: $\Pr_{x \sim D_1}\left[\bigwedge_{i \in I} x_i = 1\right] \leq O\left(\frac{m}{n}\right)^{|I|}$ $\forall\, |I| \leq k$

$D_0$ has an $(r, 2k)$-sunflower lemma: $F = \bigvee_{i=1}^{N} T_i$ $|T_i| = \ell \leq 2k$, $N \geq r^\ell$

$\Rightarrow \exists F' = \bigvee_{i=1}^{p} T_i$ : $\Pr_{x \sim D_0}\left[F'(x) \neq \bigcap_{i=1}^{p} T_i(x)\right] \leq \frac{1}{n^{10k}}$.

# Proving lower bounds for $f_M$

$$M = \begin{pmatrix} | & & | \\ v_1 & \cdots & v_n \\ | & & | \end{pmatrix}_{m \times n} \qquad f_M(x_1, \ldots, x_n) = 1 \iff \{v_i \mid x_i = 1\} \text{ full rank.}$$

Random $M \in \mathbb{F}_2^{m \times n}$ $(n = m^{O(1)})$

$\rightarrow$ All subsets of size $t = m/\log m$ independent.

$D_1$ is $k$-spread: $\Pr_{x \sim D_1}\left[\bigwedge_{i \in I} x_i = 1\right] \leq O\left(\frac{w}{n}\right)^{|I|} \quad \forall\, |I| \leq k$

$D_0$ has an $(r, 2k)$-sunflower lemma: $\quad F = \bigvee_{i=1}^{N} T_i \quad |T_i| = \ell \leq 2k, \quad N \geq r^\ell$

$\Rightarrow \exists F' = \bigvee_{i=1}^{p} T_i : \Pr_{x \sim D_0}\left[F'(x) \neq \bigcap_{i=1}^{p} T_i(x)\right] \leq \frac{1}{n^{10k}}$

## Proving lower bounds for $f_M$

$$M = \begin{pmatrix} | & & | \\ v_1 & \cdots & v_n \\ | & & | \end{pmatrix}_{m \times n} \qquad f_M(x_1, \dots, x_n) = 1 \iff \{v_i \mid x_i = 1\} \text{ full rank.}$$

Random $M \in \mathbb{F}_2^{m \times n}$ $(n = m^{O(1)})$

$\rightarrow$ All subsets of size $t = m/\log m$ independent.

$D_0$: $u \in_R \mathbb{F}_2^n \quad x_i = 1 \iff u \cdot v_i = 0$

$D_1$ is $k$-spread: $\Pr_{x \sim D_1}\left[\bigwedge_{i \in I} x_i = 1\right] \leq O\left(\frac{w}{n}\right)^{|I|} \; \forall\, |I| \leq k$

$D_0$ has an $(r, 2k)$-sunflower lemma: $F = \bigvee_{i=1}^{N} T_i \quad |T_i| = \ell \leq 2k, \; N \geq r^{\ell}$

$\Rightarrow \exists F' = \bigvee_{i=1}^{p} T_i : \Pr_{x \sim D_0}\left[F'(x) \neq \bigcap_{i=1}^{p} T_i(x)\right] \leq \frac{1}{n^{10k}}$.

# Proving lower bounds for $f_M$

$$M = \begin{pmatrix} | & & | \\ v_1 & \cdots & v_n \\ | & & | \end{pmatrix}_{m \times n}$$

$f_M(x_1, \ldots, x_n) = 1 \iff \{v_i \mid x_i = 1\}$ full rank.

Random $M \in \mathbb{F}_2^{m \times n}$ $(n = m^{O(1)})$

$\Rightarrow$ All subsets of size $t = m/\log m$ independent.

$D_0$: $u \in_R \mathbb{F}_2^n$ $\quad x_i = 1 \iff u \cdot v_i = 0$

$D_0$ has uniform marginals & $t$-wise independence

$D_1$ is $k$-spread: $\Pr_{x \sim D_1}\left[\bigwedge_{i \in I} x_i = 1\right] \le O\left(\frac{\omega}{n}\right)^{|I|}$ $\forall\, |I| \le k$

$D_0$ has an $(r, 2k)$-sunflower lemma: $\quad F = \bigvee_{i=1}^{N} T_i \quad |T_i| = \ell \le 2k$, $N \ge r^\ell$

$\Rightarrow \exists F' = \bigvee_{i=1}^{p} T_i$ : $\Pr_{x \sim D_0}\left[F'(x) \ne \bigcap_{i=1}^{p} T_i(x)\right] \le \frac{1}{n^{10k}}$.

# Proving lower bounds for $f_M$

$$M = \begin{pmatrix} | & & | \\ v_1 & \cdots & v_n \\ | & & | \end{pmatrix}_{m \times n}$$

$f_M(x_1, \ldots, x_n) = 1 \iff$ $\{v_i \mid x_i = 1\}$ full rank.

Random $M \in \mathbb{F}_2^{m \times n}$ $(n = m^{O(1)})$

$\Rightarrow$ All subsets of size $t = m/\log m$ independent.

$D_0$: $u \in_R \mathbb{F}_2^n$ $\quad x_i = 1 \iff u \cdot v_i = 0$

$D_0$ has uniform marginals & $t$-wise independence

$\Longrightarrow$ Sunflower lemma for $D_0$

$D_1$ is $k$-spread: $\Pr_{x \sim D_1}\left[\bigwedge_{i \in I} x_i = 1\right] \le O\left(\frac{w}{n}\right)^{|I|}$ $\forall\, |I| \le k$

$D_0$ has an $(r, 2k)$-sunflower lemma: $\quad F = \bigvee_{i=1}^{N} T_i \quad |T_i| = \ell \le 2k$, $N \ge r^\ell$

$\Rightarrow \exists F' = \bigvee_{i=1}^{p} T_i$ : $\Pr_{x \sim D_0}\left[F'(x) \ne \bigcap_{i=1}^{p} T_i(x)\right] \le \frac{1}{n^{10k}}$

Bazzi's thm + Sunflowers for $U_n$

# Explicit Matrix

$$\begin{pmatrix} 1 & \cdots & 1 \\ \alpha_1 & & \alpha_n \\ \vdots & \cdots & \vdots \\ \alpha_1^{t-1} & & \alpha_n^{t-1} \end{pmatrix} \qquad \alpha_i \in \mathbb{F}_{2^{\log n}}$$

# Explicit Matrix

$$\begin{pmatrix} 1 & & 1 \\ \alpha_1 & & \alpha_n \\ \vdots & \cdots & \vdots \\ \alpha_1^{t-1} & & \alpha_n^{t-1} \end{pmatrix} \qquad \alpha_i \in \mathbb{F}_{2^{\log n}}$$

$\mathbb{F}_2$-matrix: replace $\alpha_i$ by $M_i \in \mathbb{F}_2^{\log n \times \log n}$

representing $x \in \mathbb{F}_{2^{\log n}} \mapsto x \cdot \alpha_i \in \mathbb{F}_{2^{\log n}}$.

## Summary

→ Stronger lower bounds for monotone functions defined by linear algebra.

## Summary

- → Stronger lower bounds for monotone functions defined by linear algebra.
- → Approximation method + sunflower lemmas + Bazzi's theorem

## Summary

→ Stronger lower bounds for monotone functions defined by linear algebra.

→ Approximation method + sunflower lemmas + Bazzi's theorem

→ Better derandomization? $NC^1$ vs. non-monotone?

## Summary

→ Stronger lower bounds for monotone functions defined by linear algebra.

→ Approximation method + sunflower lemmas + Bazzi's theorem

→ Better derandomization? ($NC^1$ vs. non-monotone)?

Thank you!