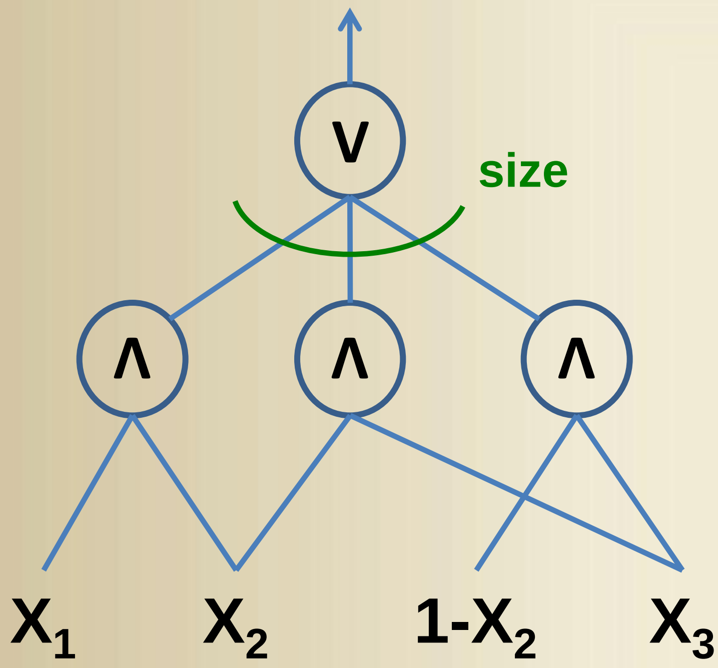
On the Complexity of DNF of Parities

Igor Shinkar
(NYU)

Joint work with Gil Cohen
(Caltech)

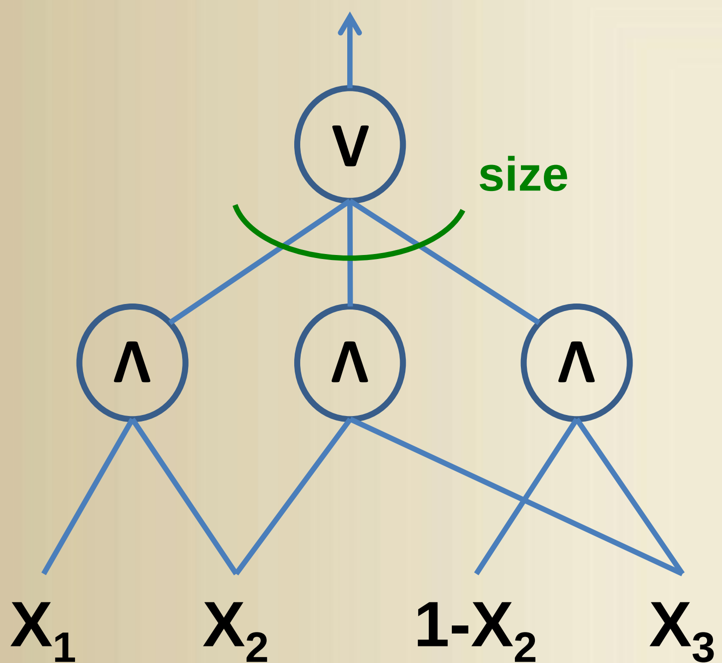
DNF and DNF$_+$

DNF

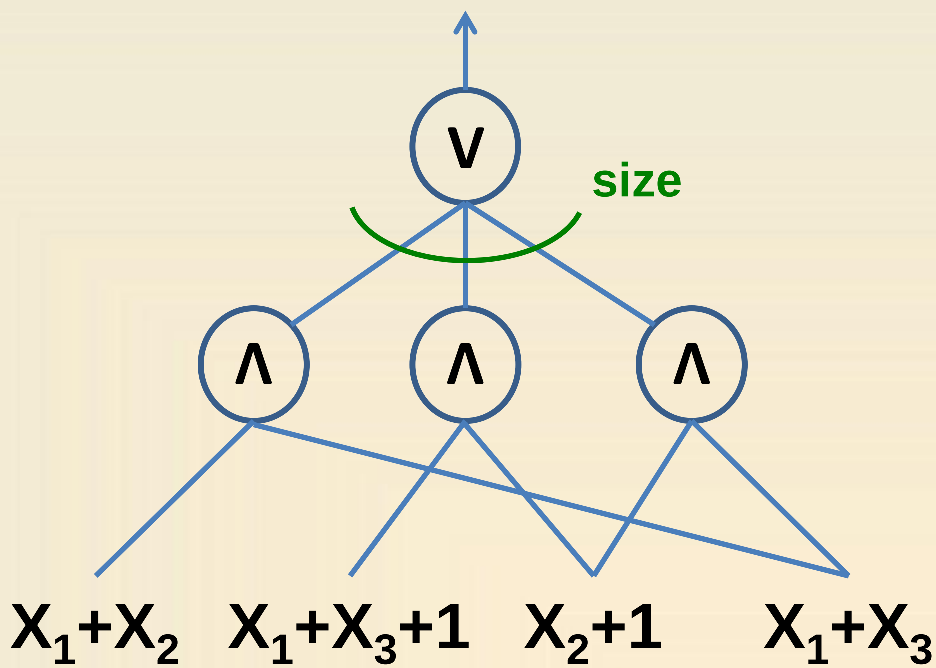


DNF and DNF_+

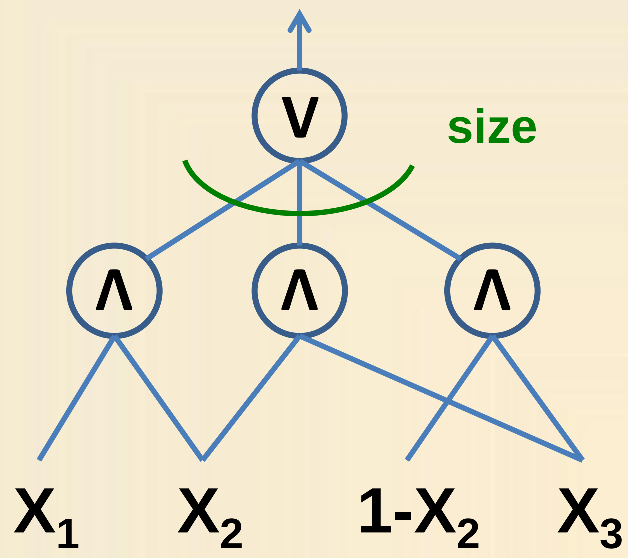
DNF



DNF_+

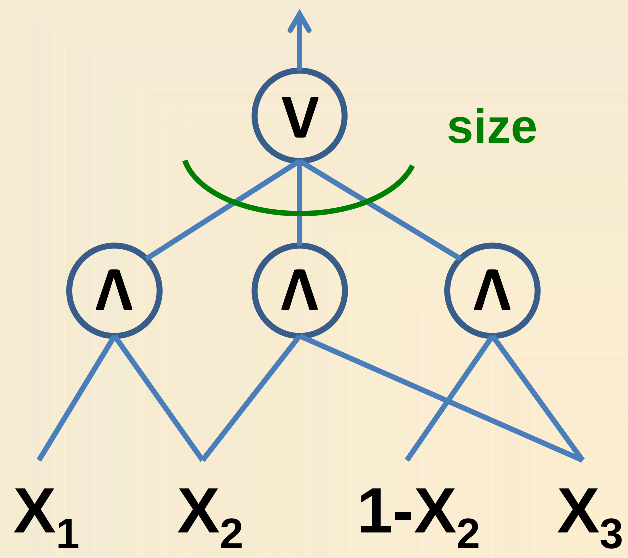


Accepting inputs of a DNF formula



Accepting inputs of a DNF formula

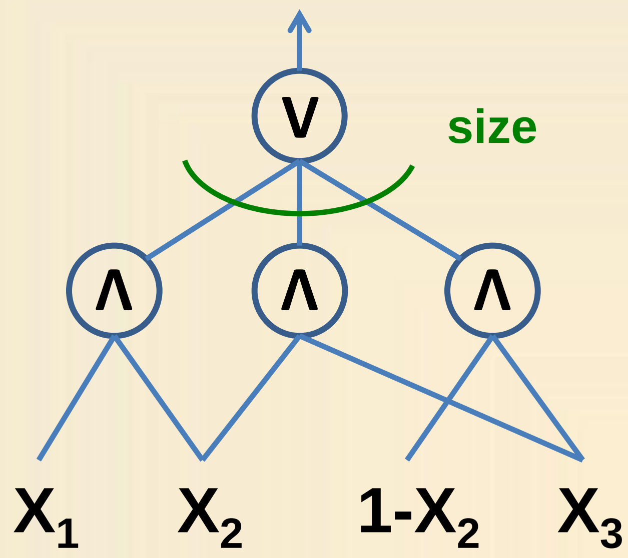
Each AND gate is an indicator of a ***subcube***
(e.g., defined by $X_2=0$ $X_3=1$).



Accepting inputs of a DNF formula

Each AND gate is an indicator of a ***subcube***
(e.g., defined by X_2=0 X_3=1).

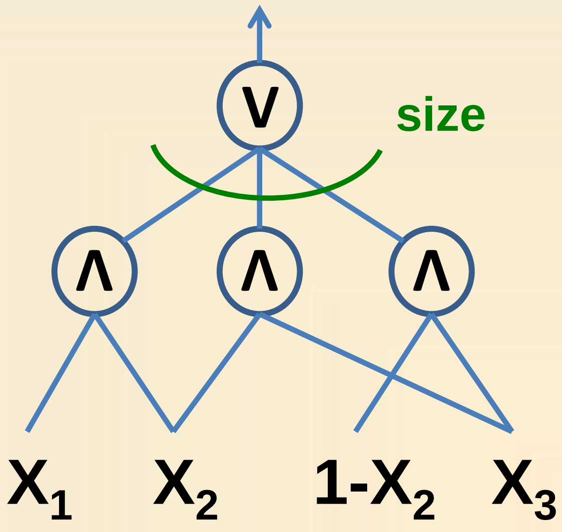
➔ DNF is an indicator of a union of subcubes.



DNF-size of a boolean function

<u>Definition</u>: Let $f: \{0,1\}^n \to \{0,1\}$

sizeDNF(f) = minimal size of a DNF computing f.

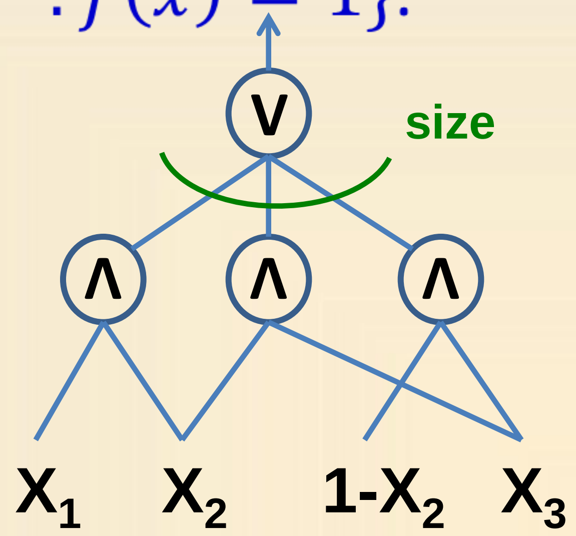


DNF-size of a boolean function

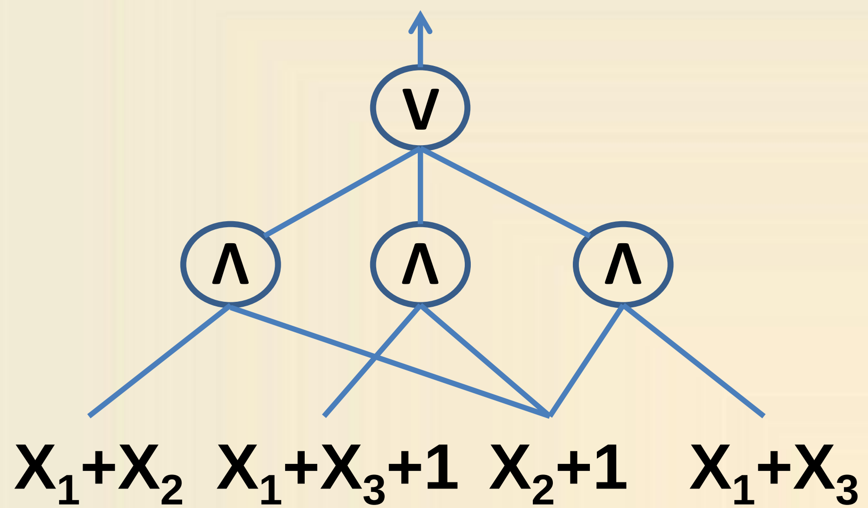
<u>Definition</u>: Let $f: \{0,1\}^n \to \{0,1\}$

sizeDNF(f) = minimal size of a DNF computing f.

Equivalently, it is the *minimal number of subcubes* needed to cover the set $\{x \in \{0,1\}^n : f(x) = 1\}$.

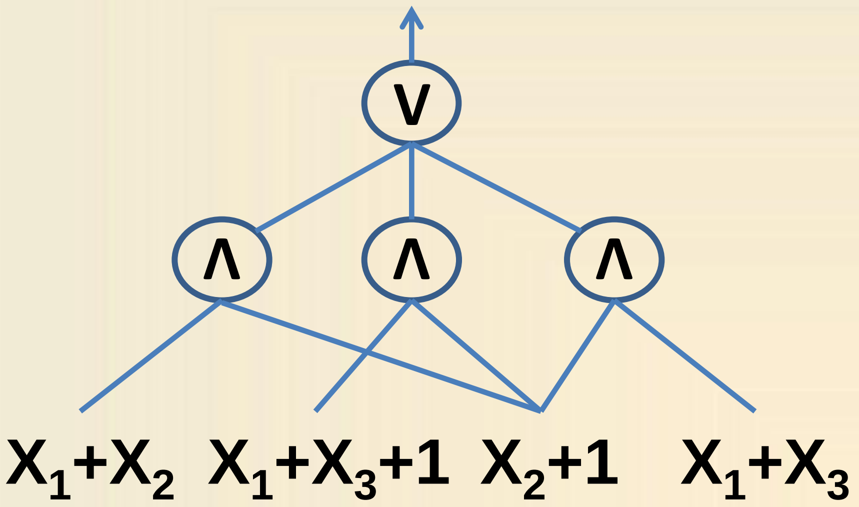


Accepting inputs of a DNF_+ formula



Accepting inputs of a DNF_+ formula

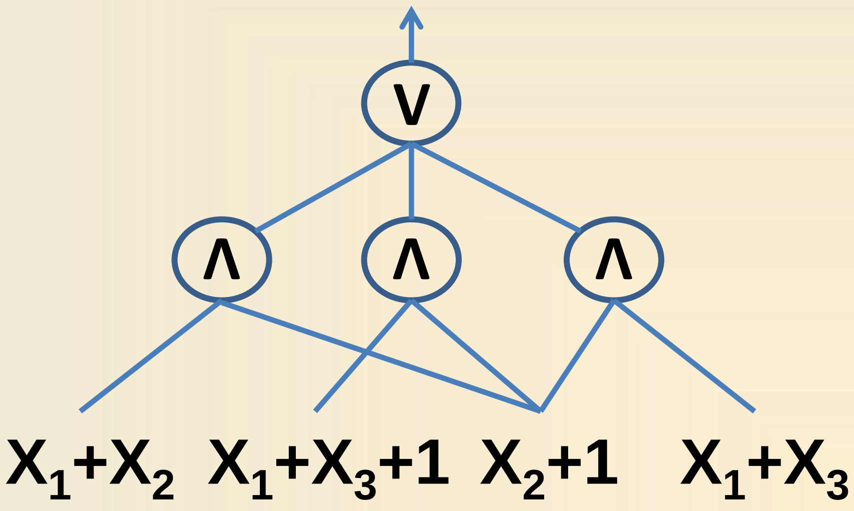
Each AND gate is an indicator of a ***subspace***.



Accepting inputs of a DNF_+ formula

Each AND gate is an indicator of a ***subspace***.

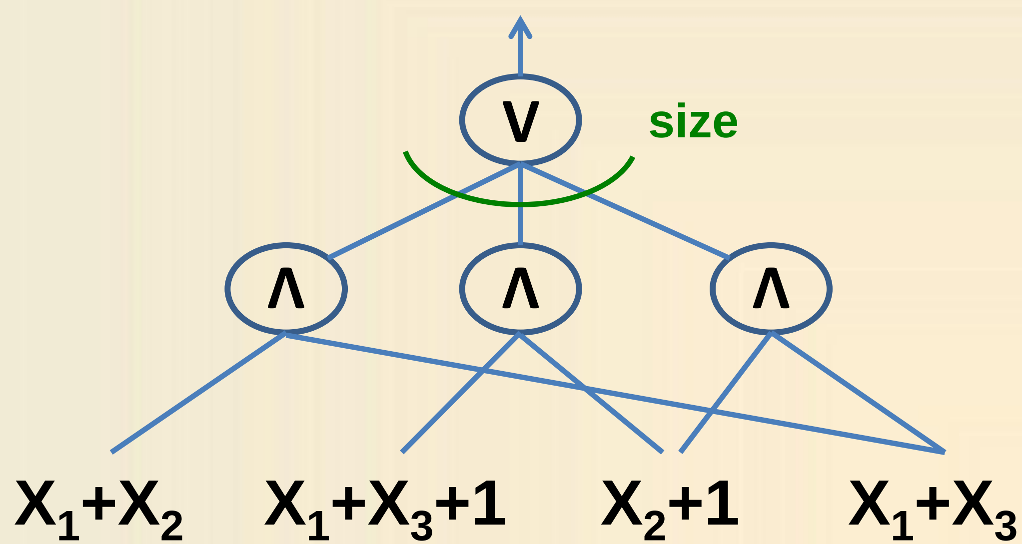
➔ DNF_+ is an indicator of a union of subspaces.



DNF$_+$ size of a boolean function

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

sizeDNF$_+$(f) = minimal size of a DNF$_+$ computing f.

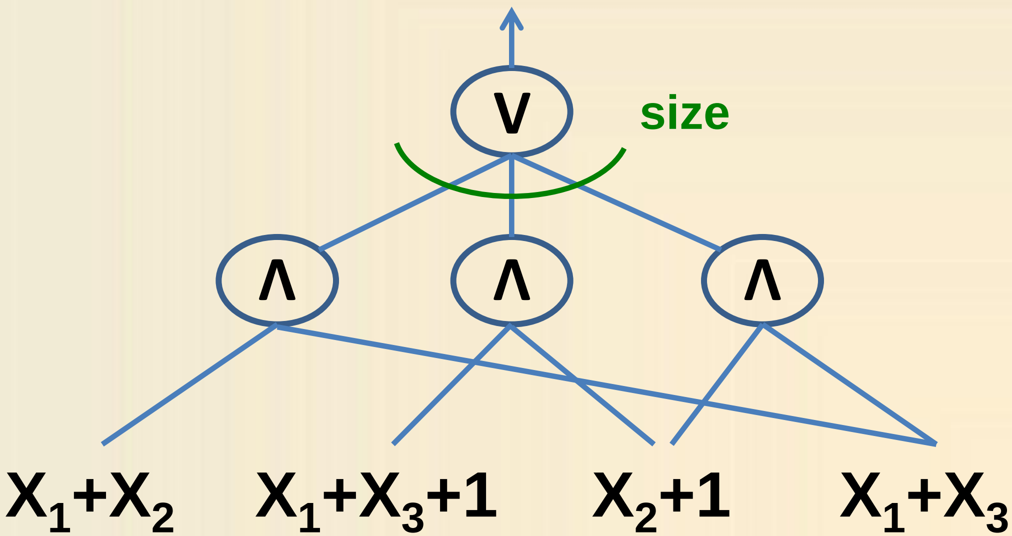


DNF_+ size of a boolean function

<u>Definition:</u> Let $f: \{0,1\}^n \rightarrow \{0,1\}$

sizeDNF$_+$(f) = minimal size of a DNF$_+$ computing f.

Equivalently, it is the minimal number of ***subspaces*** needed to cover the set $\{x \in \{0,1\}^n : f(x) = 1\}$.



Is DNF_+ stronger than DNF?

Is DNF$_+$ stronger than DNF?

The obvious example: XOR function

$$sizeDNF(XOR_n) = 2^{n-1} \qquad sizeDNF_+(XOR_n) = 1$$

Is DNF_+ stronger than DNF?

What about the Majority function?

Is DNF$_+$ stronger than DNF?

What about the Majority function?

<u>Fact</u>: $sizeDNF(Majority_n) = \binom{n}{(n+1)/2} \approx \frac{2^n}{\sqrt{n}}$.

Is DNF$_+$ stronger than DNF?

What about the Majority function?

Fact: $sizeDNF(Majority_n) = \binom{n}{(n+1)/2} \approx \frac{2^n}{\sqrt{n}}$.

The size of the middle layer of the hypercube

Is DNF$_+$ stronger than DNF?

What about the Majority function?

<u>Fact</u>: $sizeDNF(Majority_n) = \binom{n}{(n+1)/2} \approx \frac{2^n}{\sqrt{n}}$.

The size of the middle layer of the hypercube

<u>Upper bound</u>:
For each point in the middle layer take the subcube above it

Is DNF$_+$ stronger than DNF?

What about the Majority function?

Fact: $sizeDNF(Majority_n) = \binom{n}{(n+1)/2} \approx \frac{2^n}{\sqrt{n}}$.

The size of the middle layer of the hypercube

Upper bound:
For each point in the middle layer take the subcube above it

Lower bound:
Each point in the middle layer must be in a different subcube

Is DNF$_+$ stronger than DNF?

What about the Majority function?

Fact: $sizeDNF(Majority_n) = \binom{n}{(n+1)/2} \approx \frac{2^n}{\sqrt{n}}$.

Is DNF$_+$ stronger than DNF?

What about the Majority function?

Fact: $sizeDNF(Majority_n) = \binom{n}{(n+1)/2} \approx \frac{2^n}{\sqrt{n}}$.

Question: What is $sizeDNF_+(Majority_n)$?

Is DNF$_+$ stronger than DNF?

What about the Majority function?

Fact: $sizeDNF(Majority_n) = \binom{n}{(n+1)/2} \approx \frac{2^n}{\sqrt{n}}$.

Question: What is $sizeDNF_+(Majority_n)$?

Theorem: $sizeDNF_+(Majority_n) \leq poly(n) \cdot 2^{n/2}$.

Is DNF$_+$ stronger than DNF?

What about the Majority function?

Fact: $sizeDNF(Majority_n) = \binom{n}{(n+1)/2} \approx \frac{2^n}{\sqrt{n}}$.

Question: What is $sizeDNF_+(Majority_n)$?

Theorem: $sizeDNF_+(Majority_n) \leq poly(n) \cdot 2^{n/2}$.

Quadratically smaller than sizeDNF.

Is DNF$_+$ stronger than DNF?

What about the Majority function?

Fact: $sizeDNF(Majority_n) = \binom{n}{(n+1)/2} \approx \frac{2^n}{\sqrt{n}}$.

Question: What is $sizeDNF_+(Majority_n)$?

Theorem: $sizeDNF_+(Majority_n) \leq poly(n) \cdot 2^{n/2}$.

Tight up to poly(n) factor

DNF$_+$ complexity of symmetric functions

Theorem 1: $sizeDNF_+(Majority_n) \leq poly(n) \cdot 2^{n/2}$.

Quadratically smaller than sizeDNF

DNF_+ complexity of symmetric functions

Theorem 1: $sizeDNF_+(Majority_n) \leq poly(n) \cdot 2^{n/2}$.

Quadratically smaller than sizeDNF

Theorem 2: For every symmetric $f : \{0,1\}^n \to \{0,1\}$

$$sizeDNF_+(f) \leq poly(n) \cdot 1.5^n.$$

Compare to sizeDNF(XOR) = 2^{n-1}

A general upper bound on DNF$_+$ complexity

Theorem 3: For every $f: \{0,1\}^n \to \{0,1\}$

$$sizeDNF_+(f) = O(2^n/n)\ .$$

A general upper bound on DNF$_+$ complexity

<u>Theorem 3</u>: For every $f:\{0,1\}^n \rightarrow \{0,1\}$

$$sizeDNF_+(f) = O(2^n/n)\ .$$

Smaller than sizeDNF(XOR) by O(n) factor

A general upper bound on DNF$_+$ complexity

Theorem 3: For every $f: \{0,1\}^n \to \{0,1\}$

$$sizeDNF_+(f) = O(2^n/n)\ .$$

Almost tight:
Affine dispersers for dimension O(log(n)) require
$$\boldsymbol{sizeDNF(f) \geq 2^n/poly(n).}$$

More results in the paper…

Some proof sketches:

DNF_{+} complexity of symmetric functions

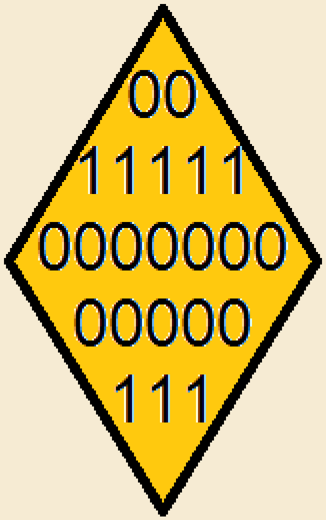
Theorem 2: For every symmetric $f: \{0,1\}^n \rightarrow \{0,1\}$

$$sizeDNF_{+}(f) \leq poly(n) \cdot 1.5^n.$$

DNF_+ complexity of symmetric functions

<u>Theorem 2</u>: For every symmetric $f\colon\{0,1\}^n \to \{0,1\}$

$$sizeDNF_+(f) \le poly(n) \cdot 1.5^n.$$



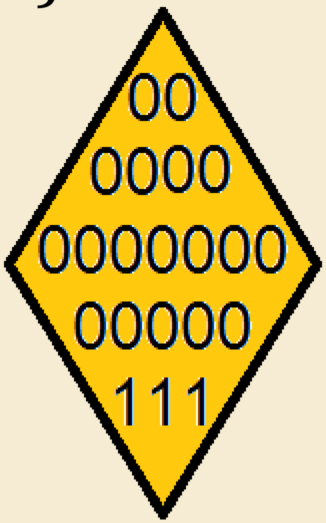
DNF$_+$ complexity of symmetric functions

Theorem 2: For every symmetric $f: \{0,1\}^n \to \{0,1\}$

$$sizeDNF_+(f) \leq poly(n) \cdot 1.5^n.$$

Proof: Let $k \in \{0,1, \dots, n\}$.

Let g_k be the indicator of the k'th layer of $\{0,1\}^n$.



DNF_+ complexity of symmetric functions

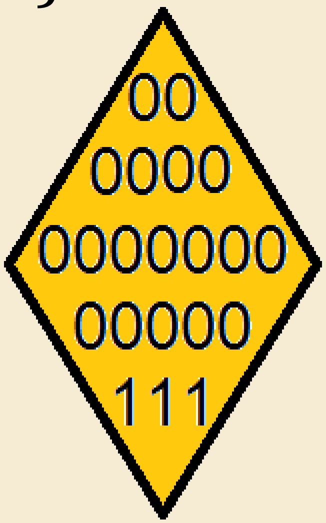
<u>Theorem 2</u>: For every symmetric $f: \{0,1\}^n \to \{0,1\}$

$$sizeDNF_+(f) \leq poly(n) \cdot 1.5^n.$$

<u>Proof</u>: Let $k \in \{0,1,\ldots,n\}$.

Let g_k be the indicator of the k'th layer of $\{0,1\}^n$.

It is enough to prove the theorem for g_k.

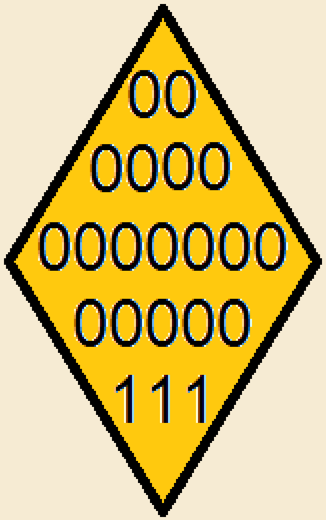


DNF_+ complexity of symmetric functions

Theorem 2': Let $k \in \{0,1,\dots,n/2\}$.
Let g_k be the indicator of the k'th layer of $\{0,1\}^n$. Then

$$sizeDNF_+(g_k) \leq poly(n) \cdot 2^{(H(p)-p)n},$$

where $p = \frac{k}{n} \in [0,0.5]$.



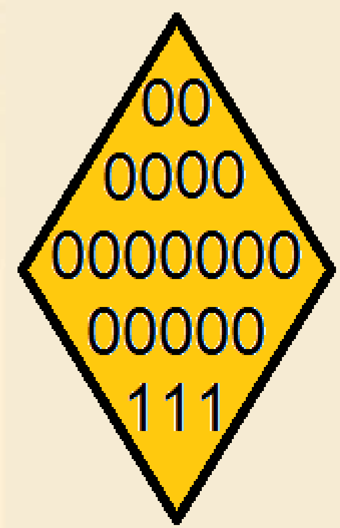
DNF$_+$ complexity of symmetric functions

<u>Theorem 2'</u>: Let $k \in \{0,1,\ldots,n/2\}$.
Let g_k be the indicator of the k'th layer of $\{0,1\}^n$. Then

$$sizeDNF_+(g_k) \le poly(n) \cdot 2^{(H(p)-p)n},$$

where $p = \frac{k}{n} \in [0,0.5]$.

<u>Fact</u>: $2^{(H(p)-p)n} \le 1.5^n$ for all $p \in [0,0.5]$.



DNF$_+$ complexity of symmetric functions

Theorem 2' [special case of $k = n/2$]:

Let $g_{n/2}$ be the indicator of the *middle* layer of $\{0,1\}^n$.

Then

$$sizeDNF_+(g_{n/2}) \leq n \cdot 2^{n/2}.$$

DNF_+ complexity of symmetric functions

Theorem 2’ [special case of $k = n/2$]:
Let $g_{n/2}$ be the indicator of the *middle* layer of $\{0,1\}^n$.
Then

$$sizeDNF_+\left(g_{n/2}\right) \leq n \cdot 2^{n/2}.$$

Proof:

DNF_+ complexity of symmetric functions

Theorem 2’ [special case of $k = n/2$]:
Let $g_{n/2}$ be the indicator of the *middle* layer of $\{0,1\}^n$.
Then

$$sizeDNF_+\left(g_{n/2}\right) \leq n \cdot 2^{n/2}.$$

Proof:

Step 1: Find an affine subspace V of $\dim(V) = n/2$ such that V is contained in the middle layer of $\{0,1\}^n$.

DNF$_+$ complexity of symmetric functions

Theorem 2' [special case of $k = n/2$]:
Let $g_{n/2}$ be the indicator of the *middle* layer of $\{0,1\}^n$.
Then

$$sizeDNF_+(g_{n/2}) \leq n \cdot 2^{n/2}.$$

Proof:

Step 1: Find an affine subspace V of $\dim(V) = n/2$ such that V is contained in the middle layer of $\{0,1\}^n$.

One subspace covers $2^{n/2}$ points

DNF$_+$ complexity of symmetric functions

Theorem 2' [special case of $k = n/2$]:
Let $g_{n/2}$ be the indicator of the *middle* layer of $\{0,1\}^n$.
Then

$$sizeDNF_+\left(g_{n/2}\right) \leq n \cdot 2^{n/2}.$$

Proof:

Step 1: Find an affine subspace V of $\dim(V) = n/2$ such that V is contained in the middle layer of $\{0,1\}^n$.

DNF$_+$ complexity of symmetric functions

Theorem 2' [special case of $k = n/2$]:
Let $g_{n/2}$ be the indicator of the *middle* layer of $\{0,1\}^n$.
Then

$$sizeDNF_+(g_{n/2}) \leq n \cdot 2^{n/2}.$$

Proof:

Step 1: Find an affine subspace V of $\dim(V) = n/2$ such that V is contained in the middle layer of $\{0,1\}^n$.

Step 2: Permute the coordinates and find $\sim n2^{n/2}$ subspaces that together cover the entire middle layer.

DNF$_+$ complexity of symmetric functions

Step 1: Find an affine subspace V of $\dim(V) = n/2$ such that V is contained in the middle layer of $\{0,1\}^n$.

DNF$_+$ complexity of symmetric functions

<u>Step 1</u>: Find an affine subspace V of $\dim(V) = n/2$ such that V is contained in the middle layer of $\{0,1\}^n$.

$$\text{Define } V = \{x \in \{0,1\}^n : \begin{matrix} x_1 + x_2 = 1 \\ x_3 + x_4 = 1 \\ \dots \\ x_{n-1} + x_n = 1 \end{matrix} \}$$

DNF_+ complexity of symmetric functions

Step 2: Permute the coordinates.

DNF_+ complexity of symmetric functions

Step 2: Permute the coordinates.

Pick a random permutation $\sigma \in S_n$

Define $V_\sigma = \{ \; x \in \{0,1\}^n \colon \begin{matrix} x_{\sigma(1)} + x_{\sigma(2)} = 1 \\ x_{\sigma(3)} + x_{\sigma(4)} = 1 \\ \cdots \\ x_{\sigma(n-1)} + x_{\sigma(n)} = 1 \end{matrix} \; \}$

DNF_+ complexity of symmetric functions

<u>Completing the proof:</u>

For a random $\sigma \in S_n$ every x is contained in V_σ with probability

$$\Pr[x \in V_\sigma] = \frac{2^{n/2}}{\binom{n}{n/2}} \approx 2^{-n/2}$$

DNF$_+$ complexity of symmetric functions

Completing the proof:

For a random $\sigma \in S_n$ every x is contained in V_σ with probability

$$\Pr[x \in V_\sigma] = \frac{2^{n/2}}{\binom{n}{n/2}} \approx 2^{-n/2}$$

Taking $n2^{n/2}$ random permutations will cover all x's with high probability. Therefore

$$sizeDNF_+(g_{n/2}) \leq n \cdot 2^{n/2}$$

A general upper bound on DNF_+ complexity

Theorem 3: For every $f : \{0,1\}^n \to \{0,1\}$

$$sizeDNF_+(f) = O(2^n/n)\ .$$

A general upper bound on DNF$_+$ complexity

Theorem 3: For every $f: \{0,1\}^n \rightarrow \{0,1\}$

$$sizeDNF_+(f) = O(2^n/n)\ .$$

Proof: Follows immediately from the following claim:

Claim: Let $A \subset \{0,1\}^n$ of size $|A| = \epsilon 2^n$ ($\epsilon > 2^{-n/4}$).
Then, A contains an affine subspace V of dimension

$$\dim(V) > \log(n) - \log\log 1/\epsilon\ - 2.$$

A general upper bound on DNF_+ complexity

Claim: Let $A \subset \{0,1\}^n$ of size $|A| = \epsilon 2^n$ ($\epsilon > 2^{-n/4}$).
Then, A contains an affine subspace V of dimension

$$\dim(V) > \log(n) - \log\log 1/\epsilon \; - 2.$$

A general upper bound on DNF_+ complexity

<u>Claim</u>: Let $A \subset \{0,1\}^n$ of size $|A| = \epsilon 2^n$ ($\epsilon > 2^{-n/4}$).
Then, A contains an affine subspace V of dimension

$$\dim(V) > \log(n) - \log\log 1/\epsilon \; - 2.$$

<u>Proof</u>:

Gowers-Cauchy-Schwartz inequality.

$$\Pr[x + Span(y_1, \dots, y_d) \subset A] > \epsilon^{2^d}$$

Open problems

1. Give an explicit $f\colon \{0,1\}^n \to \{0,1\}$ such that a DNF_+ circuit that ϵ-approximates f must be of size at least 1.1^{n}.

2. Can small DNF_+ approximate an affine extractor?

Thank You