On the Complexity of DNF of Parities

Igor Shinkar
(NYU)

Joint work with Gil Cohen
(Caltech)
DNF and DNF$_+$

DNF

\[
\begin{align*}
&\land \\
&\land \\
&\land
\end{align*}
\]

\[
\begin{align*}
&X_1 \\
&X_2 \\
&1-X_2 \\
&X_3
\end{align*}
\]
DNF and DNF$_+$

DNF

\[
\begin{align*}
V \quad \Lambda \quad \Lambda \\
\Lambda \quad \Lambda \quad \Lambda \\
X_1 \quad X_2 \quad 1-X_2 \quad X_3
\end{align*}
\]

DNF$_+$

\[
\begin{align*}
V \quad \Lambda \quad \Lambda \\
\Lambda \quad \Lambda \quad \Lambda \\
X_1+X_2 \quad X_1+X_3+1 \quad X_2+1 \quad X_1+X_3
\end{align*}
\]
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 $X_2=0 \ X_3=1$).

\[
\begin{array}{c}
\text{size} \\
\vee \\
\wedge \\
\wedge \\
\wedge \\
X_1 \quad X_2 \quad 1-X_2 \quad X_3
\end{array}
\]
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

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

\[
\text{sizeDNN}(f) = \text{minimal size of a DNF computing } f.
\]
DNF-size of a boolean function

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

$$\text{size} \text{DNF}(f) = \text{minimal size of a DNF computing } f.$$  

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

\[ X_1 + X_2 \quad X_1 + X_3 + 1 \quad X_2 + 1 \quad X_1 + X_3 \]
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**.

$\Rightarrow$ DNF$_+$ is an indicator of a union of subspaces.
**DNF⁺ size of a boolean function**

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

\[ \text{size} \text{DNF}_\oplus(f) = \text{minimal size of a DNF}_\oplus \text{ computing } f. \]
DNF$_+$ size of a boolean function

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

$$\text{sizeDNF}_+(f) = \text{minimal size of a DNF}_+ \text{ computing } f.$$  

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

![Diagram showing DNF_+ size with variables and logical operations]
Is DNF_+ stronger than DNF?
Is $\text{DNF}_+$ stronger than DNF?

The obvious example: XOR function

$$\text{sizeDNF}(\text{XOR}_n) = 2^{n-1} \quad \text{sizeDNF}_+(\text{XOR}_n) = 1$$
Is $\text{DNF}_+$ stronger than DNF?

What about the Majority function?
Is $\text{DNF}_+ \text{ stronger than DNF}$?

What about the $\text{Majority}$ function?

Fact: $\text{size}_{\text{DNF}}(\text{Majority}_n) = \binom{n}{(n+1)/2} \approx \frac{2^n}{\sqrt{n}}$. 

Is DNF$_+$ stronger than DNF?

What about the Majority function?

**Fact:** $\text{size}_{\text{DNF}}(\text{Majority}_n) = \binom{n}{(n+1)/2} \approx \frac{2^n}{\sqrt{n}}$. 

*The size of the middle layer of the hypercube*
Is DNF+ stronger than DNF?

What about the Majority function?

Fact: $\text{size} \text{DNF}(\text{Majority}_n) = \binom{n}{(n+1)/2} \approx \frac{2^n}{\sqrt{n}}$.  

The size of the middle layer of the hypercube

Upper bound:  
For each point in the middle layer take the subcube above it
Is DNF⁺ stronger than DNF?

What about the **Majority** function?

**Fact:** \(\text{size DNF}(\text{Majority}_n) = \binom{n}{(n+1)/2} \approx \frac{2^n}{\sqrt{n}}.\)

- **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.

**The size of the middle layer of the hypercube**
Is $\text{DNF}_+$ stronger than DNF?

What about the $\text{Majority}$ function?

**Fact:** $\text{size}_{\text{DNF}}(\text{Majority}_n) = \binom{n}{(n+1)/2} \approx \frac{2^n}{\sqrt{n}}$. 
Is $\text{DNF}_+^+$ stronger than DNF?

What about the $\text{Majority}$ function?

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

**Question:** What is $\text{sizeDNF}_+(\text{Majority}_n)$?
Is $\text{DNF}_+ \text{ stronger than DNF?}$

What about the $\text{Majority}$ function?

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

**Question:** What is $\text{sizeDNF}_+(\text{Majority}_n)$?

**Theorem:** $\text{sizeDNF}_+(\text{Majority}_n) \leq \text{poly}(n) \cdot 2^{n/2}.$
Is DNF$_+^*$ stronger than DNF?

What about the **Majority** function?

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

**Question**: What is $\text{sizeDNF}_+(\text{Majority}_n)$?

**Theorem**: $\text{sizeDNF}_+(\text{Majority}_n) \leq \text{poly}(n) \cdot 2^{n/2}.$

*Quadratically smaller than sizeDNF.*
Is DNF$_+^*$ stronger than DNF?

What about the Majority function?

**Fact**: \( \text{size} \text{DNF}(\text{Majority}_{n}) = \binom{n}{(n+1)/2} \approx \frac{2^n}{\sqrt{n}}. \)

**Question**: What is \( \text{sizeDNF}_+(\text{Majority}_{n}) \)?

**Theorem**: \( \text{sizeDNF}_+(\text{Majority}_{n}) \leq \text{poly}(n) \cdot 2^{n/2}. \)

**Tight up to poly(n) factor**
DNF\(_+\) complexity of symmetric functions

**Theorem 1:** \( \text{size} \text{DNF}_+(\text{Majority}_n) \leq \text{poly}(n) \cdot 2^{n/2} \).

*Quadratically smaller than size\text{DNF}
DNF$_+$ complexity of symmetric functions

**Theorem 1:** \( \text{sizeDNF}_+(\text{Majority}_n) \leq \text{poly}(n) \cdot 2^{n/2} \).  

*Quadratically smaller than sizeDNF*

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

\[ \text{sizeDNF}_+(f) \leq \text{poly}(n) \cdot 1.5^n. \]

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

A general upper bound on DNF_+ complexity

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

\[ sizeD\text{NF}_+(f) = O\left(\frac{2^n}{n}\right) . \]
A general upper bound on DNF\(_+\) complexity

**Theorem 3**: For every \( f : \{0,1\}^n \rightarrow \{0,1\} \)

\[
\text{size}_{\text{DNF}_+}(f) = O\left(\frac{2^n}{n}\right).
\]

*Smaller than size_{\text{DNF}(XOR)} by O(n) factor*
A general upper bound on $\text{DNF}_+$ complexity

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

$$\text{sizeDNF}_+(f) = O\left(\frac{2^n}{n}\right).$$

*Almost tight:*

*Affine dispersers for dimension $O(\log(n))$ require*

$$\text{sizeDNF}(f) \geq \frac{2^n}{\text{poly}(n)}.$$
More results in the paper...
Some proof sketches:
**DNF**\(_+\) complexity of symmetric functions

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

\[
\text{sizeDNF}_+(f) \leq \text{poly}(n) \cdot 1.5^n.
\]
DNF$_+$ complexity of symmetric functions

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

\[
\text{size} \text{DNF}_+(f) \leq \text{poly}(n) \cdot 1.5^n.
\]
**Theorem 2:** For every symmetric $f : \{0,1\}^n \rightarrow \{0,1\}$

\[
size_{DNF_+}(f) \leq \text{poly}(n) \cdot 1.5^n.
\]

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

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

00
0000
000000
000000
111
DNF$_+$ complexity of symmetric functions

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

$$\text{size} \text{DNF}_+(f) \leq \text{poly}(n) \cdot 1.5^n.$$ 

**Proof**: 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 $g_k$. 

![Diamond with binary values](image)
DNF$_+$ complexity of symmetric functions

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

\[
\text{size} \text{DNF}_+(g_k) \leq \text{poly}(n) \cdot 2^{(H(p)-p)n},
\]

where $p = \frac{k}{n} \in [0,0.5]$. 
DNF$_+$ complexity of symmetric functions

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

$$\text{size} \text{DNF}_+(g_k) \leq \text{poly}(n) \cdot 2^{(H(p)-p)n},$$

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

**Fact**: $2^{(H(p)-p)n} \leq 1.5^n$ 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

$$\text{size}_+ \text{DNF} \left(g_{n/2}\right) \leq n \cdot 2^{n/2}.$$
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

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

**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

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

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

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

$$\text{size} \text{DNF}_+(g_{n/2}) \leq n \cdot 2^{n/2}.$$ 

**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\textsubscript{+} 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

$$\text{sizeDNF}_+(g_{n/2}) \leq n \cdot 2^{n/2}.$$  

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

\[
\text{sizeDNF}_+(g_{n/2}) \leq n \cdot 2^{n/2}.
\]

**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

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

Define $V = \{x \in \{0,1\}^n : \begin{align*} x_1 + x_2 &= 1 \\ x_3 + x_4 &= 1 \\ \cdots \\ x_{n-1} + x_n &= 1 \}$. 

DNF$^+_\pm$ complexity of symmetric functions

Step 2: Permute the coordinates.
DNF\_p complexity of symmetric functions

**Step 2:** Permute the coordinates.

Pick a random permutation $\sigma \in S_n$

Define $V_\sigma = \{ x \in \{0,1\}^n : x_{\sigma(1)} + x_{\sigma(2)} = 1, x_{\sigma(3)} + x_{\sigma(4)} = 1, \ldots, x_{\sigma(n-1)} + x_{\sigma(n)} = 1 \}$
DNF\_+ complexity of symmetric functions

Completing the proof:
For a random \( \sigma \in S_n \) every \( x \) is contained in \( V_\sigma \) 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 $V_\sigma$ 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

$$\text{size}_{\text{DNF}}(g_{n/2}) \leq n \cdot 2^{n/2}$$
A general upper bound on $\text{DNF}_+$ complexity

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

$$\text{size}_{\text{DNF}_+}(f) = O\left(\frac{2^n}{n}\right).$$
A general upper bound on DNF$_+$ complexity

**Theorem 3:** For every $f : \{0,1\}^n \rightarrow \{0,1\}$
\[
\text{sizeDNF}_+(f) = O(2^n/n).
\]

**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
\[
\text{dim}(V) > \log(n) - \log \log 1/\epsilon - 2.
\]
A general upper bound on $\text{DNF}_+ \text{ complexity}$

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

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

**Proof:**

Gowers-Cauchy-Schwartz inequality.

$$\Pr[x + \text{Span}(y_1, ..., y_d) \subseteq A] > \epsilon^{2^d}$$
Open problems

1. Give an explicit $f: \{0,1\}^n \rightarrow \{0,1\}$ such that a DNF$_+$ circuit that $\epsilon$-approximates $f$ must be of size at least $1.1^n$.

2. Can small DNF$_+$ approximate an affine extractor?
Thank You