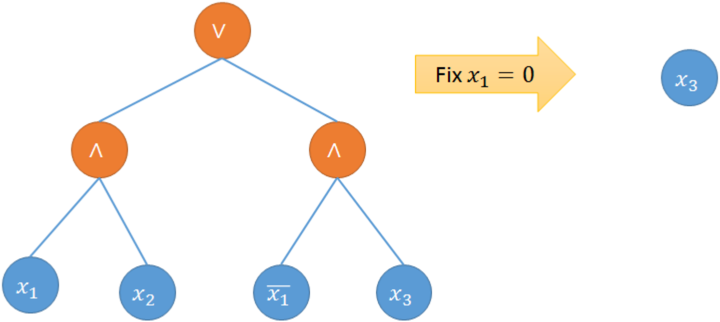
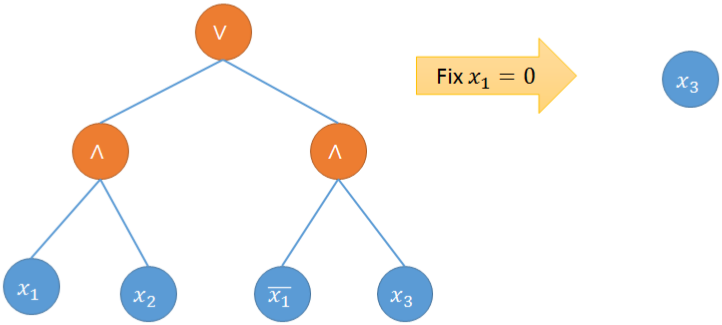
Shrinkage of De Morgan Formulae using Spectral Techniques

Avishay Tal

Weizmann Institute of Science, Rehovot

December 2014


∨
∧
∧
x_1
x_2
$\overline{x_1}$
x_3
Fix $x_1 = 0$
x_3



No coincidence!

- A **De Morgan formula**, F, is a binary tree whose leaves are labeled with $\{x_1, \ldots, x_n, \neg x_1, \ldots, \neg x_n\}$ and whose internal nodes are labeled with $\mathrm{AND}, \mathrm{OR}$ gates.
- The **size** of the formula, $L(F)$, is the number of leaves in the tree.

Definitions and Challenges

- A **De Morgan formula**, F, is a binary tree whose leaves are labeled with $\{x_1, \dots, x_n, \neg x_1, \dots, \neg x_n\}$ and whose internal nodes are labeled with $\mathrm{AND}, \mathrm{OR}$ gates.
- The **size** of the formula, $L(F)$, is the number of leaves in the tree.
- for a Boolean **function** $f : \{0,1\}^n \to \{0,1\}$:

$$L(f) = \min_{F:F \text{ computes } f} L(F) \; .$$

Definitions and Challenges

- A **De Morgan formula**, F, is a binary tree whose leaves are labeled with $\{x_1, \ldots, x_n, \neg x_1, \ldots, \neg x_n\}$ and whose internal nodes are labeled with $\mathrm{AND}, \mathrm{OR}$ gates.
- The **size** of the formula, $L(F)$, is the number of leaves in the tree.
- for a Boolean **function** $f : \{0,1\}^n \to \{0,1\}$:

$$L(f) = \min_{F : F \text{ computes } f} L(F) .$$

- **The Challenge:** Find an explicit function f (in **P**) with $L(f) = n^{\omega(1)}$.
- Still open, even for **NEXP**.

Lower Bounds from Shrinkage

- A **restriction** is a function $\rho : \{1, \dots, n\} \to \{0, 1, *\}$.
- Given a function $f : \{0,1\}^n \to \{0,1\}$ the **restricted function** $f|_\rho : \{0,1\}^n \to \{0,1\}$ is defined as:

$$f|_\rho(x) = f(y) \quad ; \quad y_i = \begin{cases} x_i, & \rho(i) = * \\ \rho(i), & \textit{otherwise} \end{cases} .$$

Lower Bounds from Shrinkage

- A **restriction** is a function $\rho : \{1, \ldots, n\} \to \{0, 1, *\}$.
- Given a function $f : \{0,1\}^n \to \{0,1\}$ the **restricted function** $f|_\rho : \{0,1\}^n \to \{0,1\}$ is defined as:

$$f|_\rho(x) = f(y) \quad ; \quad y_i = \begin{cases} x_i, & \rho(i) = * \\ \rho(i), & otherwise \end{cases} .$$

- $\mathcal{R}_p$ is a distribution over restrictions. For each $i \in [n]$, ind.

$$\rho(i) = \begin{cases} *, & \text{w.p. p} \\ 0, & \text{w.p. (1-p)/2} \\ 1, & \text{w.p. (1-p)/2} \end{cases} .$$

Lower Bounds from Shrinkage

- A **restriction** is a function $\rho : \{1, \ldots, n\} \to \{0, 1, *\}$.
- Given a function $f : \{0,1\}^n \to \{0,1\}$ the **restricted function** $f|_\rho : \{0,1\}^n \to \{0,1\}$ is defined as:

$$f|_\rho(x) = f(y) \quad ; \quad y_i = \begin{cases} x_i, & \rho(i) = * \\ \rho(i), & otherwise \end{cases} .$$

- $\mathcal{R}_p$ is a distribution over restrictions. For each $i \in [n]$, ind.

$$\rho(i) = \begin{cases} *, & \text{w.p. p} \\ 0, & \text{w.p. (1-p)/2} \\ 1, & \text{w.p. (1-p)/2} \end{cases} .$$

- **Theorem [Subbotovskaya '61]**:

$$\mathop{\mathbf{E}}_{\rho \sim \mathcal{R}_p} [L(f|_\rho)] = O(p^{1.5} L(f) + 1) .$$

Lower Bounds from Shrinkage

- **Theorem [Sub '61]**: $\mathbf{E}_{\rho\sim\mathcal{R}_p}[L(f|_\rho)] = O(p^{1.5}L(f)+1)$.
- $\Leftrightarrow L(f) \geq \frac{\Omega(\mathbf{E}[L(f|_\rho)])-1}{p^{1.5}}$
- $\implies L(Parity) \geq \Omega(n^{1.5})$.

Lower Bounds from Shrinkage

- **Theorem [Sub '61]**: $\mathbf{E}_{\rho\sim\mathcal{R}_p}[L(f|_\rho)] = O(p^{1.5}L(f)+1)$.
- $\Leftrightarrow L(f) \geq \frac{\Omega(\mathbf{E}[L(f|_\rho)])-1}{p^{1.5}}$
- $\implies L(Parity) \geq \Omega(n^{1.5})$.
- **[Andreev '87]** gave an explicit function $A : \{0,1\}^n \to \{0,1\}$ such that for $p \approx \log(n)/n$

$$\mathop{\mathbf{E}}_{\rho\sim\mathcal{R}_p}[L(A|_\rho)] \geq \Omega\left(\frac{n}{\log\log n}\right) .$$

- $\implies L(A) \geq \Omega\left(\frac{n^{2.5}}{\mathrm{poly}\log(n)}\right)$

- **Theorem [Sub '61]**: $\mathbf{E}_{\rho\sim\mathcal{R}_p}[L(f|_\rho)] = O(p^{1.5}L(f)+1)$.
- $\Leftrightarrow L(f) \geq \frac{\Omega(\mathbf{E}[L(f|_\rho)])-1}{p^{1.5}}$
- $\implies L(Parity) \geq \Omega(n^{1.5})$.
- **[Andreev '87]** gave an explicit function $A: \{0,1\}^n \to \{0,1\}$ such that for $p \approx \log(n)/n$

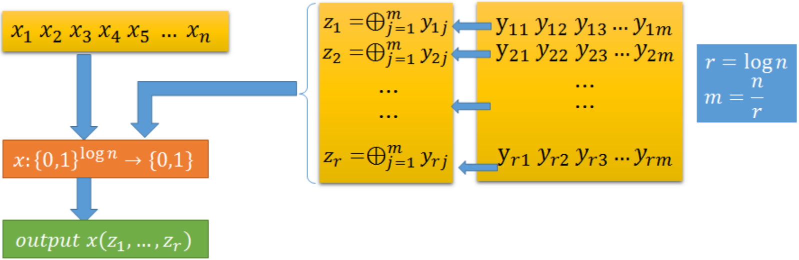
$$\mathop{\mathbf{E}}_{\rho\sim\mathcal{R}_p}[L(A|_\rho)] \geq \Omega\left(\frac{n}{\log\log n}\right) .$$

- $\implies L(A) \geq \Omega\left(\frac{n^{2.5}}{\text{poly}\log(n)}\right)$
- **[Håstad '93]** improved Subbotovskaya's result:

$$\mathop{\mathbf{E}}_{\rho\sim\mathcal{R}_p}[L(f|_\rho)] = O\left(p^2\left(1+\log^{3/2}(1/p)\right)L(f)+1\right)$$

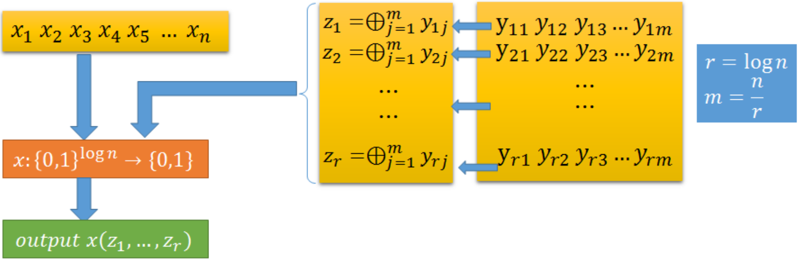
Andreev's Function

$$A : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$$



Andreev's Function

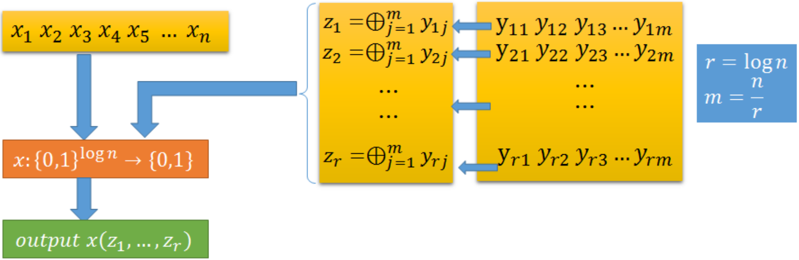
$$A : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$$



Let $A_h(y) = A(tt(h), y)$ for the **hardest** $h : \{0,1\}^{\log n} \to \{0,1\}$, then $L(A) \geq L(A_h)$.

Andreev's Function

$$A : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$$



Let $A_h(y) = A(tt(h), y)$ for the **hardest** $h : \{0,1\}^{\log n} \to \{0,1\}$, then $L(A) \geq L(A_h)$.

For $p = \frac{\log\log(n)\log(n)}{n}$, $\quad \mathbf{E}_{\rho\sim\mathcal{R}_p}[L(A_h|_\rho)] \geq \Omega(L(h)) \geq \Omega\left(\frac{n}{\log\log(n)}\right)$

Main Theorem:

$$\mathop{\mathbf{E}}_{\rho\sim\mathcal{R}_p}[L(f|_\rho)] = O(p^2 L(f) + 1)\ .$$

Main Theorem:

$$\mathop{\mathbf{E}}_{\rho\sim\mathcal{R}_p}[L(f|_\rho)] = O(p^2L(f)+1)\ .$$

The result is **tight** as demonstrated by *Parity*.

Main Theorem:

$$\mathop{\mathbf{E}}_{\rho\sim\mathcal{R}_p}[L(f|_\rho)] = O(p^2 L(f) + 1)\ .$$

The result is **tight** as demonstrated by *Parity*.

Applications:

- Theorem $\implies L(A) \geq \Omega\left(\frac{n^3}{\log^2(n)\log^3\log(n)}\right)$.
- This is **tight** up to $\log^3\log(n)$ factor.
- Theorem $\implies$ improved analysis of **average case** lower bound by **[Komargodski Raz T '13]**.

- Every function $f : \{-1,1\}^n \to \{-1,1\}$ has a unique (Fourier) representation as a multilinear polynomial

$$f(x) = \sum_{S \subseteq [n]} \hat{f}(S) \prod_{i \in S} x_i$$

where $\hat{f}(S) = \mathbf{E}_x[f(x) \prod_{i \in S} x_i]$.

- Every function $f : \{-1,1\}^n \to \{-1,1\}$ has a unique (Fourier) representation as a multilinear polynomial

$$f(x) = \sum_{S \subseteq [n]} \hat{f}(S) \prod_{i \in S} x_i$$

where $\hat{f}(S) = \mathbf{E}_x[f(x) \prod_{i \in S} x_i]$.

- **Parseval's identity:** $1 = \mathbf{E}_x[f(x)^2] = \sum_S \hat{f}(S)^2$.

- Every function $f : \{-1,1\}^n \to \{-1,1\}$ has a unique (Fourier) representation as a multilinear polynomial

$$f(x) = \sum_{S \subseteq [n]} \hat{f}(S) \prod_{i \in S} x_i$$

  where $\hat{f}(S) = \mathbf{E}_x[f(x) \prod_{i \in S} x_i]$.
- **Parseval's identity:** $1 = \mathbf{E}_x[f(x)^2] = \sum_S \hat{f}(S)^2$.
- **Fourier weights:** $\mathbf{W}^k[f] \triangleq \sum_{S:|S|=k} \hat{f}(S)^2$.

- Every function $f : \{-1,1\}^n \to \{-1,1\}$ has a unique (Fourier) representation as a multilinear polynomial

$$f(x) = \sum_{S \subseteq [n]} \hat{f}(S) \prod_{i \in S} x_i$$

  where $\hat{f}(S) = \mathbf{E}_x[f(x) \prod_{i \in S} x_i]$.
- **Parseval's identity:** $1 = \mathbf{E}_x[f(x)^2] = \sum_S \hat{f}(S)^2$.
- **Fourier weights:** $\mathbf{W}^k[f] \triangleq \sum_{S:|S|=k} \hat{f}(S)^2$.
- $\deg(f) \triangleq \max\{|S| : \hat{f}(S) \neq 0\}$.

- Every function $f : \{-1,1\}^n \to \{-1,1\}$ has a unique (Fourier) representation as a multilinear polynomial

$$f(x) = \sum_{S \subseteq [n]} \hat{f}(S) \prod_{i \in S} x_i$$

where $\hat{f}(S) = \mathbf{E}_x[f(x) \prod_{i \in S} x_i]$.

- **Parseval's identity:** $1 = \mathbf{E}_x[f(x)^2] = \sum_S \hat{f}(S)^2$.
- **Fourier weights:** $\mathbf{W}^k[f] \triangleq \sum_{S:|S|=k} \hat{f}(S)^2$.
- $\deg(f) \triangleq \max\{|S| : \hat{f}(S) \neq 0\}$.
- **Granularity:** if $\deg(f) = d$ then $\forall S : \hat{f}(S) = \text{integer} \cdot 2^{-d}$.

- Every function $f : \{-1,1\}^n \to \{-1,1\}$ has a unique (Fourier) representation as a multilinear polynomial

$$f(x) = \sum_{S \subseteq [n]} \hat{f}(S) \prod_{i \in S} x_i$$

  where $\hat{f}(S) = \mathbf{E}_x[f(x) \prod_{i \in S} x_i]$.
- **Parseval's identity:** $1 = \mathbf{E}_x[f(x)^2] = \sum_S \hat{f}(S)^2$.
- **Fourier weights:** $\mathbf{W}^k[f] \triangleq \sum_{S:|S|=k} \hat{f}(S)^2$.
- $\deg(f) \triangleq \max\{|S| : \hat{f}(S) \neq 0\}$.
- **Granularity:** if $\deg(f) = d$ then $\forall S : \hat{f}(S) = \text{integer} \cdot 2^{-d}$.
- **Approximate Degree:**
  $\widetilde{\deg}_\epsilon(f) \triangleq \min\{\deg(p) \mid \forall x : |p(x) - f(x)| \leq \epsilon\}$.

Proof Overview

1. $\widetilde{\deg}_{1/3}(f) \le O(\sqrt{L(f)})$

Proof Overview

1. $\widetilde{\deg}_{1/3}(f) \leq O(\sqrt{L(f)})$
2. Exponentially small Fourier tails: $\mathbf{W}^{>k}[f] \leq e^{-k/\sqrt{L(f)}}$.
   (where $\mathbf{W}^{>k}[f] \triangleq \sum_{|S|>k} \hat{f}(S)^2$)

Proof Overview

1. $\widetilde{\deg}_{1/3}(f) \leq O(\sqrt{L(f)})$
2. Exponentially small Fourier tails: $\mathbf{W}^{>k}[f] \leq e^{-k/\sqrt{L(f)}}$.
   (where $\mathbf{W}^{>k}[f] \triangleq \sum_{|S|>k} \hat{f}(S)^2$)
3. Degree shrinkage: $\mathbf{Pr}_{\rho\sim\mathcal{R}_p}[\deg(f|_\rho) = d] \leq \left(4p\sqrt{L(f)}\right)^d$.

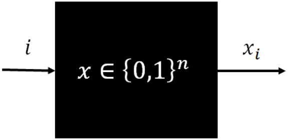
Proof Overview

1. $\widetilde{\deg}_{1/3}(f) \le O(\sqrt{L(f)})$
2. Exponentially small Fourier tails: $\mathbf{W}^{>k}[f] \le e^{-k/\sqrt{L(f)}}$.
   (where $\mathbf{W}^{>k}[f] \triangleq \sum_{|S|>k} \hat{f}(S)^2$)
3. Degree shrinkage: $\mathbf{Pr}_{\rho\sim\mathcal{R}_p}[\deg(f|_\rho) = d] \le \left(4p\sqrt{L(f)}\right)^d$.
4. The low probability case:
   if $p \le \frac{1}{1000\sqrt{L(f)}}$, then $\mathbf{E}_{\rho\sim\mathcal{R}_p}[L(f|_\rho)] = O(1)$.

Proof Overview

1. $\widetilde{\deg}_{1/3}(f) \le O(\sqrt{L(f)})$
2. Exponentially small Fourier tails: $\mathbf{W}^{>k}[f] \le e^{-k/\sqrt{L(f)}}$.
   (where $\mathbf{W}^{>k}[f] \triangleq \sum_{|S|>k} \hat{f}(S)^2$)
3. Degree shrinkage: $\mathbf{Pr}_{\rho\sim\mathcal{R}_p}[\deg(f|_\rho) = d] \le \left(4p\sqrt{L(f)}\right)^d$.
4. The low probability case:
   if $p \le \frac{1}{1000\sqrt{L(f)}}$, then $\mathbf{E}_{\rho\sim\mathcal{R}_p}[L(f|_\rho)] = O(1)$.
5. The general case: $\mathbf{E}_{\rho\sim\mathcal{R}_p}[L(f|_\rho)] = O(p^2 L(f) + 1)$.

- **Recall:** $\widetilde{\deg}_\epsilon(f) \triangleq \min\{\deg(p) \mid \forall x : |p(x) - f(x)| \le \epsilon\}$
- The **Black Box model**



$$\widetilde{\deg}_{1/3}(f) \le O(Q_2(f)) \quad \text{([Beals Buhrman Cleve Mosca de Wolf '98])}$$
$$= \Theta(\mathrm{ADV}^{\pm}(f)) \quad \text{([Reichardt '11])}$$
$$\le O(\sqrt{L(f)}) \quad \text{([Høyer Lee Spalek '07])}$$

- **Open:** is there a classical proof for $\widetilde{\deg}_{1/3}(f) \le O(\sqrt{L(f)})$?

Claim [Buhrman Newman Röhrig de Wolf '05]:

$\forall t : \widetilde{\deg}_{e^{-t}}(f) \leq \widetilde{\deg}_{1/3}(f) \cdot t.$

Proof Idea: If $p(x)$ approx. $f(x)$ up to err. $1/3$ then $\mathrm{MAJ}_t(p(x), \ldots, p(x))$ approx. $f(x)$ up to err. $\exp(-t)$.

Claim [Buhrman Newman Röhrig de Wolf '05]:

$\forall t : \widetilde{\deg}_{e^{-t}}(f) \leq \widetilde{\deg}_{1/3}(f) \cdot t.$

Proof Idea: If $p(x)$ approx. $f(x)$ up to err. $1/3$ then $\mathrm{MAJ}_t(p(x), \ldots, p(x))$ approx. $f(x)$ up to err. $\exp(-t)$.

Claim:

$\forall k : \mathbf{W}^{>k}[f] \leq e^{-k/\widetilde{\deg}_{1/3}(f)}$

Proof Idea:

1. An L_∞ approx. is in particular an L_2 approx.
2. $f^{\leq k}(x) \triangleq \sum_{|S| \leq k} \hat{f}(S) \prod_{i \in S} x_i$
   is the best L_2 approx. among degree $\leq k$ polynomials.

Theorem

Let t be some parameter. If $\forall k : \mathbf{W}^{>k}[f] \leq e^{-k/t}$ then

$$\forall p, d : \Pr_{\rho \sim \mathcal{R}_p} [\deg(f|_\rho) = d] \leq (4pt)^d$$

Theorem

Let t be some parameter. If $\forall k : \mathbf{W}^{>k}[f] \leq e^{-k/t}$ then

$$\forall p, d : \Pr_{\rho \sim \mathcal{R}_p} [\deg(f|_\rho) = d] \leq (4pt)^d$$

Proof Idea:

1. Under restriction the Fourier mass at level d is extremely small: $\mathbf{E}_{\rho \sim \mathcal{R}_p}[\mathbf{W}^d[f|_\rho]] \leq (pt)^d$.

Theorem

Let t be some parameter. If $\forall k : \mathbf{W}^{>k}[f] \leq e^{-k/t}$ then

$$\forall p, d : \mathop{\mathbf{Pr}}_{\rho \sim \mathcal{R}_p}[\deg(f|_\rho) = d] \leq (4pt)^d$$

Proof Idea:

1. Under restriction the Fourier mass at level d is extremely small: $\mathbf{E}_{\rho \sim \mathcal{R}_p}[\mathbf{W}^d[f|_\rho]] \leq (pt)^d$.
2. If $f|_\rho$ is of degree d then Fourier mass at level d is at least 4^{-d} (Granularity).

Theorem

Let t be some parameter. If $\forall k : \mathbf{W}^{>k}[f] \leq e^{-k/t}$ then

$$\forall p, d : \Pr_{\rho \sim \mathcal{R}_p} [\deg(f|_\rho) = d] \leq (4pt)^d$$

Proof Idea:

1. Under restriction the Fourier mass at level d is extremely small: $\mathbf{E}_{\rho \sim \mathcal{R}_p}[\mathbf{W}^d[f|_\rho]] \leq (pt)^d$.
2. If $f|_\rho$ is of degree d then Fourier mass at level d is at least 4^{-d} (Granularity).
3. $\implies$ the probability that the degree is d must be small:

$$(pt)^d \geq \mathop{\mathbf{E}}_{\rho \sim \mathcal{R}_p} [\mathbf{W}^d[f|_\rho]]$$

Theorem

Let t be some parameter. If $\forall k : \mathbf{W}^{>k}[f] \leq e^{-k/t}$ then

$$\forall p, d : \underset{\rho \sim \mathcal{R}_p}{\mathbf{Pr}}[\deg(f|_\rho) = d] \leq (4pt)^d$$

Proof Idea:

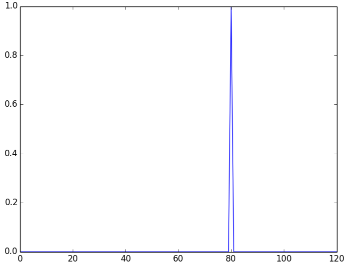
1. Under restriction the Fourier mass at level d is extremely small: $\mathbf{E}_{\rho \sim \mathcal{R}_p}[\mathbf{W}^d[f|_\rho]] \leq (pt)^d$.
2. If $f|_\rho$ is of degree d then Fourier mass at level d is at least 4^{-d} (Granularity).
3. $\implies$ the probability that the degree is d must be small:

$$(pt)^d \geq \underset{\rho \sim \mathcal{R}_p}{\mathbf{E}}[\mathbf{W}^d[f|_\rho]] \geq 4^{-d} \cdot \underset{\rho \sim \mathcal{R}_p}{\mathbf{Pr}}[\deg(f|_\rho) = d]$$

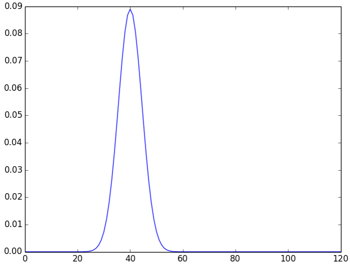
Claim [Linial Mansour Nisan '89]

$$\mathbf{E}_{\rho\sim\mathcal{R}_p}[\mathbf{W}^d[f|_\rho]] = \sum_{k\geq d} \mathbf{W}^k[f]\cdot\mathbf{Pr}[\mathrm{Bin}(k,p)=d]$$

$\mathbf{W}^k[f]$



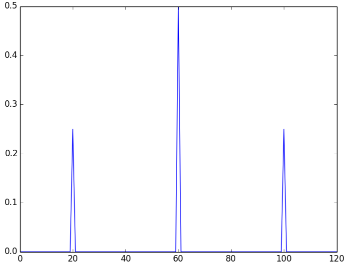
$\mathbf{E}[\mathbf{W}^d[f|_\rho]]$



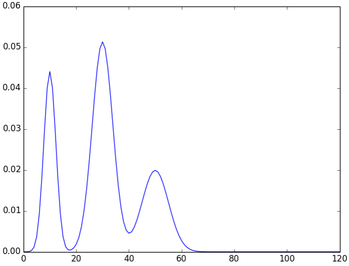
Claim [Linial Mansour Nisan ’89]

$$\mathbf{E}_{\rho\sim\mathcal{R}_p}[\mathbf{W}^d[f|_\rho]] = \sum_{k\geq d} \mathbf{W}^k[f] \cdot \mathbf{Pr}[\mathrm{Bin}(k,p) = d]$$

$\mathbf{W}^k[f]$



$\mathbf{E}[\mathbf{W}^d[f|_\rho]]$



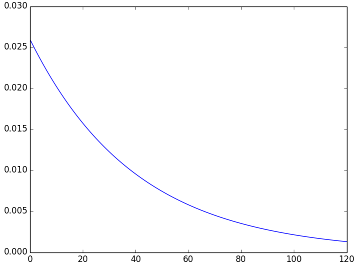
Step 3.1

Exponentially small Fourier tails implies "Degree Shrinkage"

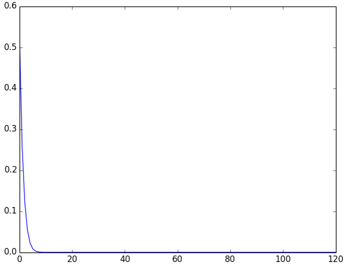
Claim [Linial Mansour Nisan '89]

$$\mathbf{E}_{\rho\sim\mathcal{R}_p}[\mathbf{W}^d[f|_\rho]] = \sum_{k\geq d}\mathbf{W}^k[f]\cdot\mathbf{Pr}[\mathrm{Bin}(k,p)=d]$$

$\mathbf{W}^k[f]$



$\mathbf{E}[\mathbf{W}^d[f|_\rho]]$



$$\forall k : \mathbf{W}^{>k}[f] \leq e^{-k/t} \implies \forall d : \mathbf{E}_{\rho\sim\mathcal{R}_p}[\mathbf{W}^d[f|_\rho]] \leq (pt)^d.$$

Step 4 - The low probability case

- **Recall:** $\mathbf{Pr}[\deg(f|_\rho) = d] \leq (4p\sqrt{L(f)})^d$.
- **Fact:** If $\deg(g) = d$ then $L(g) \leq 32^d$.

Theorem

If $p \leq \frac{1}{1000\sqrt{L(f)}}$ then $\mathbf{E}[L(f|_\rho)] = O(1)$.

Step 4 - The low probability case

- **Recall:** $\mathbf{Pr}[\deg(f|_\rho) = d] \leq (4p\sqrt{L(f)})^d$.
- **Fact:** If $\deg(g) = d$ then $L(g) \leq 32^d$.

Theorem

If $p \leq \frac{1}{1000\sqrt{L(f)}}$ then $\mathbf{E}[L(f|_\rho)] = O(1)$.

Proof:

$$\mathbf{E}[L(f|_\rho)] = \sum_{d=0}^{n} \mathbf{Pr}\left[\deg(f|_\rho) = d\right] \cdot \mathbf{E}\left[L(f|_\rho) | \deg(f|_\rho) = d\right]$$

$$\leq \sum_{d=0}^{n} \left(\frac{1}{250}\right)^d \cdot 32^d = O(1)$$

Step 4 - The low probability case

- **Recall:** $\mathbf{Pr}[\deg(f|_\rho) = d] \le (4p\sqrt{L(f)})^d$.
- **Fact:** If $\deg(g) = d$ then $L(g) \le 32^d$.

Theorem

If $p \le \frac{1}{1000\sqrt{L(f)}}$ then $\mathbf{E}[L(f|_\rho)] = O(1)$.

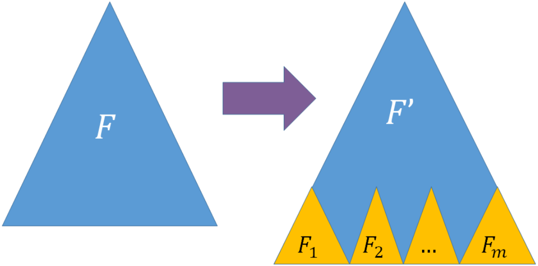
Proof:

$$\mathbf{E}[L(f|_\rho)] = \sum_{d=0}^{n} \mathbf{Pr}\left[\deg(f|_\rho) = d\right] \cdot \mathbf{E}\left[L(f|_\rho) \middle| \deg(f|_\rho) = d\right]$$

$$\le \sum_{d=0}^{n} \left(\frac{1}{250}\right)^d \cdot 32^d = O(1)$$

Step 5 - The general case

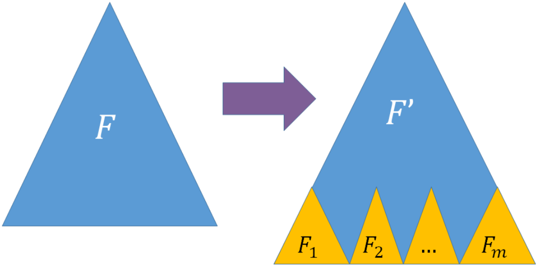
- Based on **[Impagliazzo Meka Zuckerman '12]**: For a given ℓ, we can transform any formula F into a nicer formula F',



where $m = O\left(\frac{L(F)}{\ell} + 1\right)$, and $\forall i : L(F_i) \leq \ell$.

Step 5 - The general case

- Based on **[Impagliazzo Meka Zuckerman '12]**: For a given ℓ, we can transform any formula F into a nicer formula F',



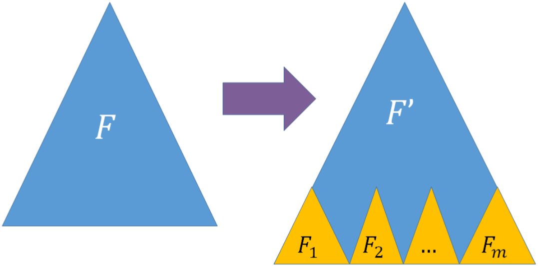
where $m = O\left(\frac{L(F)}{\ell} + 1\right)$, and $\forall i : L(F_i) \leq \ell$.

- Pick $\ell := \frac{1}{1000^2 p^2}$. In each subformula $\mathbf{E}[L(F_i|_\rho)] = O(1)$.

$$\mathbf{E}[L(F'|_\rho)] \leq \sum_i \mathbf{E}[L(F_i|_\rho)] = O\left(m\right) = O(p^2 L(F) + 1).$$

Step 5 - The general case

- Based on **[Impagliazzo Meka Zuckerman '12]**: For a given ℓ, we can transform any formula F into a nicer formula F',



where $m = O\left(\frac{L(F)}{\ell} + 1\right)$, and $\forall i : L(F_i) \leq \ell$.

- Pick $\ell := \frac{1}{1000^2 p^2}$. In each subformula $\mathbf{E}[L(F_i|_\rho)] = O(1)$.

$$\mathbf{E}[L(F'|_\rho)] \leq \sum_i \mathbf{E}[L(F_i|_\rho)] = O\left(m\right) = O(p^2 L(F) + 1). \quad \blacksquare$$

Recap

- Main motivation: **P** vs. $\mathbf{NC^1}$.
- $O(p^2)$ shrinkage implies $\frac{n^3}{(\log n)^{2+o(1)}}$ lower bounds for A.

Recap

- Main motivation: **P** vs. $\mathbf{NC^1}$.
- $O(p^2)$ shrinkage implies $\frac{n^3}{(\log n)^{2+o(1)}}$ lower bounds for A.
- New proof for $O(p^2)$ shrinkage:
  1. $\widetilde{\deg}(f) \le O(\sqrt{L(f)})$ using quantum query complexity
  2. Exponentially small Fourier tails
  3. Degree shrinkage
  4. The low probability case
  5. The general case

Recap

- Main motivation: **P** vs. $\mathbf{NC^1}$.
- $O(p^2)$ shrinkage implies $\frac{n^3}{(\log n)^{2+o(1)}}$ lower bounds for A.
- New proof for $O(p^2)$ shrinkage:
  1. $\widetilde{\deg}(f) \leq O(\sqrt{L(f)})$ using quantum query complexity
  2. Exponentially small Fourier tails
  3. Degree shrinkage
  4. The low probability case
  5. The general case
- **Open Question:** Breaking the n^3 barrier.

Recap

- Main motivation: **P** vs. $\mathbf{NC^1}$.
- $O(p^2)$ shrinkage implies $\frac{n^3}{(\log n)^{2+o(1)}}$ lower bounds for A.
- New proof for $O(p^2)$ shrinkage:
  1. $\widetilde{\deg}(f) \leq O(\sqrt{L(f)})$ using quantum query complexity
  2. Exponentially small Fourier tails
  3. Degree shrinkage
  4. The low probability case
  5. The general case
- **Open Question:** Breaking the n^3 barrier.
- **Open Question [Håstad, Paterson-Zwick]**: What is the shrinkage exponent of monotone De Morgan formulae?
- Enough to prove the low probability case.

Thank You